Smart Data

Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data

Datenschutzgrundprinzipien im Diskurs.
Eine Veröffentlichung der Fachgruppen „Rechtsrahmen“ und „Sicherheit“ der Smart-Data-Begleitforschung.

Impressum

Herausgeber
Smart-Data-Begleitforschung
FZI Forschungszentrum Informatik
Außenstelle Berlin
Friedrichstr. 60, 10117 Berlin
www.smart-data-programm.de

Redaktion und Konzeption
Fachgruppen Rechtsrahmen und Sicherheit der
Smart-Data-Begleitforschung

Schlussredaktion und Gestaltung
LoeschHundLiepold Kommunikation GmbH

Stand
November 2016

Druck
WIRmachenDRUCK

Bildnachweis
Weissblick – Fotolia.com (Titel), sebra – Fotolia.com (S. 4), ra2 studio – Fotolia.com (S.7), Pavlo Vakhrushev – Fotolia.com (S. 13), WavebreakmediaMicro – Fotolia.com (S. 17), Boggy – Fotolia.com (S. 24), Kzenon – Fotolia.com (S. 30, 32), Oskar – Fotolia.com (S. 35), GRÜNBUCH Digitale Plattformen, Bundesministerium für Wirtschaft und Energie (BMWi) – gettyimages.de (S. 38), Rawpixel.com – Fotolia.com (S. 49)

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

Einleitung

Dieses Arbeitspapier präsentiert den aktuellen Stand der Diskussion in der Fachgruppe Rechtsrahmen. Die wesentlichen Erkenntnisse sollen Rechtsanwendern einen einfachen Überblick über die rechtlichen Anforderungen geben. Dabei gilt es jedoch zu berücksichtigen, dass generalisierende Aussagen nicht die Besonderheiten des Einzelsachverhalts und ggf. einschlägige bereichsspezifische Sonderregelungen adressieren können. Daneben sollen technische, aber auch rechtliche Lösungskonzepte sowie aktuelle Spannungen und Entwicklungen im Kontext von Smart Data dargestellt werden.

Der erste Themenkomplex behandelt nach der Diskussion der Begriffe Datensparsamkeit und Datenreichtum rechtliche Fragestellungen im Hinblick auf die Zweckbindung: ein Überblick über die Grundlagen der aktuellen Rechtslage und zu erwartende Anpassungen durch die ab 2018 anzuwendende Datenschutzgrundverordnung sowie die Zweckbindung im Rahmen der Einwilligung in wissenschaftliche Forschungsvorhaben. Weiterer Harmonisierungsbedarf wird bezüglich des Datenschutzes in der medizinischen Forschung aufgezeigt. Als Ausblick auf eine künftige Interpretation der Zweckbindung wird erörtert, ob die Gesamtheit der Grundrechte einen Maßstab für das Zweckbindungsprinzip herangezogen werden sollte. Im Anschluss werden aus datenschutz- und wettbewerbsrechtlicher Sicht Impulse für einen „Rechtsrahmen 4.0“ gegeben.

Im Themenkomplex „Smart-Data-Lösungskonzepte zur technischen Durchsetzung der Zweckbindung“ wird die Möglichkeit des Einsatzes der Datennutzungskontrolle (Usage Control) zur technischen Durchsetzung

festgelegter Datennutzungszwecke vorgestellt. Mit Ind²uce wird ein Verfahren zur Datennutzungskontrolle präsentiert. Darüber hinaus wird ein Modell zum automatisierten Abgleich von Zertifikaten vorgestellt, das bei der Einbindung externer Anbieter in Geschäftsmodelle die Einhaltung der mit dem Nutzer vereinbarten Datenschutzpräferenzen unterstützen kann.

Hier vorgestellte Konzepte und Forschungsansätze erheben keinen Anspruch auf Vollständigkeit, sondern sollen Denkanstöße bieten. Wichtig ist jedoch, die bereits zurückgelegten Schritte zu dokumentieren, zu veröffentlichen und zu diskutieren, damit ein stetiger Fortschritt nicht nur im Rahmen der Forschung, sondern auf sämtlichen Ebenen der Gesellschaft, der Politik und der Wirtschaft möglich ist. Daneben dürfen aktuelle Entwicklungen und Trends nicht unbeachtet bleiben. Die technische Machbarkeit von Softwarelösungen zur Wissensgenerierung löst zwangsläufig den Wunsch aus, diese auch zu nutzen, jedoch können die Informationsgewinnung und-auswertung persönlichkeitsverletzenden Charakter haben. Nur die Zusammenarbeit der Experten aus den verschiedenen Bereichen, wie Juristen, Softwareentwickler und Ökonomen, kann zu einem Gelingen neuartiger Smart-Data-Konzepte beitragen.

Thesen der Fachgruppe Rechtsrahmen

Was bedeutet Smart Data?

Anonymisierung und Privacy by Design

Smart Data ist eine Weiterentwicklung von Big Data. Unter Big Data werden überwiegend solche Szenarien verstanden, die ein erhebliches Konfliktpotenzial in Bezug auf die Grundprinzipien des Datenschutzes, insbesondere die der Zweckbindung und der Datensparsamkeit, mit sich bringen.[1]

Die Smart-Data-Projekte arbeiten an Lösungen, die Ziele der Datenauswertung und des Datenschutzes in Einklang zu bringen. Denn „smart“ bedeutet nicht nur intelligente Analyse, sondern auch datenschutzfreundliche Technikgestaltung.

Selektion wertvoller Inhalte (Filterung)

Der Fokus vieler Smart-Data-Projekte liegt größtenteils in der Auswertung von Sach- und Ereignisdaten. Datenschutzrechtliche Implikationen stellen sich jedoch oft bei der Frage, wann eine rechtswirksame Anonymisierung vorliegt, da die Datenquellen durchaus Personenbezug aufweisen können.

Smart Data Protection

Datenschutz als Wettbewerbsvorteil nutzen

Aufgrund von Konzepten wie Zweckbindung und Datensparsamkeit empfinden viele Rechtsanwender das deutsche bzw. europäische Datenschutzrecht gegenüber anderen Rechtsordnungen wie beispielsweise dem amerikanischen Recht als streng und innovationshemmend. Die Mehrheit der Smart-Data-Projekte sieht in diesen im Vergleich strengeren Regelungen jedoch eher einen Wettbewerbsvorteil, da die Konformität mit den gesetzlichen Anforderungen weltweit das Vertrauen der Kunden in einen die widerstreitenden Interessen angemessen ausgleichenden Schutz der Privatsphäre wecken kann. Dass eine Mehrheit der Verbraucher/-innen sehr viel Wert auf den Schutz ihrer Privatsphäre legt und sich eine Vielzahl durch neue datengetriebene Geschäftsmodelle im Zusammenhang mit Big Data verunsichert fühlt, zeigen jüngste Studien.[2] Umso wichtiger ist es für innovative Unternehmen, Vertrauen zu schaffen und nachweisbare Schutzmaßnahmen vorweisen zu können. „Made in Germany“ kann somit auch im digitalen Zeitalter eine Qualitätsmarke sein.

Dissonanz zwischen Recht und Wirklichkeit überwinden

Jedoch zeigt sich gerade im Datenschutzrecht häufig ein wesentliches Durchsetzungsdefizit: Viele Anbieter digitaler Inhalte erheben aus unterschiedlichen Gründen eine Vielzahl personenbezogener Daten, ohne Nutzer klar und unmissverständlich darüber aufzuklären.[3] Dies könnte einerseits der Nichtanwendbarkeit deutschen Rechts im internationalen Kontext und andererseits dem Fehlen effektiver Kontroll- und Sanktionsmechanismen geschuldet sein. Neben der Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Nutzer kann dieser Umstand auch wettbewerbsverzerrende Auswirkungen haben: Konkurrierende Anbieter, die sich, um Rechtskonformität zu gewährleisten, auf die Erhebung und Verarbeitung zwingend erforderlicher Daten beschränken oder aufgrund von Pseudonymisierung oder Anonymisierung Qualitätsverluste der Datenbasis hinnehmen, können benachteiligt sein. Daher stellt sich die zentrale Frage: Sollte das Recht stärker durchgesetzt werden oder das Recht an die Wirklichkeit angepasst werden?

Einen wichtigen Schritt in Richtung „level playing field“ könnte die Datenschutzgrundverordnung mit dem Marktortprinzip sowie empfindlichen Sanktionen mit sich bringen.

Das Prinzip der Einwilligung handhabbar machen

Die datenschutzrechtlichen Einwilligungen werden vermehrt als reine Fiktion bezeichnet, da die Erklärungen selten informiert, sondern häufig pauschal erfolgen.[4] Eine Herausforderung auch für Smart-Data-Projekte ist daher, wie technische oder rechtliche Konzepte die freiwillige, informierte und bewusste Selbstbestimmung herstellen können. Auch hier finden sich aus rechtlicher Sicht erste Ansätze in der Datenschutzgrundverordnung: Die Aufklärung über die Datenverarbeitung muss in verständlicher, leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erfolgen. Die Informationen können auch in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um die Wahrnehmbarkeit, Verständlichkeit und Nachvollziehbarkeit sowie einen aussagekräftigen Überblick zu gewährleisten. Eine vertragliche Leistung darf nicht an die Einwilligung in für diese Leistung nicht erforderliche Datenverarbeitung abhängig gemacht werden (Kopplungsverbot). Vielmehr muss dem Betroffenen eine echte Wahlmöglichkeit gewährt werden.

Es existieren bereits technische Lösungen, um ausdifferenzierte Auswahlmöglichkeiten umzusetzen, wie beispielsweise Sticky Policies, Datennutzungskontrolle[5] oder der automatisierte Abgleich von Privatsphäreneinstellungen.[6] Nutzer könnten somit selbstbestimmt entscheiden, inwieweit die Verarbeitung ihrer Daten begrenzt werden soll oder öffentlich preisgegebene Daten als Gemeingut für Informationsintermediäre frei nutzbar sein sollen.

Berücksichtigung des Umfelds der Datenverarbeitung für die Bestimmung des Personenbezugs

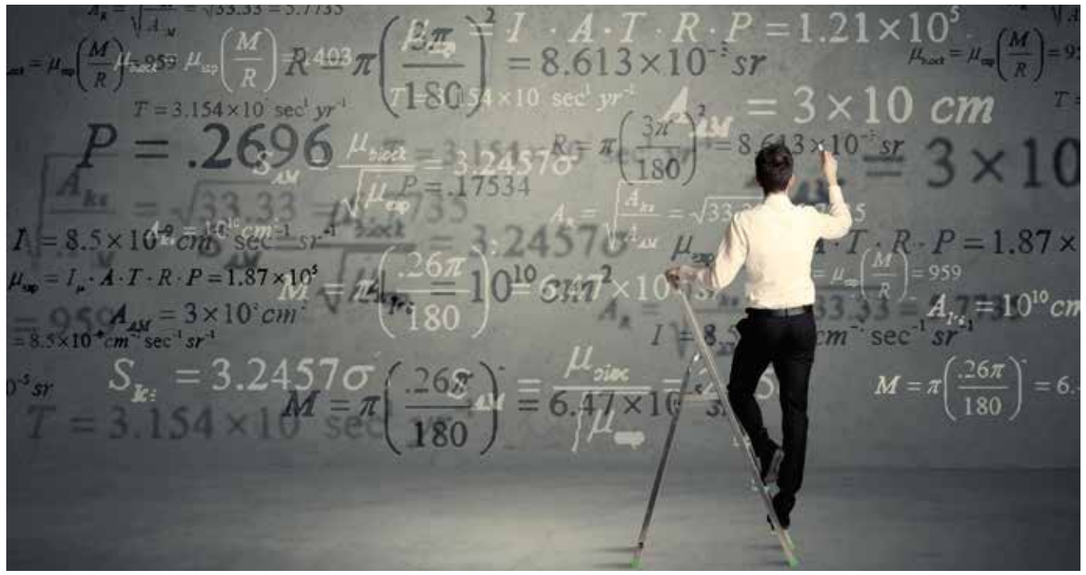
Personenbezogene Daten werden in Smart-Data-Projekten in den unterschiedlichsten Kontexten erhoben. Sensordaten aus Maschinen könnten Personenbezug aufweisen, sobald die Zuordnung zu dem die Maschine bedienenden Menschen möglich ist. Anonymisierte Datenbanken könnten durch die Kombination mit weiteren Daten deanonymisiert werden.[7] Nutzer hinterlassen Onlinespuren, sodass mittels Tracking die Identifizierung erfolgen kann.[8] Dabei hängt die Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung maßgeblich vom Umfeld und Kontext der Datenverarbeitung ab: Richtet sich die Verarbeitung auf die Individualisierung und Ausforschung des Betroffenen oder ist der Personenbezug vielmehr eine zufällige Begleiterscheinung? Lassen die Daten Rückschlüsse auf die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben zu, handelt es sich um besondere Arten personenbezogener Daten. Die Sensibilität der Daten kann nicht kontextunabhängig bestimmt werden. Zum einen ist nicht garantiert, dass bereits zum Erhebungszeitpunkt besonders sensible Daten vorliegen – diese können auch erst aus der Analyse entstehen.[9] Zum anderen könnte sich der starre Katalog als Innovations- und Effizienzbremse erweisen, wenn keine Kontextbetrachtung hinzutritt.

Gesetzliche Anreize für den Einsatz von Privacy Enhancing Technologies schaffen

Privacy Enhancing Technologies (PET) können Datenschutzrisiken abwenden, indem die Eingriffsintensität gesenkt wird. Daher stellt sich die Frage, ob beim Einsatz dieser Technologien eine weitergehende Verarbeitungserlaubnis z. B. bei der Zweckbindung gesetzlich gewährt werden sollte. Eine solche Privilegierung könnte in der Datenschutzgrundverordnung dadurch bewirkt werden, dass Pseudonymisierung und Verschlüsselung als geeignete Garantien bei der Prüfung der Vereinbarkeit neuer Zwecke mit den ursprünglichen Zwecken anerkannt werden. Eine Verpflichtung, PETs einzusetzen, könnte aus Art. 25, data protection by design und by default (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung), folgen.

Datensparsamkeit nicht zugunsten des Datenreichtums aufgeben

Die Datensparsamkeit gebietet so wenig Daten mit Personenbezug wie möglich zu verarbeiten sowie, wo möglich und zumutbar, zu anonymisieren oder zu pseudonymisieren. Aufgrund von Big Data und Vorratsdatenspeicherung ist dieser Grundsatz häufig angegriffen worden: Sollten sowohl private als auch öffentliche Stellen personenbezogene Daten auf Vorrat erheben und speichern dürfen, um diese bei Bedarf auf noch unbekannte Zusammenhänge und ggf. für noch unbekannte Zwecke zu analysieren? Damit einhergehen würde auch eine wesentliche Aufweichung des Zweckbindungsprinzips. Hier stellt sich die Frage: Kann das Datenschutzrecht in seiner derzeitigen Konzeption ohne Zweckbindung funktionieren und gibt es Mechanismen, die als Kompensation eine Aufweichung der Zweckbindung bei gleichzeitiger Aufrechterhaltung des verfassungsrechtlich gebotenen Schutzniveaus ermöglichen könnten?



Das Datenschutzgrundprinzip der Zweckbindung: zwischen angemessenem Schutzniveau und digitalem Fortschritt

Datensparsamkeit und Datenreichtum – ein Widerspruch?

Von Peter Schaar, Europäische Akademie für Informationsfreiheit und Datenschutz

Der im Jahr 2001 in das Bundesdatenschutzgesetz eingefügte § 3a verpflichtet die für die Datenverarbeitung verantwortlichen Stellen zu „Datenvermeidung und Datensparsamkeit“. Konkret geht es dabei um die Ausrichtung der Auswahl, der Gestaltung und des Betriebs von Datenverarbeitungssystemen an der Maxime, „so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen“. Insbesondere sind die Daten zu anonymisieren oder zu pseudonymisieren, „soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert“. Mit der Einführung des Grundsatzes der Datenvermeidung und-sparsamkeit wollte der Gesetzgeber Einfluss auf die Gestaltung der Systemstrukturen nehmen, in denen personenbezogene Daten erhoben und verarbeitet werden.[10]

Insbesondere der Begriff der „Datensparsamkeit“ ist im Kontext von Big-Data-Konzepten und im Rahmen von auf Smart Data basierenden Geschäftsmodellen in Frage gestellt worden. So heißt es etwa in den vom Bundesministerium für Wirtschaft und Energie zum IT-Gipfel 2015 veröffentlichten „Leitplanken Digitaler Souveränität“, die „Möglichkeit, mit Daten umgehen und ‚arbeiten‘ zu können, ist essenziell für die Entwicklung eigener Geschäftsmodelle und die Nutzung der Chancen der Digitalisierung. Deshalb dürfen datenbasierte digitale Geschäftsmodelle nicht durch ein unzeitgemäßes Datensparsamkeitsdiktat verhindert werden. … Bisherige Grundprinzipien des Datenschutzes wie Datensparsamkeit und Zweckbindung müssen überprüft und durch Prinzipien der Datenvielfalt und des Datenreichtums ergänzt und ersetzt werden“.[11]

> Das Privacy-by-Design-Konzept ist die Operationalisierung der verfassungsrechtlich begründeten Prinzipien der Erforderlichkeit und der Zweckbindung.

Nun ist der Begriff „Datensparsamkeit“ – genauso wie sein Pendant „Datenreichtum“ – durchaus **ambivalent**. Zum einen handelt es sich dabei nicht wirklich um Gegensätze, denn die Negationen von Sparsamkeit sind – positiv – Großzügigkeit oder – negativ – Verschwendung. Und das Gegenteil von Reichtum ist Armut. Ob Sparsamkeit eine Tugend ist, wie sie der schwäbischen Hausfrau zugeschrieben wird, oder aber in ihrer übersteigerten Form im Sinne von Geiz eine der sieben Todsünden, mag dahingestellt bleiben.

Daten unterscheiden sich ohnehin von körperlichen Gegenständen und deshalb sind Analogien zu anderen Alltagserkenntnissen mit Vorsicht zu genießen. Dies gilt für diese Begriffe genauso wie für andere gerne zitierte Sachverhalte, etwa „Datendiebstahl“, „Datenhehlerei“ oder „Dateneigentum“. Und trotzdem können diese Übertragungen auf unsere Alltagswelt durchaus zu dem Diskurs über die Gestaltung und Nutzung von Informationstechnik beitragen, insbesondere wenn es um die ethische und gesellschaftliche Dimension geht.

Datenüberfluss

Das empirisch belegte „Moore’sche Gesetz“, wonach sich die Leistungsfähigkeit der IT-Komponenten alle 18 bis 24 Monate verdoppelt, legt nahe, dass die technologische Realität von immer größeren Datenmengen geprägt ist. Den nächsten Quantensprung bringt das Internet of Things, das unsere Lebensumwelt auch in Bereichen digitalisiert, die bisher durch analoge Techniken geprägt waren. Die Datenverarbeitungsprozesse sind dabei funktional in die Gegenstände, Prozesse und Interaktionen integriert. Daten sind nicht mehr allein „Werkstoff“, sondern sowohl Voraussetzung als auch Ergebnis des Verarbeitungsprozesses, und sie fallen in bislang unbekanntem Umfang an. Insofern stimmt es schon, dass unsere hochtechnisierten Gesellschaften zunehmend „Datenreichtum“ produzieren.

Damit ist allerdings nicht gesagt, dass das Konzept der Datensparsamkeit auf den Müllhaufen der IT-Geschichte gehört. Um im Bild zu bleiben: Es gibt auch in reichen Gesellschaften durchaus Gründe, sparsam zu handeln, sei es beim Umgang mit natürlichen Ressourcen oder auch als Vorsorge für Notsituationen. Dass materieller Reichtum bisweilen auch zu Lasten wichtiger anderer Güter – etwa der Umwelt – geht oder dass die ihm zugrunde liegenden Prozesse vielfach Ungleichheit und Ausbeutung voraussetzen oder erzeugen, kann heute niemand mehr bestreiten. Auch bei dem Umfang gespeicherter Daten und der Verfügung über sie muss die Frage erlaubt sein, ob es hier zu vergleichbaren negativen externen Effekten kommt. Sofern man nicht der maßlosen Datenerzeugung das Wort redet, was ich nicht einmal den Befürwortern des „Datenreichtums“ unterstellen würde, stellt sich die Frage des rechten Maßes, und zwar nicht nur in Bezug auf Datenvolumina, sondern auch im Hinblick auf die Rahmenbedingungen ihrer Verarbeitung, der Transparenz der Prozesse und Strukturen und der Verwendung der einzelnen Daten oder der aus großen Datenmengen gewonnenen Erkenntnisse.

> Nicht nur die Gefährdungsszenarien, sondern auch die Möglichkeiten zum technologischen Datenschutz haben sich seit dem Volkszählungsurteil verändert.

Es geht um die sehr bedeutsame Frage, inwieweit es überhaupt wünschenswert ist, Informationstechnik datenschutzgerecht zu gestalten, denn die kritisierten Begriffe stehen im Zusammenhang mit dem übergreifenden Konzept „Privacy by Design“ (PbD), das heute zu den unbestrittenen Werkzeugen im globalen Datenschutz-Instrumentenkasten gehört und auch die im Jahr 2018 in Kraft tretende EU-Datenschutzgrundverordnung prägt. Wer diese Frage verneint, stellt nicht nur Privacy by Design in Frage, sondern den Datenschutz überhaupt. Denn das PbD-Konzept ist letztlich nichts anderes als die Operationalisierung der verfassungsrechtlich begründeten Prinzipien der Erforderlichkeit und der Zweckbindung. Erforderlichkeit und Zweckbindung ergeben nur zusammen einen Sinn, denn ohne Zweckfestlegung lässt sich die Erforderlichkeit der Daten nicht beurteilen. Die Speicherung von Daten ohne vorgegebenen Zweck stellt eine Vorratsspeicherung dar, die nur in besonderen Verarbeitungskontexten überhaupt zulässig sein kann (Statistik, Wissenschaft), wobei das zusätzliche Risiko durch entsprechende rechtliche und technisch-organisatorische Schutzvorkehrungen zu kompensieren ist. Insofern würde mit dem Abgehen von der Zweckbindung zwangsläufig auch der Erforderlichkeitsgrundsatz entsorgt.

Informationelle Selbstbestimmung

Zweckbindung und Erforderlichkeit sind – ebenso wie der Grundsatz der Vertraulichkeit – nicht deshalb überholt, weil sich die Technologie seit dem Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 rasant weiterentwickelt hat. Das Gericht hatte in dieser wegweisenden Entscheidung sein Konzept eines Grundrechts auf informationelle Selbstbestimmung entwickelt, wonach unter den „Bedingungen der modernen Datenverarbeitung … der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt“ werde. Das Grundrecht gewährleiste insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[12] Gerade die potenzielle Unbegrenztheit der elektronischen Datenverarbeitung mache den Schutz des Einzelnen erforderlich und verpflichte den Staat zur Gewährleistung der entsprechenden Rahmenbedingungen.

Das Gericht hatte dabei im Blick, dass sich die Informationstechnologie weiterentwickelt und immer leistungsfähiger wird. Die Befugnis zur Datenverarbeitung bedürfe „unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes.“[13] Personenbezogene Daten seien technisch gesehen unbegrenzt speicherbar und könnten jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abgerufen werden und sie „können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann“.[14]

Indem das Bundesverfassungsgericht im Volkszählungsurteil auf neue technische Verfahren zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten Bezug nimmt und eine angemessene rechtliche und technisch-organisatorische Absicherung derselben verlangt, folgt es im Grunde einem risikobasierten Ansatz: Je stärker die Gefährdungen, desto höher sind die Anforderungen an den Schutz. Damit unvereinbar ist jedenfalls die in den „Leitplanken“ erfolgende Polemik gegen ein angebliches „Datensparsamkeitsdiktat“ und das Plädoyer zur Aufweichung der Zweckbindung. Statt die verfassungsrechtlich erforderlichen Leitplanken der Informationsgesellschaft den gestiegenen Risiken anzupassen, wird für ihren Abbau plädiert.

Gleichwohl wäre es verfehlt, die Diskussion über einen zeitgemäßen und technikadäquaten Datenschutz mit Hinweis auf das Volkszählungsurteil zu beenden. Bei der Debatte kann und muss allerdings die Frage diskutiert werden, mit welchen dem heutigen Stand entsprechenden Mitteln das mittlerweile auch auf EU-Ebene garantierte Grundrecht auf Datenschutz gesichert werden kann. Denn nicht nur die Gefährdungsszenarien, sondern auch die Möglichkeiten zum technologischen Datenschutz haben sich seither sehr verändert. Ein solcher Ansatz ist das im Rahmen des Projekts vorgestellte Konzept der **Datennutzungskontrolle**.[15]

Big Data

„Big Data“ steht wie kein anderer Begriff für den Übergang zu einem neuen Modell des Umgangs mit Informationen. Der Begriff umschreibt den Umgang mit riesigen Datenmengen, „die zumeist im Rahmen einer Zweitverwertung zusammengeführt, verfügbar gemacht und ausgewertet werden“.[16] Bisweilen wird auch von den „3 Vs“ gesprochen: “high-volume, high-velocity and high-variety information assets“.[17]

Das Datenschutzrecht konnte in Zeiten von „Small Data“ durchaus Lösungen bereitstellen, die den Interessen der von der Datenverarbeitung betroffenen Personen und den für die Datenverarbeitung verantwortlichen Stellen (Behörden und Unternehmen) gleichermaßen genügten oder sie zumindest zum Ausgleich brachten.

> Die Herausforderung für Smart-Data-Projekte besteht darin, die Möglichkeiten einer rechts- und sozialverträglichen Technikgestaltung und -verwendung zu aktivieren.

Gleichwohl war bereits in den 1990er Jahren deutlich geworden, dass die Vorgaben des Datenschutzrechts technisch unterfüttert werden müssten. Die Begrenzung des technologischen Datenschutzes auf die Gewährleistung der Datensicherheit, also den eigentlichen Missbrauchsschutz, reiche nicht aus. Vielmehr bedürfe es der **Unterfütterung durch datenschutzgerechte Techniken**.[18]

„Big Data“-Ansätze folgen dem Paradigma, immer größere Datenberge anzuhäufen, in der Hoffnung, durch den Einsatz immer leistungsfähigerer Hard- und Software neue Erkenntnisse zu gewinnen. Gemäß diesem Paradigma handeln auch die erfolgreichen globalen Internetunternehmen, allen voran Google und Facebook. Je umfangreicher die aus dem Nutzungsverhalten gewonnenen Erkenntnisse sind, desto zielgenauer lassen sich Werbebotschaften adressieren und desto genauer passen sich die den Nutzern dargebotenen Informationen deren vermeintlichen oder tatsächlichen individuellen Interessen an. Bezogen auf das jeweilige Nutzerprofil für weniger relevant gehaltene Informationen werden ihnen nicht präsentiert oder nur nachrangig verfügbar gemacht. Je zielgenauer die entsprechende Werbebotschaft platziert wird, desto geringer ist der Streuverlust und desto höher ist der Preis, den der jeweilige Werbetreibende zu bezahlen hat.

Die nicht unbedeutenden Kosten der – nur vordergründig kostenlosen – Suchmaschinen, sozialen Netzwerke und anderer Internetdienste werden zum größten Teil mit einer Art **Umwegfinanzierung** über die werbende Wirtschaft aufgebracht, die ihre Aufwendungen den Kundinnen und Kunden natürlich über den Preis in Rechnung stellt. Auch Vermittlungsplattformen wie Uber oder Airbnb sind für die Nutzer nicht wirklich kostenlos. Letztlich bezahlen sie sogar

Datensparsamkeit trotz Massendaten

doppelt: durch ihre persönlichen Daten, die sie dem Anbieter der Vermittlungsplattform zur Verfügung stellen, und durch die in den Kaufpreis eines Produkts oder in die Nutzungsgebühr für kostenpflichtige Dienstleistungen einkalkulierte Vermittlungsprovision. Die genaue Höhe oder auch nur die Größenordnung des durch die Datennutzung erzielten Mehrwerts bleibt dem Verbraucher bzw. Nutzer verborgen.

Das einzelne Datum, das nach klassischem Datenschutzverständnis danach bewertet wird, ob es für die eigentliche Aufgabenerfüllung erforderlich ist oder eben nicht, verliert aus Sicht der Plattformbetreiber an Bedeutung. Gefragt sind immer größere, möglichst aus unterschiedlichen Quellen und Verarbeitungskontexten stammende Daten, die miteinander korreliert werden und dadurch Hinweise auf Zusammenhänge liefern können.

Datenschützer würden sich aber bei dem Versuch überheben, Big Data oder das Internet of Things zu verhindern. Auch um dem falschen Eindruck zu begegnen, sie kämpften als moderne Don Quijotes gegen die informationstechnischen „Windmühlen" des 21. Jahrhunderts, müssen sie sich auf die Gestaltungsmöglichkeiten von Big Data, Cloud-Diensten und des IoT konzentrieren. Die Herausforderung besteht also darin, die Möglichkeiten einer rechts- und sozialverträglichen Technikgestaltung und-verwendung zu erkennen und zu aktivieren. Bereits jetzt lassen sich eine Reihe von Stellschrauben erkennen, mit denen sich Datenschutzanforderungen auch angesichts neuer Paradigmen der Informationsgewinnung und sich schnell entwickelnder Technologien durchsetzen lassen. Die Sammlung, Aufbereitung und Auswertung der Daten sollten so gestaltet werden, dass sie grundsätzlich **ohne Personenbezug** erfolgen.

Bei einem solchen zeitgemäßen Datenschutzansatz geht es also nicht darum, das Datenaufkommen insgesamt zu minimieren, sondern darum, die Menge der auf einzelne natürliche Personen beziehbaren Daten zu minimieren. Dabei sollten der Charakter der personenbezogenen Daten und ihr Verwendungskontext beachtet werden.

> Bei einem zeitgemäßen Datenschutzansatz geht es nicht darum, das Datenaufkommen insgesamt zu minimieren, sondern darum, die Menge der auf einzelne natürliche Personen beziehbaren Daten zu minimieren.

Sowohl die Aussagekraft von Daten als auch die mit ihrer Verwendung verbundenen Risiken hängen vielfach mit der Speicherungsdauer zusammen. Von zentraler Bedeutung bleibt deshalb die Festlegung der entsprechenden Fristen, bei deren Erreichen Daten gelöscht bzw. anonymisiert werden.

Zunächst sollte die Verarbeitung großer Datenmengen so kanalisiert werden, dass der Umfang und die Menge direkt auf einzelne Personen bezogener Daten von Beginn an so gering wie möglich bleiben. Schon bei der Erhebung sollte stets geprüft werden, ob tatsächlich eine Vollerhebung aller in Frage kommenden personenbezogenen Daten erforderlich ist, und wenn ja für welchen Zeitraum.[19] Dies gilt speziell für die Prozessdaten (Meta Data), die zur Ausführung einer spezifischen Transaktion (Informationsabfrage im Internet, Steuerung eines technischen Geräts, Positionsbestimmung usw.) benötigt werden. Diese Daten weisen zwar im Regelfall bei isolierter Betrachtung eine geringe Sensitivität auf, ermöglichen aber – wenn sie massenhaft gespeichert werden – datenschutzrechtlich problematische detaillierte Persönlichkeitsprofile.

Bei der Speicherung sollten die Identifikationsangaben (Name, Anschrift usw.) von den Nutz- bzw. Inhaltsdaten getrennt werden. In vielen Anwendungsfeldern lässt sich durch die **Absonderung** und ggf. **Löschung** der Identifikationsdaten eine hinreichende Anonymisierung erreichen.

Sofern Daten einer Person, die aus verschiedenen Bereichen oder aus unterschiedlichen Zeitpunkten stammen, für rechtmäßige Zwecke zusammengeführt werden sollen, ist darauf zu achten, dass die Zusammenführung nicht mittels der persönlichen Identifikationsdaten, sondern unter **Pseudonym** erfolgt. Die Pseudonymisierung führt zwar vielfach nicht zur Aufhebung des Personenbezugs, vermindert aber die **Eingriffstiefe** in das Recht auf informationelle Selbstbestimmung und das Risiko des Datenmissbrauchs bei unrechtmäßigem Zugriff. Die Verwendung kryptographischer Verfahren kann den Risiken für die Vertraulichkeit und Integrität der Daten entgegenwirken.

Schließlich geht es darum, den Einzelnen wieder verstärkt zu befähigen, die Kontrolle über die ihn betreffenden Daten auszuüben. Inwieweit dies gelingt, ist ebenfalls eine Frage der **Technikgestaltung**. Digitale Systeme, deren Funktionsweise durch Hard- und Software determiniert ist, bestimmen mindestens in demselben Ausmaß wie rechtliche Vorgaben darüber, welche Einflussmöglichkeiten der Einzelne hat, wenn er sie selbst nutzt, oder ob er Objekt der Verarbeitung seiner Daten durch Dritte ist.

> Die Legitimation durch Pro-forma-Einwilligungen wird kaum mehr der Komplexität gerecht. Technische Ansätze zur Kontrolle werden notwendiger denn je.

Dabei kommt Ansätzen, die Nutzerpräferenzen bzw. rechtliche Vorgaben technisch abbilden, besondere Bedeutung zu. Angesichts der Komplexität der technischen Systeme und der tendenziell unbegrenzten Nutzungsmöglichkeiten der Daten läuft das informationelle Selbstbestimmungsrecht leer, wenn letztlich der komplette Datenverarbeitungsprozess allein auf Pro-forma-Einwilligungen beruht, die den für die Verarbeitung verantwortlichen Stellen de facto freie Hand lassen. Vor diesem Hintergrund sind technische Ansätze wie P3P (Platform for Privacy Preferences)[20] und IND²UCE[21] heute notwendiger denn je.

Bei Beachtung dieser Maximen steht der Datenschutz nicht in unauflösbarem Widerspruch zu Geschäftsmodellen, die auf der Auswertung großer Datenmengen beruhen.

Zugleich muss deutlich mehr Augenmerk auf die Verwendung der Daten gelegt werden: Weil Big-Data- und Smart-Data-Ansätze – auch bei Verwendung anonymisierter Daten – mächtige Werkzeuge zur Auswertung, Bewertung und Prognose menschlichen Verhaltens zur Verfügung stellen, bedarf es auch hierfür klarer Regeln und Grenzen, die technisch operationalisiert werden müssen. Ansonsten droht eine an vermeintlich objektiven Kriterien orientierte systematische Diskriminierung einzelner Personen und von Gruppen, die allein aufgrund ihres Datenprofils als besonders risikoträchtig angesehen werden. Dies zu verhindern ist eine Aufgabe, die weit über den am Schutz der informationellen Selbstbestimmung orientierten Datenschutz hinausgeht, die aber ohne zeitgemäße Datenschutztechniken nicht zu bewältigen sein wird.

Die Zweckbindung: Ein Überblick über die aktuelle Rechtslage und Harmonisierung durch die EU-Datenschutzgrundverordnung

Von PD Dr. Oliver Raabe, KIT - Karlsruher Institut für Technologie und FZI Forschungszentrum Informatik und Manuela Wagner, ebenfalls KIT

Das Bundesministerium für Wirtschaft und Energie widmete sich im Rahmen von „Leitplanken Digitaler Souveränität“ der Frage, ob „datenbasierte digitale Geschäftsmodelle nicht durch ein unzeitgemäßes Datensparsamkeitsdiktat verhindert werden“ und die „bisherigen Grundprinzipien des Datenschutzes wie Datensparsamkeit und Zweckbindung überprüft und durch Prinzipien der Datenvielfalt und des Datenreichtums ergänzt und ersetzt werden“ sollten.[22] Kritisch bezeichnet wurde diese Aussage als „unsachlicher Frontalangriff auf ein Kernprinzip des Datenschutzes in Deutschland und Europa“.[23] Diese Diskussion aufgreifend soll im Rahmen der Begleitforschung zum BMWi-Technologieprogramm „Smart Data – Innovationen aus Daten“ das im Kontext von Big Data umstrittene Prinzip der Zweckbindung im nationalen wie auch im europäischen Rahmen näher beleuchtet und nachvollziehbar aufbereitet werden. Gerade für die Rechtsanwender ist es lohnend, die Bedeutung sowie die Grenzen der Zweckbindung aufzuzeigen. Daneben ist bei einer Überarbeitung immer zu bedenken, dass eine Abkehr von Schutzprinzipien nur dann möglich und sinnvoll ist, wenn neue Lösungskonzepte mit einem vergleichbaren Schutzniveau erarbeitet werden.

Die Wurzeln der Zweckbindung

Die Notwendigkeit einer Kontextbestimmung der Datenverarbeitung wurde bereits im Volkszählungsurteil benannt:
*„[…] bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines **Verwendungszusammenhangs**: Erst wenn Klarheit darüber besteht, zu welchem **Zweck** Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.“*[24]

Die Begründung des Grundrechts auf informationelle Selbstbestimmung mit dem Grundsatz der Menschenwürde dürfte einen Wegfall kaum zulassen, da Art. 1 GG der Ewigkeitsgarantie des Grundgesetzes unterliegt.[25] Auch wenn Grundrechte als Abwehrrechte primär den Staat binden, entfalten sie mittelbare Drittwirkung gegenüber Privatpersonen. Als verfassungsrechtliche Schutzgebote verpflichten sie den Gesetzgeber die Rechtsordnung so auszugestalten, dass elementare Rechte auch gegen Datenverarbeitung nichtstaatlicher, privater Stellen ausreichend geschützt sind.[26] Der Schutz personenbezogener Daten hat als „Fundamental Right“ Eingang in die EU-Grundrechte-Charta gefunden. Laut Art. 8 Abs. 2 EU-GrCh dürfen Daten nur „für festgelegte Zwecke“ verarbeitet werden. Dem Grundsatz der Zweckbindung wird infolgedessen eine dem Verfassungsrang entsprechende Stellung zugesprochen.[27]

Das Gebot der Zweckbindung gilt jedoch nicht ausnahmslos. Ein Bedürfnis nach „Vorratsspeicherung“ ohne konkrete Zweckumschreibung erkennt bereits das Bundesverfassungsgericht beispielsweise bei der Datenerhebung für statistische Zwecke an.[28] Für solche Ausnahmen verlangt das Gericht im Gegenzug, dass der zweckfreien Verwendung entsprechende Schranken (meist prozedurale Anforderungen an die Datenverarbeitung) gegenüberstehen, sodass Betroffene nicht zum „bloßen Informationsobjekt“ werden.[29] Im Rahmen der aktuellen Entwicklung von Smart Data werden bisher bekannte Formen der wirtschaftlichen Tätigkeit mehr und mehr durch Geschäftsmodelle in mehrseitigen Märkten, bei denen der Konsument einer Leistung diese nicht mehr bezahlt, sondern vielmehr selbst zum Produkt wird, abgelöst.[30] Dass die Aussagen des Volkszählungsurteils auch im Zeitalter der Digitalisierung noch aktuell sind, zeigt eine europäische Studie.[31] Danach bringen Betroffene „Big Data“ ein relativ geringes Vertrauens entgegen. Obwohl die Befragten mehrheitlich Bereitschaft signalisieren, Daten für Verbesserungen in den Bereichen Gesundheit, Verkehr und Umwelt preiszugeben, lehnen sie eine pauschale Weitergabe der Daten an Dritte mehrheitlich ab. Mehr Transparenz und Kontrolle darüber, wie welche Daten genutzt werden, könnte u. a. über knappere, einfacher verständliche Information sowie über technische Möglichkeiten, Privatsphäreneinstellungen selbst vornehmen zu können, erreicht werden.[32] Zu dieser Form der individuellen digitalen Souveränität dürfte neben der Auswahl bestimmter Daten auch die Festlegung des Verwendungskontextes zählen. Ob die bestehende Rechtslage den neuen Herausforderungen gewachsen ist, wurde laut Studie uneinheitlich beantwortet: 35 % halten die existierenden Gesetze für adäquat, 38 % empfinden das Gegenteil und 27 % enthielten sich.[33]

Das Zweckbindungsprinzip soll unbeschränkten Zugriff auf personenbezogene Daten unterbinden

Konkretisierungsbedarf der Zweckbestimmung

Die notwendige Vorstufe der Zweckbindung ist die Festlegung eines konkreten Zwecks.[34] Das in Art. 6 (1) RL 95/46/EG verankerte Konzept beruht somit auf zwei Grundbausteinen:

Zweckbestimmung: Personenbezogene Daten müssen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden ...

Zweckbindung: ... und dürfen nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken nicht vereinbar ist.[35]

Ein wesentliches Kriterium für die Begrenzungswirkung der Zweckbindung ist die Frage, wie konkret ein Zweck festgelegt werden muss.[36] Je weiter ein Zweck gewählt werden darf, desto mehr Verarbeitungsvorgänge können unter diesen fallen. Art. 6 (1) (b) RL 95/46/EG (wie auch der nahezu wortgleiche Art. 5 (1) (b) DSGVO) nennt zur Zweckbestimmung die folgenden Anforderungen:

- **„festgelegt“ (specified)**
  - hinreichend konkretisiert, um den Umfang der Datenverwendung einzugrenzen.
- **„eindeutig“ (explicit)**[37]
  - unmissverständlich und unzweideutig sowie klar und deutlich zum Ausdruck kommend.
- **„rechtmäßig“ (legitimate)**
  - darf nicht im Konflikt mit der Rechtsordnung stehen und sollte die vernünftigen Erwartungen der Betroffenen berücksichtigen.[38]

Je schwerer der Eingriff in die Privatsphäre ausfällt, desto konkreter muss die Festlegung der Zweckbestimmung sein.[39] Die Zweckbestimmung stellt eine wesentliche Voraussetzung für die Anwendung der weiteren Datenschutzgrundprinzipien dar. Um sich

dem Konkretisierungsbedarf der Zweckbestimmung zu nähern, soll im Folgenden erörtert werden, welche Schlussfolgerungen aus der Interaktion der Datenschutzprinzipien bezüglich der Zweckbestimmung gezogen werden können. Diese Schlussfolgerungen sind nicht zwingend, können jedoch ein grundlegenderes Verständnis der Bedeutung des Prinzips ermöglichen.

Erforderlichkeit
Das Prinzip der Erforderlichkeit besagt, dass „die Datenverarbeitung auf den für ihren **Erhebungszweck** notwendigen Umfang zu begrenzen ist".[40] Die Zweckbestimmung muss somit konkretisieren, welche Daten der Zweckerreichung dienen und welche Daten hierfür überflüssig sind. Sobald der Zweck erfüllt ist, müssen die Daten gelöscht werden.

Zweck bestimmt
- Art und Umfang der notwendigen Datenverwendung
- Verwendungszusammenhang
- Dauer der Datenspeicherung

Datensparsamkeit
Neben der Ausrichtung der Datenverarbeitungssysteme an dem Ziel, die Datenverwendung auf ein Minimum zu beschränken, sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem **Verwendungszweck** möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.[41]

Zweck bestimmt
- Art und Weise der Datenerhebung und -verwendung
- die Erforderlichkeit der Identifizierung des Betroffenen im Einzelfall
- Eingriffsintensität und Missbrauchsgefahr

Transparenz
Bei der Datenpreisgabe haben Betroffene in der Regel eine Erwartung in Bezug darauf, in welchem Kontext und mit welcher Zielsetzung ihre Daten verarbeitet werden. Das Bundesverfassungsgericht führte die durch das Volkszählungsgesetz entstandene Beunruhigung in der Bevölkerung darauf zurück, dass „weithin Unkenntnis über Umfang und Verwendungszwecke der Befragung bestand".[42] Deshalb soll die Zweckbindung als Grundpfeiler des Datenschutzrechts das Vertrauen in eine nicht unbegrenzte, uferlose Datenverwendung schützen und Rechtssicherheit ermöglichen.[43] Datenschutzrechtliche Informationspflichten und Auskunftsrechte[44] sollen Transparenz ermöglichen. Die Zweckbenennung gegenüber dem Betroffenen bindet die verantwortliche Stelle und bildet die Grenzen der zulässigen Datenverarbeitung.[45] Die Information des Betroffenen über die verfolgten Zwecke macht die Datenverwendung durch diesen vorhersehbar und damit kontrollierbar.[46] Dementsprechend muss die Angabe des Zwecks gegenüber sämtlichen Beteiligten ausreichend Klarheit über die Zielsetzung der geplanten Datenverarbeitung sowie ein einheitliches Verständnis sicherstellen – unabhängig von ihrem kulturellen und sprachlichen Hintergrund oder Bildungsniveau.[47]

Zweck ist
- verständlich
- einschätzbar
- nachvollziehbar

Kontrolle
Ist der Zweck einer Datenverarbeitung bestimmt, jederzeit erkennbar und nachvollziehbar, können diese „zweckorientierten Schranken" als Maßstab einer Kontrolle der Datenverwendung durch den Betroffenen oder die Aufsichtsbehörden[48] herangezogen werden. Die Zweckumschreibung darf dabei nicht so allgemein gehalten sein, dass mehrere Nutzungsmöglichkeiten eröffnet werden. Zur Überprüfbarkeit sollte die Festlegung der konkreten Zwecke nachvollziehbar dokumentiert sein (beispielsweise schriftlich).[49]

Zweck
- gewährleistet Kontrollierbarkeit
- gewährleistet Abgrenzbarkeit
- ist eindeutig

Datensicherheit
Im Rahmen der Datensicherheit kann die Zweckbestimmung über den Verwendungskontext Rückschlüsse auf erforderliche Sicherheitsanforderungen erlauben. Über technische Kontrollmechanismen muss ggf. sichergestellt werden, dass die Daten nur dem durch die Zweckbestimmung eingegrenzten Personenkreis preisgegeben werden.[50] Nach Nr. 8 Anlage zu § 9 S. 1 BDSG ist „zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können".

Zweck bestimmt
- Umfang und Ausgestaltung Datensicherheitsanforderungen
- welche Daten zusammengeführt werden dürfen

Weitere Konkretisierung im einfachen Recht – ein Überblick

Das deutsche Recht enthält keine explizite Aufzählung der Datenschutzgrundprinzipien, jedoch sind die meisten in den Rechtsnormen verankert.[51] Je nachdem welche Rechtsgrundlage auf den konkreten Einzelfall anwendbar ist, finden sich Hinweise zur Zweckbestimmung im Gesetz. Aufgrund der Vielzahl bereichsspezifischer Regelungen auf Bundes- wie auf Landesebene werden an dieser Stelle nur Beispiele für die nichtöffentliche Datenverarbeitung, d. h. die Datenverarbeitung durch private Stellen, angeführt.

Bundesdatenschutzgesetz
Werden personenbezogene Daten im Rahmen der für die nichtöffentliche Datenverarbeitung zentralen Norm[52] des § 28 Abs. 1 BDSG erhoben und verarbeitet, sind bei der Erhebung die Zwecke der geplanten Datennutzung „konkret festzulegen":[53]

- Die Zweckfestlegung der Datenverwendung im Rahmen eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses folgt dem Zweck des Rechtsgeschäfts, der durch die Rechte und Pflichten aus dem Rechtsgeschäft, d. h. aus dem Vertragstext oder „dem gesamten Inhalt der jeweiligen Vereinbarung" ermittelt wird.[54] Denn personenbezogene Daten dürfen insoweit verwendet werden, als es für die Begründung, Durchführung oder Beendigung des Schuldverhältnisses erforderlich ist.[55]
- Bei einer Datenverwendung nach § 28 Abs. 1 S. 1 Nr. 2 BDSG folgt der Verarbeitungszweck aus dem „berechtigten Interesse" der verantwortlichen Stelle, das diese hinreichend konkretisieren muss.[56] Dabei kann ein beliebiges wirtschaftliches oder ideelles, von der Rechtsordnung nicht missbilligtes Interesse benannt werden, sodass der verantwortlichen Stelle eine Art „Zwecksetzungskompetenz" zukommt.[57] In der Literatur wird eine restriktive Auslegung befürwortet, um keine Legitimationsgrundlage für Zweckentfremdungen zu schaffen.[58] Es sollte ein konkreter Nutzungszweck feststehen, im Gegensatz zu noch vagen allgemeinen Interessen, die zu einem späteren Zeitpunkt realisiert werden könnten.[59] In der Praxis ergibt sich die Schwierigkeit zu entscheiden, wann dies der Fall ist und ob Unterschiede zwischen „Zweck" und „Interesse" bestehen können bzw. ob Letzteres ggf. mehrere Verwendungszwecke umfassen könnte.
- Bei allgemein zugänglichen Daten besteht eine größere Verwendungsfreiheit: Sofern keine die berechtigten Interessen der verantwortlichen Stelle offensichtlich überwiegenden schutzwürdigen Belange der Betroffenen bestehen, darf die verantwortliche Stelle Umfang und Zweck der Verwendung grundsätzlich frei bestimmen.[60]

Telemediengesetz
Im Telemedienrecht wird mit der Einteilung in Bestands- und Nutzungsdaten bereits eine Zielrichtung zulässiger Verwendung vorgegeben:

Bestandsdaten sind erforderlich für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses zwischen Diensteanbieter und Nutzer über die Nutzung von Telemedien.

Nutzungsdaten sind erforderlich, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen.[61]

Zulässigkeit zweckändernder Sekundärnutzung

Obwohl die Zweckbindung einen Grundpfeiler des Datenschutzrechts bildet, sollten Ausnahmeregelungen bestehen, wenn die Weiterverwendung bereits vorhandener personenbezogener Daten einen gesamtgesellschaftlich erwünschten Mehrwert stiftet und schutzwürdige Interessen Betroffener kaum tangiert sind.

Die Datenschutzgrundverordnung
Die am 25.05.2016 in Kraft getretene EU-Datenschutzgrundverordnung (DSGVO) wird ab dem 25.05.2018 unmittelbar anzuwenden sein und damit sowohl die bislang den Rahmen vorgebende Richtlinie 95/46/EG als auch große Teile des BDSG und TMG ablösen.

Sekundärnutzung nach Zweckvereinbarkeitsprüfung
Die Zweckbindung dürfte in der kommenden DSGVO keine wesentlichen Neuerungen gegenüber der RL 95/46/EG erfahren. Die Formulierung der Grundsätze zur Zweckbindung und Datenminimierung sind nahezu wortgleich.[62] Bereits heute wird die Formulierung **„nicht vereinbar“** dahingehend verstanden, die Weiterverwendung zu neuen Zwecken nicht gänzlich auszuschließen, sondern einen gewissen Grad an zusätzlicher Nutzung innerhalb sorgfältig ausbalancierter Schranken zu ermöglichen.[63] In der DSGVO werden in Art. 6 (4) die Kriterien genannt, die bei der Beurteilung einer Zweckvereinbarkeit zu berücksichtigen sind. Diese decken sich stark mit den zur Richtlinie ermittelten Merkmalen:[64]

- Verbindung zwischen ursprünglichen und neuen Zwecken
- Kontext der Datenerhebung
- vernünftige Erwartung der Betroffenen
- Art der Personenbezogenen Daten
- Auswirkungen und mögliche Folgen der Weiterverwendung für die Betroffenen
- Schutzmaßnahmen und Garantien (z. B. Verschlüsselung, Pseudonymisierung)

Die Umsetzung der Richtlinie erfolgte in den Mitgliedsstaaten unterschiedlich. Obwohl einige Regelungen einen vergleichbaren Wortlaut verwenden, führte ein unterschiedliches Verständnis der Reichweite und Flexibilität zu uneinheitlicher Anwendung.[65] Die unmittelbar anwendbare DSGVO dürfte diesen Harmonierungsdefiziten auch dadurch entgegentreten, dass sie die oben genannten Merkmale gesetzlich statuiert. Allerdings wird es klarer Auslegungs- und Abwägungsmaßstäbe für die einzelnen Kriterien bedürfen, um unterschiedliche Ergebnisse je nach Interpretation und Gewichtung und damit Rechtsunsicherheit sowohl für verarbeitende Stellen als auch für Betroffene zu vermeiden.

Legitimation zur Zweckänderung
Das Verständnis der Zweckbindung in Deutschland geht bislang davon aus, dass die Zweckbestimmung die verantwortliche Stelle bindet und für eine Zweckänderung eine gesonderte Berechtigung (Legitimation) benötigt wird.[66] Diese Legitimation kann über eine Einwilligung erfolgen, oder über eine gesetzliche Erlaubnisnorm. Diese Systematik gilt für den öffentlichen wie für den privaten Sektor gleichermaßen. Allerdings sehen die Erlaubnisnormen für den privaten Sektor in

Bezug auf eine Zweckänderung grundsätzlich größere Spielräume als für den öffentlichen Sektor vor.

Bundesdatenschutzgesetz
Das BDSG enthält dabei Fälle strikter Zweckbindung wie auch Legitimationsnormen zur Zweckänderung, die die Zulässigkeit neben einzelnen Tatbestandsvoraussetzungen auch vom berechtigten Interesse der verantwortlichen Stelle im Widerstreit mit dem schutzwürdigen Interesse des Betroffenen abhängig machen.[67] Bei der Interessenabwägung der für die nichtöffentliche Datenverarbeitung zentralen Norm § 28 Abs. 2 BDSG ist je nach einschlägigen Unterfällen eine unterschiedliche Gewichtung der widerstreitenden Interessen gefordert. Die Spannbreite der gewählten Formulierungen rangiert von der Existenz eines schutzwürdigen Betroffeneninteresses bis hin zum „offensichtlichen Überwiegen“ oder „erheblichen Überwiegen“ der entgegenstehenden Interessen. Selbst wenn im Einzelfall eine Abwägung widerstreitender Interessen unterbleiben kann,[68] muss bei der praktischen Anwendung zunächst ermittelt werden, welche Betroffeneninteressen als „berechtigt“ und „schutzwürdig“ berücksichtigungsfähig sind.[69] Welche Kriterien für diese Wertung sowie die anschließende Bestimmung des Ausgleichs heranzuziehen sind, wird vom Gesetz nicht vorgegeben. Es wird konstatiert, dass für die Güterabwägung kein klarer verallgemeinerungsfähiger Abwägungsmaßstab besteht, sodass lediglich einzelfallbezogene Erkenntnisse vorliegen.[70] In der Literatur werden folgende Punkte genannt:[71]

- Art und Sensibilität der Daten
- Intensität des Eingriffs in Persönlichkeitssphären
- wirtschaftliche Betroffeneninteressen
- negative Folgen für die Freiheit der privaten, sozialen und beruflichen Lebensgestaltung
- Minderjährigkeit
- Anonymisierung

Telemedienrecht
Die Zweckbindung ist in § 12 Abs. 2 TMG mit der Einschränkung normiert, dass sich gesetzliche Legitimationen zweckändernder Datenverwendung auf Telemedien beziehen müssen. §§ 14, 15 TMG legitimieren die Weiterverwendung zu konkret benannten Zwecken.[72] Weitere sich auf Telemedien beziehende Erlaubnisnormen bestehen derzeit nicht.[73]

Unterschiede und Konsequenzen?
Somit zeigen sich schon heute wesentliche Unterschiede zwischen dem deutschen und dem europäischen Konzept. Im nationalen Recht legitimieren einschlägige Erlaubnisnormen teils nur für vorgegebene neue Zwecke (z. B. Forschung, Werbezwecke, Strafverfolgung) und teils auch nur für bestimmte Verwendungsformen (z. B. Übermittlung und Nutzung).[74] Mehr Flexibilität für neuartige Zwecke eröffnen Normen, die eine Interessenabwägung vorsehen.[75] Hiermit vergleichbar könnte die Vereinbarkeitsprüfung des europäischen Zweckbindungskonzepts sein, die die Auswahl eines neuen Zwecks der verantwortlichen Stelle insoweit überlässt, als nach Prüfung der vorgegebenen Abwägungskriterien die Vereinbarkeit mit dem ursprünglichen Zweck festgestellt werden kann.

Reichweite und Auswirkungen des tatsächlichen Unterschieds der Konzeptionen auf Anwendungsebene werden sich erst durch die endgültige Umsetzung und Interpretation manifestieren. Einen Hinweis geben die Erwägungen zur aktuellen Richtlinie. So kann bereits heute eruiert werden, inwieweit bei der Vereinbarkeitsprüfung andersgeartete Abwägungskriterien gegenüber vergleichbaren Normen mit Interessenabwägung herangezogen werden müssen: Ein maßgebliches Merkmal ist das **Verhältnis** des ursprünglichen Zwecks zum neuen Zweck: War dieser bereits implizit im Ursprungszweck enthalten, der logische nächste Schritt oder existiert kein Zusammenhang der Zwecke?[76] Eine Inkompatibilität liegt nahe, wenn der neue Zweck nach dem Erhebungskontext **unerwartet** oder **überraschend** erscheint. Dabei sol-

len auch das **Kräfteverhältnis** zwischen Betroffenem und verantwortlicher Stelle sowie die **Transparenz** und **Datensensitivität** berücksichtigt werden.[77] Die Ermittlung möglicher positiver und negativer Folgen für den Betroffenen umfasst emotionale Einwirkungen, wie beispielsweise durch Kontrollverlust verursachte Angst. Je **negativer**, **unklarer** oder **unkontrollierbarer** die zu befürchtenden Auswirkungen der Datenverwendung auf den Betroffenen ausfallen können, desto unwahrscheinlicher ist eine Vereinbarkeit. Als Kompensator können technisch-organisatorische **Schutzmaßnahmen** (beispielsweise teilweise oder vollständige Anonymisierung, Pseudonymisierung, Aggregation) oder Einwilligungsmöglichkeiten (Opt-in oder Opt-out) dienen.[78] Jedoch soll eine Einwilligung nur dann die zweckändernde Datenverwendung legitimieren, wenn die Anforderungen der Vereinbarkeitsprüfung **kumulativ** vorliegen.[79]

Zum BDSG wird hingegen der Standpunkt vertreten, dass die Interessenabwägung im Rahmen einer Zweckänderung im Prinzip nur eine erneute Prüfungspflicht der Betroffeneninteressen in Relation zum neuen Zweck mit sich bringt.[80] Dementsprechend fehlt auch hier ein klarer Abwägungsmaßstab.

Im Ergebnis dürfte die kommende Rechtslage einen stärkeren Vergleich des ursprünglichen mit dem neuen Zweck gebieten. Grundlegend andere Zwecke dürften dann nur unter Verwendung zusätzlicher Schutzmaßnahmen verfolgt werden.

Fazit und Ausblick

Die Intentionen des datenschutzrechtlichen Rahmens, zu dem das Prinzip der Zweckbindung zählt, sind keinesfalls „digitalisierungsfeindlich".[81] Die Interessen der Unternehmen in Bezug auf umfassende Datenverarbeitung sowie der Bürger in Bezug auf umfassenden Schutz müssen sich nicht zwangsläufig widersprechen. Wenn effektiv durchsetzbare Schutz- und Kontrollmechanismen Bedrohungen wie informationelle Ausforschung, Manipulation oder Diskriminierung ausschließen sowie Rechtssicherheit schaffen, kann damit das Vertrauen der Bürger in die Verwendung digitaler Technologien gestärkt werden. Die Bereitschaft, die eigene Identität sowie die Privatsphäre betreffende Informationen wahrheitsgemäß anzugeben, ist auch eine durchaus nicht zu unterschätzende Frage der Datenqualität. Laut einer Studie haben knapp mehr als die Hälfte der Befragten bei der Datenabfrage schon falsche Angaben gemacht.[82] Vertrauen in eine rechtmäßige und verantwortungsbewusste Datenverwendung kann geschaffen werden, wenn die Art und Weise sowie Umfang und Dauer der Datenverwendung vorab festgelegt sind und der Betroffene darüber informiert wird. Die negative Konsequenz fehlender Vertrauensmechanismen ist die Ablehnung neuer Phänomene wie Big Data in der Bevölkerung.[83] In diesem Sinne konstatieren die BMWi-Leitplanken: „Stärkung der Transparenzprinzipien und Verbesserung der Kontrolle und Sanktionsmechanismen bei Verstößen gegen Datenschutzrecht sind Wege zu einer innovativen Datenpolitik."[84] Hierfür bedarf es objektiver Kriterien, die einer Überprüfbarkeit und Sanktionierbarkeit zugänglich sind. Im Prinzip erfüllt dieses Kriterium die Zweckbindung in Verbindung mit der Reduzierung des Datenumgangs auf das für den jeweiligen Zweck erforderliche Maß. Diese Anforderungen sollen beim Betroffenen Transparenz erzeugen, da der Kontext der Datenverarbeitung im Vorfeld (zum Zeitpunkt der Datenerhebung) eingeschätzt werden kann. Die Prinzipien der Transparenz und Kontrolle bauen auf dem Verarbeitungskontext auf. Die Effektivität der damit verbundenen Schutzanforderungen steht und fällt allerdings mit dem Vorhandensein eines Maßstabs, anhand dessen die Verarbeiter personenbezogener Daten genauso wie die Betroffenen beurteilen können, wie konkret die Zwecke anzugeben sind.

Zweckbindung und „Informed Consent" für wissenschaftliche Forschungsvorhaben

Von Ass. jur. Valérie Gläß LL.M. und Dr. Johannes Drepper, TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.

Im Rahmen von **wissenschaftlichen Forschungsvorhaben** kommt der Verarbeitung personenbezogener Daten eine große Bedeutung zu. Denn für eine Vielzahl von Forschungsfragen werden verschiedene Gesundheitsdaten erhoben, genutzt und gespeichert, die häufig auch nicht ausschließlich anonymisiert verarbeitet werden können. Anwendungsfälle finden sich z. B. in der klinischen Forschung zur Feststellung der Wirksamkeit und Sicherheit neuer Medikamente oder auch im Rahmen von medizinischen Registern, in denen Daten tendenziell langfristig und auch für künftige Fragestellungen nutzbar aufgehoben werden.

Die zulässige **Verarbeitung von Gesundheitsdaten** basiert nach den allgemeinen Grundsätzen des Datenschutzrechts entweder auf einer gesetzlichen Grundlage oder einer **Einwilligung** des Patienten oder Probanden. In der Einwilligungserklärung sind die zu nutzenden (Gesundheits-)Daten und die anvisierte spezifische Form der Datennutzung konkret zu bezeichnen. Daher wird diese Form der Einwilligung auch als **„informed consent"** (informierte Einwilligung) bezeichnet.

Die vom Patienten oder Probanden erteilte Einwilligung geht auf das **Grundrecht auf informationelle Selbstbestimmung** zurück, das wiederum aus dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG)[85] abgeleitet wird. Danach hat der Einzelne grundsätzlich das Recht, selbst über die Weitergabe und Nutzung seiner personenbezogenen Daten bestimmen zu können. Die Einwilligung ermöglicht es dem Einzelnen, in Fällen, in denen keine gesetzliche Grundlage die Datennutzung vorsieht, darüber zu entscheiden, ob, wie lange und für welche Zwecke sie genutzt werden.

> Wissenschaftlich zu erforschende Fragestellungen können im Vorfeld eines Forschungsvorhabens oft nicht abschließend definiert werden, Einwilligungserklärungen dürfen aber nicht zu unbestimmt formuliert sein.

Diese Festlegung auf einen oder mehrere bestimmte Zwecke wird als **„Zweckbindungsgrundsatz"** (vgl. vorheriges Kapitel) bezeichnet, der auch für Einwilligungserklärungen gilt. Eine vorherige Festlegung auf einen oder mehrere spezifische Zwecke kann jedoch gerade im Bereich der medizinischen Forschung problematisch sein. Nennenswert sind hier etwa Fragestellungen der **Versorgungsforschung**, in denen die tatsächliche medizinische Gesundheitsversorgung von Patienten auf mögliche Defizite untersucht wird. Die wissenschaftlichen Fragestellungen entwickeln sich hier häufig in Abhängigkeit von bestimmten Erkrankungen, dem regionalen Versorgungsangebot und dem Verhalten der Patienten. Sie können daher häufig nicht im Vorfeld abschließend definiert werden, weshalb solchen Einwilligungserklärungen das Risiko anhaftet, dass sie zu unbestimmt formuliert sind.

Die Zweckbindung im Rahmen des „broad consents"

Aufgrund der oben beschriebenen Rechtsrisiken hat sich in Deutschland bereits seit einigen Jahren für verschiedene Forschungsbereiche ein Vorgehen auf Grundlage des **„broad consents" („breite Einwilligung")** etabliert. 2003 hatte die TMF im Rahmen ihrer generischen Datenschutzkonzepte[86] erstmals in Deutschland das Prinzip einer weniger engen Zweckbeschreibung mit einem **zweistufigen Bewilligungsprinzip**[87] entwickelt und diese mit entsprechend aufwändigeren technischen und organisatorischen Schutzmechanismen verknüpft. Diese Lösung wurde mit den Datenschützern abgestimmt. Im Jahr 2006 wurden die Lösungsmodelle für Biobanken und im Jahr 2014 die Lösungsmodelle für die Verknüpfung unterschiedlicher Forschungsbereiche weiterentwickelt.

Einwilligungsmanagement für Gesundheitsdaten

Nach heutiger Rechtslage reicht es daher aus, wenn Einwilligungserklärungen bei epidemiologischen Datenbanken[88] oder Biobanken allgemeine Ausführungen zu den geplanten Nutzungen enthalten.

So findet sich z. B. in der Einwilligungserklärung zur Teilnahme an der Nationalen Kohorte[89], einer Langzeitbevölkerungsstudie, die von einem Netzwerk deutscher Forschungseinrichtungen (Helmholtz-Gemeinschaft, Universitäten, Leibniz-Gemeinschaft) organisiert und durchgeführt wird, ein Passus, wonach die Daten zur Erforschung **„häufiger Krankheiten“** insbesondere zur Untersuchung von Ursachen und Risikofaktoren von Erkrankungen und zur Entwicklung wirksamer Diagnose-, Präventions- und Behandlungsmöglichkeiten verwendet werden dürfen.

Der Arbeitskreis „Medizinische Ethikkommissionen in der Bundesrepublik Deutschland e. V.“, in dem fast alle in Deutschland tätigen Ethikkommissionen zusammenarbeiten, hat Mustereinwilligungserklärungen[90] für deutsche Biobanken erarbeitet. Dort ist z. B. folgende „breite“ Datennutzung für wissenschaftliche Forschungen vorgesehen: *„Die von Ihnen zur Verfügung gestellten Biomaterialien und Daten werden **ausschließlich für die medizinische Forschung** bereitgestellt. Sie sollen im Sinne eines breiten Nutzens für die Allgemeinheit für viele verschiedene medizinische Forschungszwecke verwendet werden. Zum derzeitigen Zeitpunkt können noch nicht alle zukünftigen medizinischen Forschungsziele beschrieben werden. Diese können sich sowohl auf bestimmte Krankheitsgebiete (z. B. Krebsleiden, Herz-Kreislauf-Erkrankungen, Erkrankungen des Gehirns) als auch auf heute zum Teil noch unbekannte Krankheiten und genetische Defekte beziehen. Es kann also sein, dass Ihre Proben und Daten auch für medizinische Forschungsfragen verwendet werden, die wir heute noch nicht absehen können.“*

Auswirkungen der EU-Datenschutzgrundverordnung

Die am 25.05.2016 in Kraft getretene EU-Datenschutzgrundverordnung wird in Deutschland, jedenfalls für den überwiegenden Regelungsbereich, ab dem 25.05.2018 unmittelbare Rechtswirkung entfalten und damit den Rechtsrahmen im Datenschutz vorgeben. Die bislang geltende europäische Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ wird durch die EU-Verordnung abgelöst. Die sie umsetzenden Gesetze, wie das BDSG und die Landesdatenschutzgesetze, werden im Hinblick auf die EU-Datenschutzgrundverordnung derzeit entsprechend angepasst.

Indes werden die meisten der bisher geltenden Grundsätze im Datenschutzrecht für den Bereich der wissenschaftlichen Forschung durch die EU-Datenschutzgrundverordnung nicht berührt.

Die Einwilligung zur Datennutzung in der wissenschaftlichen Forschung

Die EU-Datenschutzgrundverordnung enthält Vorschriften zur Einwilligung, die den bisherigen ähneln. Für die Nutzung von besonders schutzwürdigen Gesundheitsdaten ist z. B. in Art. 9 Abs. 2 a) vorgesehen, dass die Einwilligungserklärung ausdrücklich die Verarbeitung „für einen oder mehrere Zwecke“ nennt.[91] Die EU-Datenschutzgrundverordnung geht wie das bisher geltende Datenschutzrecht vom **Grundsatz der informierten Einwilligung** aus.

Broad consent für die Datennutzung in der wissenschaftlichen Forschung

Im Hinblick auf den bereits erwähnten **„broad consent“** ist der **Erwägungsgrund 33** für Einwilligungserklärungen besonders interessant: „Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. **Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht.** Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.“

Wenn die Begrenzung der für die Forschung notwendigen Zwecke vor der Datenerhebung nicht möglich ist, erlaubt der Erwägungsgrund, Einwilligungen für bestimmte Bereiche der wissenschaftlichen Forschung abzugeben, wenn die ethischen Standards der wissenschaftlichen Forschung eingehalten werden. Es wird präzisiert, dass in dem vom verfolgten Forschungszweck zugelassenen Maße den Betroffenen die Möglichkeit eingeräumt werden soll, Einwilligungen auch für bestimmte Bereiche der Forschung oder Teile von Forschungsprojekten zu erteilen.

Aus der Kombination der Vorschrift Art. 9 Abs. 2 a) mit dem Erwägungsgrund 33 lässt sich daher ableiten, dass bei Forschungsvorhaben eine breitere Zweckbestimmung zulässig ist.[92] Allerdings kann daraus auch hergeleitet werden, dass in diesen Fällen **gestufte Einwilligungen** (für die verschiedenen Bereiche) – wenn möglich – vorzusehen sind. Dennoch kommt dem Erwägungsgrund eine wichtige Bedeutung zu, da er den in **Deutschland praktizierten „broad consent“ als zulässige Form der Einwilligung nunmehr erstmals übergreifend regelt.**

- ☒ Ich willige in die Teilnahme an Studie XY ein.
- ☒ Ich willige darüber hinaus ein, dass meine Daten nach Abschluss der Studie für Forschungsprojekte zum Krankheitsgebiet XY genutzt werden.
- ☒ Ich willige darüber hinaus ein, dass meine Daten auch für weitere medizinische Forschungsprojekte verwendet werden.

Beispiel einer gestuften Einwilligung

Weiterverarbeitung von Gesundheitsdaten für die wissenschaftliche Forschung

Auch der bereits bekannte **Zweckbindungsgrundsatz** findet sich in Art. 5 Abs. 1 b)[93] der EU-Datenschutzgrundverordnung wieder. Ebenso findet sich darin eine Regelung, die die Weiterverarbeitung von Daten für wissenschaftliche Forschungsvorhaben nach Art. 89 Abs. 1 mit dem ursprünglichen Erhebungszweck für **vereinbar** erklärt. Hinter dieser Vorschrift steht der Grundsatz, dass die Verarbeitung von *„Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, (…) nur zulässig sein (sollte), wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. (….) Die Weiterverarbeitung für (…) wissenschaftliche Forschungszwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten“.*[94]

> Personenbezogene Daten dürfen für neue Forschungszwecke genutzt werden, wenn diese mit den ursprünglichen Zwecken der Datenerhebung vereinbar sind und eine Rechtsgrundlage besteht.

Nach Art. 5 Abs. 1 b) und dem Erwägungsgrund 50 soll die Weiterverarbeitung für wissenschaftliche Forschungsvorhaben (nach Art. 89 Abs. 1)[95] mit der ursprünglichen Datenerhebung daher vereinbar sein.

Trotz des Wortlauts des Art. 5 Abs. 1 b) ist derzeit noch nicht geklärt, ob für die **sekundäre Nutzung** von Gesundheitsdaten als privilegierte Zweckänderung eine **Rechtsgrundlage** erforderlich ist.

In der EU-Datenschutzrichtlinie 95/46/EG war eine Vorschrift[96] enthalten, die die Weiterverarbeitung für wissenschaftliche Forschungsvorhaben im Allgemeinen als vereinbar mit dem ursprünglichen Zweck ansah, wenn die Mitgliedsstaaten geeignete Garantien regelten. Die Artikel-29-Datenschutzgruppe der Europäischen Kommission hatte die Vorschrift so interpretiert, dass die Grundlage für die sekundäre Datennutzung für Forschungszwecke im mitgliedschaftlichen Recht ausgestaltet werden müsse[97] (gesetzliche Grundlage oder Einwilligung). Derzeit ist es noch offen, ob diese bisherige Auslegung der Artikel-29-Datenschutzgruppe auch für Art. 5 Abs. 1 b) EU-Datenschutzgrundverordnung gelten wird.

Zur Frage, ob eine Rechtsgrundlage für die Weiterverarbeitung der Gesundheitsdaten notwendig ist, enthielt Art. 6 Abs. 1 b) der Datenschutzrichtlinie eine entsprechende Anordnung. Art. 5 Abs. 1 b) der Datenschutzgrundverordnung enthält hingegen keinen solchen Hinweis. Der Wortlaut des Erwägungsgrundes 50 (Satz 2), der eine Weiterverarbeitung ohne Rechtsgrundlage statuiert, wenn die Weiterverarbeitung mit dem ursprünglichen Erhebungszweck vereinbar ist, enthält wohl keine eindeutige Lösung. Denn ein Blick auf die Entstehungsgeschichte zeigt, dass dieser Satz 2 als Überrest des Ansatzes des Rates im Trilog-Verfahren zu werten ist.[98] Laut der Auffassung des Europäischen Parlaments, die sich letztlich durchsetzte, sollte es bei der vorherigen Praxis bleiben, die eine Rechtsgrundlage für die Weiterverarbeitung erfordert. Dies sei aufgrund der Wirkung der europäischen Grundrechte erforderlich.

Da Art. 5 Abs. 1 b) der EU-Datenschutzgrundverordnung ein wissenschaftliches Vorhaben nach Art. 89 Abs. 1 der Verordnung voraussetzt, der eine Rechtsgrundlage erfordert, ist im Lichte der geschichtlichen Entstehung daher nicht von einer Abkehr von den bisherigen Grundsätzen auszugehen. Um Rechtssicherheit für den Bereich der wissenschaftlichen Forschung zu schaffen, wäre eine einheitliche Interpretation des Art. 5 b) Abs. 1 bei der Nutzung von Gesundheitsdaten und des Erwägungsgrundes 50 wünschenswert.

Medizinische Forschung und der Datenschutz: Plädoyer für ein Bund-Länder-Forschungsgremium

Von Thilo Weichert, Netzwerk Datenschutzexperte

Rahmenbedingungen

Gesundheitsdaten fallen heute nicht nur im Krankenhaus und in der Arztpraxis, sondern **bei vielen Stellen** an. Medizinische Leistungen erbringen weitere Heilberufe, von Psychologen und Apothekern bis hin zu Heil- und Pflegediensten. Diese nehmen für die finanzielle, organisatorische und informationstechnische Abwicklung Dienstleister sowie weitere Institutionen in Anspruch, sodass Gesundheitsdaten in öffentlichen und geschlossenen Netzen, Rechenzentren und Serviceeinrichtungen verarbeitet werden. Systembedingt müssen Gesundheitsdaten in Kassenärztlichen Vereinigungen, bei Krankenkassen und dem Medizinischen Dienst, aber auch bei privaten Abrechnungsprüfern und Versicherungen verarbeitet werden. Zunehmend generieren Betroffene über Quantified Self – Selbstüberwachung u. a. von Gesundheitsfunktionen insbesondere über sogenannte Wearables – körperbezogene Daten und gelangen so in soziale Netzwerke und zu Internet-Dienstleistern. Entsprechendes gilt bei der Inanspruchnahme von netzgestützten Beratungsdiensten und Suchmaschinen.

> Obwohl die Fragmentierung des Rechtsrahmens die praktische Umsetzung erschwert, lassen weitreichende Öffnungsklauseln der Datenschutzgrundverordnung kaum eine Harmonisierung erwarten.

Chancen und Risiken

Die rasante quantitative und qualitative Zunahme von digital verfügbaren Gesundheitsdaten ist eine Herausforderung und eine große Chance für die medizinische Forschung. Dieser eröffnen sich mit den vorhandenen Daten völlig neue Beschaffungs- und Auswertungsmöglichkeiten, mit denen **neue medizinische Erkenntnisse**, neue Behandlungsmöglichkeiten sowie Verbesserungen bei Abrechnung, Kontrolle und Organisation von Gesundheitsleistungen erreicht werden können. Zusätzliche Erkenntnisquellen zu Dispositionen, Erkrankungen und Behandlungsmöglichkeiten entwickeln sich im Bereich der der Bio- und speziell der Gentechnik.

Diesen Chancen stehen Risiken für die Betroffenen gegenüber: Bei **Verletzung der Vertraulichkeit** in der Arzt- bzw. Helfer-Betroffenen-Beziehung besteht die Gefahr, dass sich Hilfsbedürftige Helfenden nicht mehr oder nicht vollständig öffnen, was Voraussetzung für eine umfassende und vertrauensvolle Hilfe ist. Diese grundlegende Erkenntnis fand vor über 2000 Jahren schon Eingang in den Eid des Hippokrates und behielt im medizinischen Standesrecht sowie über Sanktionsregelungen – insbesondere den § 203 StGB – bis heute Gültigkeit.

Moderne Formen der Auswertung von Gesundheitsdaten provozieren **weitere Gefahren**. Sie können die Wahlfreiheit und damit die medizinische Selbstbestimmung einschränken und zur medizinischen Diskriminierung, etwa beim Versicherungsschutz oder bei der konkreten Behandlung, beitragen. Durch Beeinträchtigung der Datenintegrität oder durch fehlerhafte Programmierung können Gesundheitsmanipulationen erfolgen, mit möglicherweise gravierenden körperlichen und seelischen, ja tödlichen Folgen. Nicht zuletzt: Gesundheitsdaten sind ein weites Feld für kommerzielle Beeinflussung und Ausbeutung – vom Bereich der Werbung bis hin zum Verkauf von Pharmazeutika und gesundheitsbezogenen Dienstleistungen.

Rechtlicher Rahmen

Angesichts dieser Umstände sind die Gesellschaft, der Staat und insbesondere der Gesetzgeber gefordert, Rahmenbedingungen zu schaffen, mit denen die neuen Möglichkeiten der Nutzung von Gesundheitsdaten erschlossen und zugleich die damit verbundenen Risiken gebannt werden. Dabei ist der bestehende

verfassungsrechtliche Rahmen – national wie europäisch – zu beachten, der den Schutz der Gesundheit (Art. 2 Abs. 2 GG, Art. 3, 35 GRCh) und des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 GRCh) verspricht, zu dem aber auch die Berufsfreiheit (Art. 12 GG, Art. 15 GRCh) der medizinischen Leistungserbringer und im Hinblick auf die medizinische Forschung die Wissenschaftsfreiheit (Art. 5 Abs. 3 GG, Art. 13 GRCh) gehören. Flankierende Verfassungsgrundsätze sind das Sozialstaats- (Art. 20 Abs. 1 GG, Art. 34, 35 GRCh) und das Rechtsstaatsprinzip (Art. 19 Abs. 4 GG, Art. 47 GRCh), der Gleichheitsgrundsatz und die damit verbundenen Diskriminierungsverbote (Art. 3 GG, Art. 20 ff. GRCh) sowie der Verbraucherschutz (Art. 38 GRCh).

Die Datenschutzgrundverordnung sollte als Anlass genutzt werden, die bisher verstreuten Normen zugunsten eines einheitlichen Regelungsregimes für Forschung zu überarbeiten.

Angesichts dieses einheitlichen und modernen allgemeinen Rahmens ist es verblüffend, wie zersplittert und antiquiert die **einfachgesetzlichen Regelungen** zur Nutzung von Gesundheitsdaten für Forschungszwecke sind. Diese finden sich in allgemeinen Datenschutzgesetzen des Bundes und der Länder (vgl. §§ 40, 28 Abs. 6 Nr. 4, 14 Abs. 2 Nr. 9, 4a Abs. 3 BDSG, § 22 LDSG SH), oft ohne auf die Spezifik von Gesundheitsdaten als besondere sensitive Kategorie (vgl. § 3 Abs. 9 BDSG), die zudem regelmäßig besonderen Berufsgeheimnissen unterliegt, einzugehen. Die schon stark verstreuten allgemeinen Forschungsklauseln werden durch spezifische Regelungen in Spezialgesetzen ergänzt (statt vieler u. a. § 75 SGB X, § 287 SGB V, § 98 SGB XI, § 119 SGB XII), was die Überschaubarkeit für alle Beteiligten weiter erschwert und die praktische Umsetzung behindert.

Dieses Regelungschaos könnte nun Dank einheitlicher europäischer Vorgaben beseitigt werden. Mit der seit dem 25.05.2016 in Kraft befindlichen und zwei Jahre später direkt anwendbaren **Europäischen Datenschutzgrundverordnung** (DSGVO) wird ein supranationaler Rechtsrahmen geschaffen, in dem Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) einen höheren Schutz genießen (Art. 9 DSGVO) und insofern in Bezug auf die Nutzung für wissenschaftliche Forschungszwecke „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorschreiben (Art. 9 Abs. 2 lit. j, 89 DSGVO). Diese Hoffnung wird aber dadurch getrübt, dass durch entsprechende Öffnungsklauseln die Konkretisierung der „Maßnahmen“ den nationalen Gesetzgebern überlassen und zugleich klargestellt wird, dass die (nationalen) Regelungen zum Berufsgeheimnisschutz unberührt bleiben sollen (Art. 9 Abs. 3 und 4, 90 DSGVO).

Die damit verbundene schlechte Botschaft ist, dass alles beim Alten bleiben kann. Tatsächlich enthält ein erster Referentenentwurf für ein Allgemeines Bundesdatenschutzgesetz (ABDSG) vom August 2016 zu der Thematik in § 34 eine Regelung, die lediglich die allgemeinen Normen der DSGVO paraphrasiert und in § 36 Berufsgeheimnisträger weiter für verpflichtet erklärt. Rechtssicherheit und Klarheit gehen anders. Die gute Botschaft ist, dass der **Gesetzgeber in Deutschland** wegen der DSGVO in jedem Fall tätig werden muss und deshalb die Forschungsregelungen zumindest im allgemeinen Datenschutzrecht auf dem Prüfstand stehen. Dies ist die Gelegenheit, den Gesetzgeber dazu zu veranlassen, endlich tätig zu werden. Es ist nun nicht so, dass die Erwartungen an den Gesetzgeber in Sachen medizinischer Forschung nicht schon seit Jahren bekannt wären. Jedenfalls sind die diesbezüglichen Forderungen lauter geworden und erstrecken sich inzwischen nicht nur auf die Forschenden selbst, sondern schließen auch Datenschützer mit ein.

Grundsätzliche Erwägungen

Im Folgenden sollen **Regelungsvorschläge** gemacht werden, mit denen der Vertraulichkeits- und Persönlichkeitsschutz bzw. generell der Schutz der Freiheiten der betroffenen Menschen gewährleistet und zugleich die Forschungspotenziale so weit wie möglich ausgeschöpft werden können.

Bei den zu erarbeitenden Regelungen sind folgende **Umstände** relevant:

1. Angesichts der Möglichkeiten der Datenerfassung und-auswertung mit sogenannten Big-Data-Instrumenten bestehen nur noch geringe technische Einschränkungen in Bezug auf Umfang, Detaillierungsgrad, Raum und Zeit. Dies hat auch zur Folge, dass die faktischen Möglichkeiten der Reidentifizierung von scheinbar anonymisierten Datensätzen fast unbegrenzt sind.
2. Angesichts der technischen Möglichkeiten besteht mit Hilfe der Vergabe von Pseudonymen und dem Einsatz von Kryptografie die Möglichkeit, Datensätze so mit Attributen zu versehen, dass deren Verarbeitung auf bestimmte Stellen und für bestimmte Zwecke begrenzt werden kann.
3. Moderne Forschungsansätze beschränken sich heute oft nicht mehr auf eine Datenquelle, sondern zielen darauf ab, räumlich, zeitlich und von der Zweckgebundenheit her auseinanderliegende Datenquellen für eine gemeinsame Auswertung z usammenzuführen.
4. Forschung findet heute nicht mehr abgeschottet in separaten Einheiten statt, sondern erfolgt international, disziplinübergreifend und oft auch ohne fest definierte zeitliche Grenzen.
5. Moderne Forschung setzt grundsätzlich den Einsatz von Experten aus unterschiedlichen Bereichen und Disziplinen voraus. So bedingt medizinische Forschung i. d. R. den Einsatz von biotechnologischem, statistischem und informationstechnischem Wissen.

Bisher bestehen in Deutschland Forschungsregelungen auf Landes- wie auf Bundesebene in allgemeinen und spezifischen Datenschutzgesetzen. Diese **Rechtszersplitterung** muss zugunsten eines möglichst einheitlichen Regelungsregimes beendet werden. Aus dem oben Gesagten ergibt sich, dass eine zukunftsweisende Forschungsregulierung nicht mehr – wie bisher – bereichsspezifisch geregelt sein kann, sondern dass vielmehr allgemeine Regelungen nötig sind, die zugleich in der Lage sind, die ursprünglichen Zwecke der Erhebung und Verarbeitung bei der weiteren wissenschaftlichen Nutzung zu gewährleisten.

Die **Gesetzgebungsbefugnis** im Bereich der Forschung folgt den jeweiligen geregelten Rechtsbereichen sowie den Zuständigkeiten für die tätigen Einrichtungen. Dies hat zur Folge, dass für Forschungsprojekte sowohl Bundes- wie auch Landesgesetze einschlägig sein können, wobei nicht auszuschließen ist, dass die darin enthaltenen Regelungen sich gegenseitig ausschließen. Ohne Änderung der im Grundgesetz festgeschriebenen geteilten Kompetenzen zur Gesetzgebung kann eine einheitliche Regulierung durch einen Bund-Länder-Staatsvertrag erfolgen.

Anerkannte rechtliche Forschungsgrundsätze

Hinsichtlich der einheitlichen materiellen Regelungen kann auf das in **bestehenden Forschungsklauseln** enthaltene Konzept, das sich im Grundsatz bewährt hat, zurückgegriffen werden. Dieses Konzept enthält folgende Aspekte:

1. Die Verarbeitung personenbezogener Daten für Forschungszwecke hat, soweit dies der Forschungszweck erlaubt, mit Datensätzen zu erfolgen, die zuvor anonymisiert wurden. Erlaubt dies der Forschungszweck nicht, so ist, soweit möglich, eine Pseudonymisierung der Datensätze nötig.
2. Die Verarbeitung von personenbeziehbaren Daten für Forschungszwecke ist nur zulässig, wenn diese in einem von den verantwortlich Forschenden be-

herrschten informationstechnischen System oder Netzwerk erfolgt, in dem über technisch-organisatorische Maßnahmen gewährleistet wird, dass die Schutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit und Nichtverkettbarkeit in angemessener Weise konzeptionell festgelegt und realisiert werden.

3. Zulässig ist eine Verarbeitung, wenn diese auf einer informierten, expliziten, freiwilligen, widerrufbaren Einwilligung basiert.
4. Eine Verarbeitung für Forschungszwecke kann auch ohne Einwilligung der Betroffenen zulässig sein, wenn eine Abwägung des öffentlichen Interesses an dem Forschungsvorhaben die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.
5. Die für die wissenschaftliche Forschung Verantwortlichen dürfen personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Personen der Zeitgeschichte unerlässlich ist.
6. Die datenschutzrechtlichen Betroffenenrechte müssen auch im Forschungskontext – soweit praktisch möglich – gewährleistet werden.

Berufsgeheimnisse

Ein zentrales Problem bei der Forschung mit Berufsgeheimnissen, also insbesondere Patientengeheimnissen, besteht darin, dass gemäß dem weitgehend anerkannten **Zwei-Schranken-Prinzip** neben den allgemeinen Datenschutzregelungen den rechtlichen Anforderungen an die Verarbeitung von Berufsgeheimnissen genügt werden muss. Für die arbeitsteilige medizinische Forschung, an der ein großes öffentliches Interesse besteht, hat dies derzeit zur Folge, dass sämtliche Personen, denen Patientengeheimnisse offenbart werden, wozu auch IT-Personal, IT-Dienstleister oder Anonymisierer bzw. Pseudonymisierer zählen, arbeitsrechtlich der ärztlichen Leitung der Forschungseinrichtung unterworfen werden müssten. Da dies faktisch oft nicht möglich ist, sehen Aufsichtsbehörden insofern oft – contra legem – über das Fehlen von Offenbarungsbefugnissen hinweg oder interpretieren in die allgemeinen Forschungsklauseln eine Offenbarungsbefugnis hinein.

> Das Berufsgeheimnis in § 203 StGB sollte um ein Forschungsgeheimnis erweitert werden, mit der Möglichkeit, an der Forschung Beteiligte zu erfassen.

Diese unbefriedigende Rechtslage kann und sollte dadurch geändert werden, dass an der Forschung Beteiligte unter bestimmten formellen Erfordernissen dem Berufsgeheimnis nach § 203 StGB unterworfen werden. Derartige formelle Erfordernisse können bestimmte Genehmigungen/Zertifikate sein, die nach einem geregelten Verfahren von einem Bund-Länder-Forschungsgremium (s. u. 7) vergeben werden. Ein damit begründetes **„Forschungsgeheimnis“** sollte zudem durch eine entsprechende Regelung in der Strafprozessordnung „beschlagnahmesicher“ gemacht werden.

Bund-Länder-Forschungsgremium

Neben diesen materiellen technisch-organisatorischen und rechtlichen Regelungen bestehen bisher in den bestehenden allgemeinen und spezifischen Forschungsklauseln **prozedurale Vorkehrungen** wie z. B. Genehmigungsvorbehalte und Meldepflichten. Diese haben sich in der Praxis fast durchgängig nicht bewährt, weil der Prüfaufwand von den eingeschalteten Stellen (Ministerien, Datenschutzaufsichtsbehörden) mit den vorhandenen Ressourcen nicht erbracht werden kann und oft das nötige Problembewusstsein und die nötige Sachkompetenz nicht bestehen. Zudem orientieren sich die prozeduralen Vorkehrungen an möglicherweise vielen – für die Forschenden unbekannten – Gesetzen, was für die Forschenden bei regelkonformem Vorgehen einen unverhältnismäßigen Aufwand verursacht.

Ein weiterer Aufwand besteht darin, dass parallel zu den datenschutzrechtlichen Erfordernissen bei vielen medizinischen Forschungsvorhaben analog § 15 MBO-Ä **„Ethik-Kommissionen“** einbezogen werden müssen, deren Bearbeitungszeit und Ergebnisse oft nicht einschätzbar sind. Dabei handelt es sich um eine Doppelstruktur. Ethische und datenschutzrechtliche Erwägungen verfolgen weitgehend identische Schutzziele (Würdeschutz, Persönlichkeitsschutz, sonstiger Grundrechtsschutz). Beide Verfahren fordern letztlich eine Optimierung bzw. eine Abwägung des Forschungsinteresses mit Betroffeneninteressen. Sie unterscheiden sich in der Zusammensetzung des „Spruchkörpers“
und der damit verbundenen Fachkenntnis. Daher sollte im Interesse der Entbürokratisierung und Vereinfachung ein Verfahren vorgesehen werden, in das technisch-organisatorische, datenschutzrechtliche, ethische und fachliche Erwägungen einfließen können.

Als ein solches – von einem Bund-Länder-Staatsvertrag vorgesehenes – Gremium kommt eine **unabhängige Stelle** mit der o. g. Fachkenntnis in Betracht. Dieses

Bund-Länder-Forschungsgremium sollte – gemäß der Sensitivität des jeweiligen Forschungsvorhabens – Genehmigungsrechte oder bei einer reinen Meldepflicht Vetorechte haben. Sein Verhältnis zu den Datenschutzaufsichtsbehörden sollte so geregelt werden, dass ein gegenseitiges Konsultationsrecht besteht. Eine Meldung/Genehmigung entbindet die für die Forschung Verantwortlichen nicht von ihren datenschutzrechtlichen Compliance-Pflichten und die Aufsichtsbehörden nicht von ihren Beratungs- und Kontrollpflichten.

Welche Forschungsprojekte melde- bzw. genehmigungspflichtig sind, bedarf der weiteren fachlichen Erörterung. Anknüpfungspunkt hierfür sollte die Sensitivität des jeweiligen Projektes sein. So kann wohl **auf eine Meldung verzichtet** werden, wenn klassische Eigenforschung erfolgt, und bei Einzelprojekten, wenn die Datenverarbeitung auf einer informierten Einwilligung der Betroffenen basiert.

Meldepflichtig sollten in jedem Fall institutionenübergreifende Projekte sein, die zumeist eine eigene Infrastruktur und ein umfassendes Datenschutzkonzept vorweisen müssen. Meldepflichtig müssen in jedem Fall die Projekte sein, bei denen eine Interessenabwägung die Betroffeneneinwilligung ersetzen soll. Besteht eine Meldepflicht, muss das Bund-Länder-Forschungsgremium nicht nur weitere Aufklärungs-, sondern auch Untersagungsrechte haben.

Neue medizinische Erkenntnisse durch die Auswertung von Gesundheitsdaten.

Genehmigungspflichtig sollten Projekte sein, bei denen hochsensitive Daten verarbeitet werden. Dies gilt z. B. für über Einzelmarkierungen hinausgehende Gensequenzierungen oder für Datenübermittlungen und Zweckänderungen, bei denen eng definierte Zwecke verlassen werden. Zeitlich nicht eng begrenzte Studien bzw. Forschungsdatenbanken sollten unter einen umfassenden Genehmigungsvorbehalt gestellt werden.

Für bestimmte Projekte, etwa internationale Studien, Forschungsnetzwerke, Krankheitsregister und Biomaterialdatenbanken könnten vom Bund-Länder-Forschungsgremium zusätzliche **Anforderungen oder Standards** festgelegt werden, die bei der Prüfung bzw. Genehmigung zur Grundlage gemacht werden. Das Gremium könnte zudem die Aufgabe zugewiesen bekommen, Standards für die Datenübertragbarkeit nach Art. 20 DSGVO für Forschungsprojekte sowie für nach Art. 7 DSGVO zulässige Einwilligungen in die Forschungsdatenverarbeitung festzulegen.

> Eine unabhängige Stelle sollte ethische und datenschutzrechtliche Erwägungen in Melde- und Genehmigungsverfahren für Forschungsprojekte vereinen.

Dem Bund-Länder-Forschungsgremium könnte auch die Aufgabe zukommen, eine **Pseudonymisierungs-Infrastruktur** zu erarbeiten und zu unterstützen oder diese gar selbst aufzubauen und zu betreiben. Bisher gibt es derartige (begrenzte) Infrastrukturen im Bereich der Krebsregistrierung sowie im Bereich der gesetzlichen Krankenversicherung.

Ein wichtiger Aspekt, der bisher bei der personenbezogenen Verarbeitung von Daten für Forschungszwecke stark vernachlässigt wurde, sind die demokratische Kontrolle und die hierfür nötige **Transparenz**. Bei einer Zentralisierung der bisherigen Aufgaben von Ministerien, Aufsichtsbehörden und Ethik-Kommissionen könnte das Bund-Länder-Forschungsgremium öffentlich oder teilöffentlich einsehbare Forschungsregister etablieren, die einen Überblick über die Forschung mit personenbezogenen Daten, über die Verantwortlichen, die Ziele und Fragestellungen sowie die grundrechtsschützenden Maßnahmen geben.

Schlussbemerkung

Der Forschungsstandort Deutschland leidet seit Jahren unter der Untätigkeit des Gesetzgebers hinsichtlich seiner Aufgabe, die Rahmenbedingungen für ein **zukunftsgerichtetes Forschen** bei Beachtung der Grundrechte der betroffenen Menschen zu schaffen. Dadurch ergeben sich Nachteile für die wirtschaftliche Entwicklung, den gesellschaftlichen Fortschritt und den Grundrechtsschutz der Menschen. Über die vorgeschlagenen Gesetzesänderungen mit einem Bund-Länder-Staatsvertrag könnte diese Blockade aufgelöst werden. Zugleich könnten damit Erfahrungen gesammelt werden, die auch in einem größeren einheitlichen Rechtsraum, z. B. in der Europäischen Union, nutzbar gemacht werden können.Dieser Text ist ein Beitrag in dem Sammelband der Stiftung Datenschutz (Hrsg.), Big Data und eHealth, Reihe DatenDebatten Bd. 2, Erich Schmidt Verlag Berlin 2017

Dieser Text ist ein Beitrag in dem Sammelband der Stiftung Datenschutz (Hrsg.), Big Data und eHealth, Reihe DatenDebatten Bd. 2, Erich Schmidt Verlag Berlin 2017.

Gesamtheit der Grundrechte als belastbarer Maßstab für den „risikobasierten“ Ansatz: ein Lösungsvorschlag für das Zweckbindungsprinzip

Von Maximilian von Grafenstein LL.M., Alexander von Humboldt Institut für Internet und Gesellschaft

Herausforderungen auf dem privaten Sektor

Das Zweckbindungsprinzip stellt einerseits ein intuitiv einleuchtendes Schutzinstrument der Betroffenen dar. Transparenz, Rechtssicherheit und Vorhersehbarkeit der Datenverarbeitung werden durch die Begrenzung des Datenumgangs auf bestimmte, vorab festgelegte Zwecke gewährleistet.[99] Andererseits steht es im Kontext von Big Data im Spannungsfeld der Offenheit von Innovationsprozessen in Wirtschaft und Gesellschaft. Innovationsprozesse verlaufen meist nicht linear, sondern dynamisch und nichtlinear. Das macht ihren Ausgang üblicherweise nur beschränkt vorhersehbar.[100] Der Handlungsspielraum datenverarbeitender Unternehmen wird so beschränkt, weil diese bereits bei Erhebung der Daten den Verlauf und Ausgang der folgenden Verarbeitungsprozesse antizipieren und sich grundsätzlich innerhalb der Grenzen der einmal genannten Zwecke bewegen müssen.[101] Auf den ersten Blick scheint für die Untersuchung unbekannter Zusammenhänge kein Raum zu verbleiben.

> Dynamische nicht-lineare Innovationsprozesse mit unbekanntem Ausgang erschweren eine Vorabfestlegung verfolgter Zwecke.

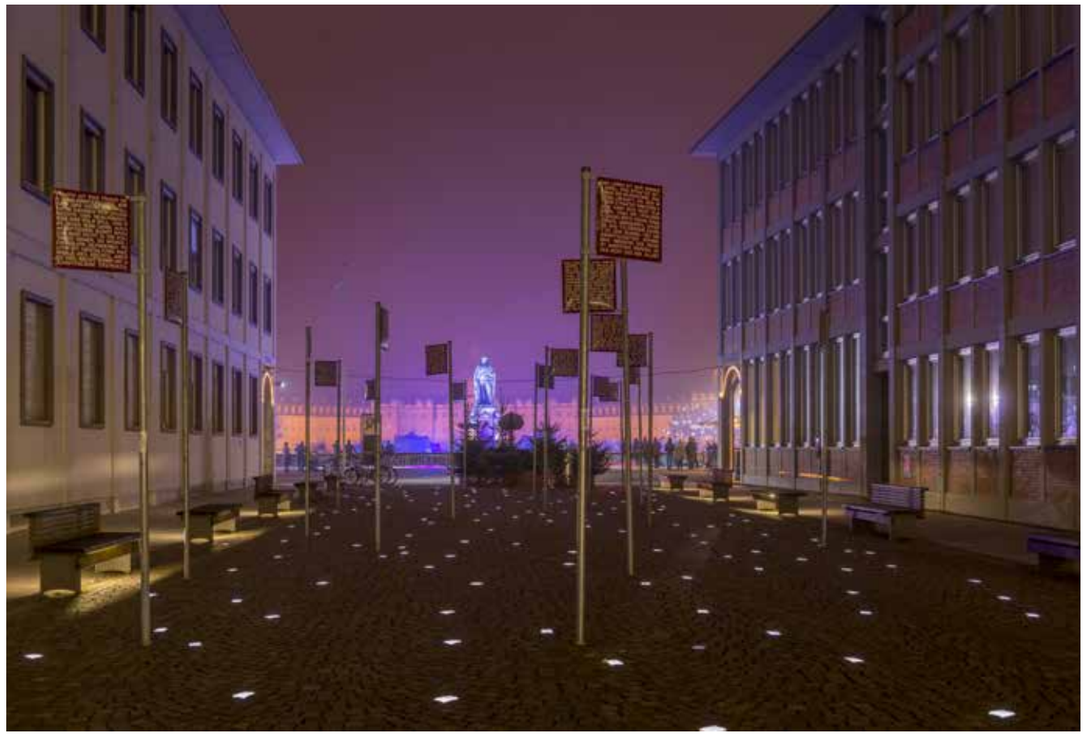
Auf den zweiten Blick lässt das Zweckbindungsprinzip jedoch einen erheblichen Spielraum bei der Auslegung. Die Umsetzung des Zweckbindungsprinzips in der Datenschutzgrundverordnung erfordert nicht die strikte Zweckidentität bei Weiterverarbeitung bereits erhobener Daten, sondern gebietet „nur“ die Zweckvereinbarkeit. Artikel 6 Abs. 4 EU 2016/679 (DSGVO) nennt einige Kriterien zur Vereinbarkeitsprüfung. Die Artikel-29-Datenschutzgruppe hatte diese Kriterien bereits im Rahmen eines Prüfungsschemas für die Datenschutzrichtlinie 95/46/EG vorgeschlagen. Danach soll der ursprüngliche Zweck mit dem neuen Zweck nicht nur formal verglichen, sondern auch der Kontext der Datenerhebung und die Erwartungen des Betroffenen, die Auswirkungen auf ihn, die Art der Daten sowie die Maßnahmen gegen einen möglichen Datenmissbrauch berücksichtigt werden.[102] Allerdings gibt es noch keine klaren Maßstäbe für die notwendige Konkretisierungstiefe bei der Bestimmung der Zwecke und auch die zuvor genannten Kriterien für die Zweckvereinbarkeit bedürfen ihrerseits eines objektiven Maßstabs. Denn welches ist der Gradmesser, um die „Distanz“ zwischen zwei Zwecken zu messen, um den Kontext der Datenerhebung zu definieren, die Vernünftigkeit einer Erwartung des Betroffenen festzustellen oder die Art der personenbezogenen Daten zu bestimmen?

Die Herausforderung, die das Zweckbindungsprinzip für private Datenverarbeiter darstellt, liegt also darin, einen belastbaren und so Rechtssicherheit schaffenden Maßstab für seine Auslegung zu entwickeln.[103] Denn der Spielraum des Datenverarbeiters bzw. die Innovationsoffenheit des Zweckbindungsprinzips hängt im Einzelfall von einem solchen Maßstab und der Gewichtung der widerstreitenden grundrechtlich geschützten Interessen ab.[104]

Dieser Beitrag schlägt eine Lösung vor, wie aus der Gesamtheit der Grundrechte des Betroffenen ein belastbarer Maßstab für die datenschutzrechtliche Risikoprüfung und damit für die Auslegung auch des Zweckbindungsprinzips abgeleitet werden kann. Damit knüpft der Beitrag an Art. 1 Abs. 2 DSGVO an, nach dem die Verordnung nicht nur das Datenschutzgrundrecht, sondern alle Grundrechte des Betroffenen schützt.

Zweckbindungsprinzip als Instrument der Risikoregulierung

Betroffene wie Datenverarbeiter können vor allem auf dem privaten Sektor die Folgen der Datenverarbeitung aufgrund der dezentral und nichtlinear ablaufenden



Platz der Grundrechte in Karlsruhe

Informationsflüsse schwer vorhersehen.[105] Auch resultieren die Risiken der Datenverarbeitung aus den unterschiedlichsten sozialen Kontexten:[106] Benachteiligung bei der Arbeitsplatzsuche, Manipulation öffentlich geführter Debatten, Diskriminierung wegen Religionszugehörigkeit, Verhandlungsungleichgewicht auf Marktplätzen usw.

> Bei der Zweckbestimmung sowie Vereinbarkeitsprüfung neuer und ursprünglicher Zwecke fehlt noch ein klarer Maßstab.

Entsprechend wird das Datenschutzrecht zunehmend als Risikoschutzrecht diskutiert.[107] Eine Konsequenz daraus ist, dass sich die Zwecke der Datenverarbeitung auf diese Risiken beziehen sollten.

Die beispielhafte Aufzählung bekannter Risiken zeigt, dass weitere über das Recht auf informationelle Selbstbestimmung bzw. das Recht auf Schutz personenbezogener Daten/Achtung des Privat- und Familienlebens[108] hinausgehende Grundrechte betroffen sein können. Nicht nur in der analogen Welt schützt Art. 12 GG (Art. 15 GrCh) vor Benachteiligung bei der Arbeitsplatzsuche, Art. 5 und 8 GG (Art. 11 und 12 GrCh) vor der Manipulation öffentlich geführter Debatten, Art. 3 und 4 GG (Art. 10 und 21 GrCh) vor Diskriminierung wegen der Religion und Art. 2 und 3 GG (Art. 21 und 38 GrCh) vor Verhandlungsungleichgewicht auf Marktplätzen. In der digitalen Welt zentriert sich der Fokus der öffentlichen Debatte auf den Datenschutz als Schutz der informationellen Selbstbestimmung (bzw. Art. 7 und/oder 8 GrCh).[109] Die für jeden Einzelschritt der Verarbeitung erforderliche Zweckbestimmung und Zweckvereinbarkeitsprüfung muss jedoch die Risiken benennen können, die in Bezug auf die Ausübung dieser Grundrechte entstehen, sie gewichten und in einen angemessenen Ausgleich bringen.

Ohne einen solchen Maßstab zur Bestimmung der rechtlich geschützten Interessen dürfte die erhebliche Rechtsunsicherheit, die aus dem Zweckbindungsprinzip resultiert, kaum in den Griff zu kriegen sein. Dies

gilt nicht nur für Verarbeiter, sondern auch für die Betroffenen, die bei jeder Datenerhebung mit einer Masse von Zweckangaben konfrontiert sind und dabei die Risiken kaum abschätzen können.[110] Unter Gesichtspunkten der Aufmerksamkeitsökonomie können die Betroffenen die Information kaum verarbeiten.[111]

Die Zweckbestimmung und Angabe gegenüber dem Betroffenen sollten daher dazu dienen, die Risiken für die Grundrechte des Betroffenen aufzudecken, die aus der Verarbeitung seiner personenbezogenen Daten resultieren. Die Zweckbindung verhindert dann, dass aus der Verarbeitung andere Risiken resultieren, als durch die ursprüngliche Zweckbestimmung vorgegeben waren. An der so definierten Risikokontrolle können die Schutzinstrumente des Datenschutzrechts spezifisch ausgerichtet werden.

Die Angabe der Verarbeitungszwecke sollte dem Betroffenen das Risiko von Grundrechtseingriffen aufzeigen.

Grundrechte als innovationsoffener Bewertungsmaßstab

Die Zweckbestimmung an allen Privatheits-, Freiheits- und Gleichheitsrechten auszurichten, erlaubt es also, die Risiken für den Betroffenen und damit die jeweils erforderlichen Schutzinstrumente effektiver zu bestimmen, als wenn nur das Recht auf informationelle Selbstbestimmung bzw. Art. 7 und/oder 8 der Grundrechte-Charta den Maßstab bilden.[112] Genauso ist es möglich, für das Zweckbindungsprinzip einen differenzierten Maßstab anhand der jeweils konkret gefährdeten Grundrechte herauszubilden. Mit dem so erreichten effektiveren Grundrechtsschutz geht zugleich eine höhere Innovationsoffenheit einher.

Denn die Datenverarbeitung kann die grundrechtlichen Schutzgüter, wie die Unverletzlichkeit der Wohnung, Vertraulichkeit der Kommunikation, Wahrung der Privatsphäre, aber auch die speziellen Freiheits- und Gleichheitsrechte betreffen oder eben nicht betreffen. So kann beispielsweise ein durchgeführtes Profiling (neben dem Recht auf informationelle Selbstbestimmung) schwerpunktmäßig die Berufsfreiheit tangieren, wenn die Informationen potenziellen Arbeitgebern verfügbar werden, selbst wenn es sich dabei um öffentlich zugängliche Daten handeln sollte und weder Intim- noch Privatsphäre betroffen sind. Die Schutzinstrumente (hier voraussichtlich insbesondere Partizipationsrechte) sollten dann so gewählt werden, dass die Risiken für die Ausübung der Berufsfreiheit möglichst reduziert oder sogar ausgeschlossen werden. Nur wenn dies nicht möglich ist, würde die Prüfung, ob die Datennutzung zu diesen neuen Zwecken mit den ursprünglichen Zwecken vereinbar ist, negativ ausfallen (es sei denn, dass Grundrechtspositionen der Unternehmen den grundrechtlichen Schutz der Berufsfreiheit des Betroffenen überwiegen). Die Abwägung kann sich dabei an der verfassungsgerichtlich herausgearbeiteten Gewichtung orientieren.[113]

Ist bei Gestaltung der Datenverarbeitungsvorgänge kein spezifisches Risiko für die Grundrechte des Betroffenen erkennbar, können sich die Zweckbestimmung und Vereinbarkeitsprüfung hierauf nicht beziehen. Der Verarbeiter muss dann lediglich Schutzmaßnahmen gegen die unspezifischen Risiken, sprich die abstrakte Gefahr einer noch nicht definierten Grundrechtsgefährdung, ergreifen. Damit wird zwischen einer konkret absehbaren Grundrechtsgefährdung und einer abstrakt nicht ausschließbaren Grundrechtsgefährdung unterschieden.[114] Anhand des so jeweils definierten Gefährdungsgrads und gegebenenfalls konkret gefährdeten Grundrechts können individuelle Schutzmaßnahmen ergriffen werden. Gleich-zeitig verbleibt ausreichend Raum für Innovationen. Im obigen Beispiel des Profilings könnte zum Beispiel eine Zugriffskontrolle ermöglichen, dass Daten nur für die Grundrechtspositionen

des Betroffenen nicht tangierende oder diese überwiegende Zwecke eingesetzt werden.

Die Zweckangabe zur Anzeige spezifischer Risiken

Teilt der Datenverarbeiter dem Betroffenen das Grundrechtsrisiko im Wege der Zweckangabe mit, kann sich der Betroffene auf das Risiko einstellen.[115] Wenn die Zweckänderung ein neues Risiko (etwa für andere Privatheits-, Freiheits- und/oder Gleichheitsrechte) eröffnet, bedarf es einer erneuten Anzeige.[116] Je intensiver das spezifische Risiko für diese Grundrechte ist, desto deutlicher sollten die ursprüngliche wie auch die nachträgliche Zweckangabe darauf hinweisen.[117] Wenn jedoch die Zweckänderung kein neues Risiko mit sich bringt, dürfte eine Warnung des Betroffenen obsolet sein. Denn dann gibt es kein Bedürfnis seitens des Betroffenen, sich auf ein neues Risiko einzustellen. Diese Grundsätze ließen sich auch auf die Einwilligung übertragen. Die Einwilligung bezieht sich dann nicht auf die Daten an sich, sondern auf die durch ihre Verarbeitung hervorgerufenen Risiken.

Standardisierung und Zertifizierung von Verarbeitungszwecken können die Rechtssicherheit erhöhen.

Die Standardisierung von Verarbeitungszwecken

Auch wenn die Gesamtheit der Grundrechte einen belastbaren Maßstab für die Risikobestimmung darstellt, reduziert das noch nicht vollständig das Problem der Rechtsunsicherheit. Denn diese folgt auch aus den Einzelfallprüfungen, die bei der Konkretisierung des Zweckbindungsprinzips durchzuführen sind.[118] Eine Lösungsmöglichkeit für dieses Problem können die Standardisierung und Zertifizierung von Verarbeitungszwecken darstellen.[119] Verarbeiter von Daten können so genauso wie die Betroffenen darauf vertrauen, dass die Verarbeitung von Daten zu diesen Zwecken (und unter gegebenenfalls weiteren Bedingungen) zumindest rechtlich unbedenklich ist.[120] Die Standardisierung kann zudem ein wichtiges weiteres Selbstregulierungsinstrument darstellen, um den internationalen Datenaustausch rechtlich abzusichern.[121] So können mit Standards verbundene Kontroll- und Sanktionsmechanismen dafür Sorge tragen, dass im Ausland operierende Unternehmen, die auf Daten unter diesen Standards zugreifen, auch die damit vorgegebenen Zwecke und gegebenenfalls weitere Bedingungen einhalten. Schließlich bilden Standards eine Voraussetzung, die technische Interoperabilität für Privacy-by-Design-Maßnahmen herzustellen. Die Kommunikation unter Maschinen erfordert eine formalisierte Sprache. Diesen Formalisierungsgrad können Standards herstellen. Standards von Verarbeitungszwecken bilden so die Voraussetzung dafür, dass Privacy-by-Design-Einstellungen vorgenommen werden können und die Verarbeiter der Daten die Einhaltung dieser Einstellungen über die Auslagerung auf Maschinen skalieren können.

Fazit

Der hier vorgestellte Ansatz knüpft an Art. 1 Abs. 2 DSGVO an und stellt die Möglichkeiten der darin vorgesehenen Ausrichtung der Datenschutzinstrumente an der Grundrechtsgesamtheit vor. Das Zusammenspiel aller grundrechtlichen Privatheits-, Freiheits- und Gleichheitsrechte kann einen Maßstab für die Auslegung des Zweckbindungsprinzips, sprich für die Frage nach dem Konkretionsgrad der Zweckbestimmung und der Zweckvereinbarkeit, darstellen. Da die Grundrechte des Betroffenen spezifische Kontexte sozialer Interaktion differenziert abbilden, stellt dieser Ansatz einen sowohl innovationsoffenen als auch effektiven Risikoschutz zur Verfügung. Über Standardisierung und Zertifizierung kann für Unternehmen die Bürde der Grundrechtsabwägung im Einzelfall erleichtert werden. So kann auch in Zeiten datengetriebener Innovation Vertrauen geschaffen werden.

Datensouveränität und Recht 4.0

Das Grünbuch „Digitale Plattformen“ im Spannungsfeld zwischen Datenschutz und Wettbewerbsrecht

Prof. Dr. Beatrix Weber, MLE
Institut für Informationssysteme, iisys, Hochschule für Angewandte Wissenschaften Hof

Einleitung

Das Grünbuch „Digitale Plattformen“ vom 30.05.2016 soll im Rahmen der Digitalen Strategie 2015 einen Ordnungsrahmen für mehr Investitionen und mehr Innovationen bei fairem Wettbewerb schaffen. Gleichzeitig sollen die Grundrechte und die Datensouveränität von Individuen und Unternehmen gesichert werden. Datenvermeidung kann nach dem Grünbuch in Zeiten von Big Data keine Leitlinie mehr sein.[122] Daten sind vielmehr der wichtigste „Grundstoff“ der digitalen Ökonomie. Zweckbindungsgrundsatz und Datensparsamkeit sind demnach konkretisierungsbedürftig und der Abwägung mit anderen Rechten und Interessen nicht entzogen.[123] Ziel soll die effektive, individuelle Datensouveränität sein. Der Dateninhaber soll hierbei vor konkreten Missbrauchsgefahren geschützt werden.

Daten wird ein wirtschaftlicher Wert zugebilligt. Sie haben insofern die Funktion einer „neuen Währung“ und können als Substitut für ein Entgelt dienen.[124] Als Leitlinie zur Einwilligung in die Nutzung und Verarbeitung personenbezogener Daten wird im Grünbuch der vom „Unternehmen kommunizierte Zweck“ in den Mittelpunkt gestellt. Mehr Kommerzialisierung erfordere allerdings auch mehr individuelle Kontrolle. Eine Einwilligung nach Sphären, das sogenannte Identity Management, standardisierte Einwilligungen für bestimmte Geschäftsmodelle, Ampelsysteme, Zertifizierungen, die treuhänderische Wahrnehmung von Datenrechten durch Dritte und die Selbst- oder Koregulierung, z. B. durch Verhaltenskodizes, werden als mögliche Regelungsansätze angesprochen.[125] Datenanalyseverfahren, die individuelle Preisbildung und das Profiling werden bei vorheriger Einwilligung, die auf ausreichender Information basiert, als zulässig erachtet.[126]

Recht 4.0

Notwendig ist die Koordinierung des gesamten Ordnungsrahmens, d. h. die Abstimmung der einzelnen Gesetze aufeinander mit Blick auf die übergeordneten Wertentscheidungen zu Innovation, Investition, Wettbewerb und Datenschutz bei digitalen Geschäftsmodellen, insbesondere unter Nutzung von Big Data.

Recht 4.0 ist nicht nur Datenschutz bei der Nutzung von Big Data für digitale Plattformen. Datenschutz ist nicht nur BDSG oder Datenschutzgrundverordnung. Recht 4.0 ist der gesamte Ordnungsrahmen, der mit Blick auf Technologien digitaler Plattformen und die Nutzung von Big Data anzupassen und zu koordinieren ist. Im Grünbuch wird daher zu Recht auf den gesamten Rechtsrahmen verwiesen, der die Rechtsbeziehungen der Marktteilnehmer regelt. Hierzu gehören neben der Datenschutzgrundverordnung u. a. das Gesetz gegen den unlauteren Wettbewerb (UWG), das Gesetz gegen Wettbewerbsbeschränkungen (GWB), das Telemediengesetz (TMG), das Urheberrechtsgesetz (UrhG) und das Telekommunikationsgesetz (TKG).

Wettbewerbsrecht 4.0

Regulierungsziel: Anwendung des Kartellrechts auf digitale Geschäftsmodelle
Die Erweiterung der Marktkriterien auf unentgeltliche Leistungen führt im Ergebnis zur wirksamen Einbeziehung neuer digitaler Geschäftsmodelle, ist aber mit Blick auf die entgeltsubstituierende Funktion von „Daten“ und „Aufmerksamkeit für Werbung“ im Gesamtregulierungsrahmen nicht stringent.

Die Anpassung des Kartellrechts an digitale Geschäftsmodelle wird mit dem Grünbuch und dem Referentenentwurf zur 9. GWB-Novelle aufgegriffen. Das Kartellrecht soll an den Strukturwandel unter Berücksichtigung der fortschreitenden Digitalisierung angepasst werden. Es soll aber kein branchenspezifisches Kartellgesetz begründet werden. Der Schutz und die Regulierungsfunktion des Kartellrechts sollen vielmehr sektorübergreifend bestehen bleiben. Im Sinne der nationalen Nachhaltigkeitsstrategie der Bundesregierung sollen Innovationspotenziale in Technologiemärkten geschützt und die Teilhabe möglichst vieler Wirtschaftsakteure (Unternehmen und Verbraucher) an dieser wirtschaftlichen Entwicklung gefördert werden.[127] Die Besonderheiten der digitalen Plattformen liegen u. a. in der häufigen Unentgeltlichkeit von Angeboten, Netzwerkeffekten und Konzentrationstendenzen, der Verarbeitung von Big Data, Lock-in-Effekten und einer hohen Dynamik technologischer Entwicklungen. Diese sind mit den herkömmlichen Marktdefinitionen des Kartellrechts häufig nicht adäquat zu erfassen.

Der **relevante Markt** wurde bisher räumlich durch ein geografisches Gebiet mit homogenen Wettbewerbsbedingungen und sachlich nach der Substituierbarkeit von Produkten und Dienstleistungen mit Blick auf Eigenschaften, Preis und Verwendungszweck abgegrenzt. Der Preis entfällt bei einer Vielzahl von unentgeltlich angebotenen Leistungen, die sich in den mehrseitigen Märkten der Internetökonomie u. a. durch Werbung finanzieren. Um hier eine Missbrauchskontrolle zu erreichen, soll nach § 18 Abs. 2a GWB-E die Unentgeltlichkeit von Leistungen einen Markt nicht mehr ausschließen. Diese Klarstellung scheint auf den ersten Blick digitale Geschäftsmodelle gut zu erfassen. Hinsichtlich des regulatorischen Gesamtvorhabens ist es allerdings nicht konsequent, auf der einen Seite den ***Daten die Qualität eines Entgeltsubstituts zuzusprechen***[128], andererseits aber für die Marktabgrenzung auf die Unentgeltlichkeit der Leistungen abzuheben. Auch die ***Finanzierung über Werbung*** beruht letztlich auf einem Entgelt für die Platzierung der Werbung oder die indirekte Einpreisung in ein Produkt. Die Änderung ist allerdings so konzipiert, dass die Unentgeltlichkeit keine marktausschließende Wirkung hat. § 18 Abs. 2a GWB-E: ***„Der Annahme eines Marktes steht nicht entgegen, dass eine Leistung unentgeltlich erbracht wird.“*** Insoweit wird das Ziel, die Besonderheiten der digitalen Geschäftsmodelle überhaupt zu erfassen, erreicht. Die Abgrenzung der entgeltlichen und unentgeltlichen Leistungen, die Zuordnung zu einem einheitlichen oder getrennten Markt und die Kriterien hierfür bleiben für die Rechtsanwendung offen. Sie sollen nach der Entwurfsbegründung der Einzelfallwürdigung überlassen bleiben,[129] was eine Rechtsunsicherheit für Unternehmen bedeutet.

Regulierungsziel: Verhinderung von Lock-in-Effekten
Das Regulierungsziel der Verhinderung von Lock-in-Effekten kann erreicht werden. Die Regelungen sind jedoch zur Herstellung von Rechtssicherheit für Unter-

nehmen zu ungenau. Die Erfahrung in anderen Märkten zeigt, dass Rechtsstreitigkeiten über Jahre ein Investitions- und Innovationshemmnis darstellen.

Für die Bewertung der Marktstellung werden über § 18 Abs. 3 GWB hinaus in § 18 Abs. 3a GWB-E zusätzliche Kriterien eingeführt, mit denen die Besonderheiten digitaler Geschäftsmodelle berücksichtigt werden sollen: direkte und indirekte Netzwerkeffekte, parallele Nutzung mehrerer Dienste, Wechselaufwand (Kosten) für Nutzer, Größenvorteile durch Netzwerkeffekte, Zugang zu Daten und der innovationsgetriebene Wettbewerbsdruck.

Indizien, die gegen einen Lock-in-Effekt, d. h. gegen Marktzutrittsschranken, sprechen, sind damit die technische und auch tatsächliche Möglichkeit, mehrere Dienste oder Produkte nebeneinander zu nutzen (Multihoming), das Bereitstellen standardisierter Schnittstellen, die Erleichterung des Wechsels durch niedrige Wechselkosten und Datenportabilität. Die Kriterien der Heterogenität der Nutzer und der horizontalen Produktdifferenzierung der Plattformen sind lediglich in der Gesetzesbegründung des Referentenentwurfes genannt.[130] Nicht alle Kriterien stellen Besonderheiten digitaler Geschäftsmodelle dar. Daten als ***„essential facilities"***[131] und der ***diskriminierungsfreie Zugang zu Daten*** sind als Kriterien nicht neu, sondern u. a. aus dem Automobil-Aftermarket im Zusammenhang mit der Bereitstellung technischer Informationen für markenungebundene oder Mehrmarkenreparaturbetriebe, sogenannte freie Werkstätten, geläufig.[132] Regelungen zur Erleichterung des Anbieterwechsels hinsichtlich Kostenfreiheit und Fristen sind aus dem Strom- und Gasmarkt[133] sowie dem Bereich der Telekommunikationsdienstleistungen[134] bekannt. Die Monopolkommission kritisiert in ihrem letzten Hauptgutachten hierzu die Beschränkung der Kriterien auf mehrseitige Märkte und Netzwerke und moniert die fehlende ausdrückliche Nennung in § 18 Abs. 3 GWB.[135]

Die Ausformung des Kriteriums des **„Zugangs zu Daten"** wird für Unternehmen einer der Hauptfaktoren der Wirtschaftlichkeit ihrer digitalen Geschäftsmodelle werden. Die wirtschaftliche Bedeutung soll in einer Gesamtbetrachtung aller Umstände abhängig sein von

- Art und Umfang der vorhandenen Daten,
- ihrer Bedeutung für die Geschäftstätigkeit,
- den Fähigkeiten und Möglichkeiten des Unternehmens zur Datenauswertung und-verarbeitung,
- der Einschränkung der Möglichkeiten der Wettbewerber, vergleichbar große Datenpools aufzubauen,
- der exklusiven Herrschaft über bestimmte Daten,
- dem Zweck der Datenerhebung und-nutzung für das Unternehmen.

Unklar bleibt hierbei:

- Unter welchen konkreten Voraussetzungen erzeugt ein Datenbestand einen Lock-in-Effekt?
- Was heißt „übermäßiges Sammeln" von Daten mit Blick auf die Nutzung von Big Data im Sinne einer Unausgewogenheit von Leistung und Gegenleistung?
- Mit welchem wirtschaftlichen Aufwand sind welche Daten in welchen Formaten zur Portierung bereitzustellen?[136]
- Wie sind sich verändernde Marktgegebenheiten mit Blick auf einen Lock-in-Effekt versus Innovationsschutz für das Unternehmen zu bewerten?

Regulierungsziel: Fusionskontrolle von Start-up-Übernahmen

Das Ziel der Fusionskontrolle gesamtwirtschaftlich bedeutenderer Fälle für digitale Geschäftsmodelle wird erreicht. Angesichts der Höhe der Aufgreifschwelle ist die tatsächliche Lenkungsfunktion fraglich. Eine Behinderung von innovativen Start-ups ist daher nicht zu erwarten.

Mit der Einführung eines neuen Aufgreifkriteriums, des ***Transaktionswertes***, soll die Fusionskontrolle bei der Übernahme von Start-ups ermöglicht werden, die ein hohes Marktpotenzial und für den Erwerber

eine hohe wirtschaftliche Bedeutung haben, die sich (noch) nicht in entsprechenden Umsätzen ausdrücken. Innovationen sollen geschützt und Märkte vor strukturellen Verschließungen bewahrt werden. Geringe Umsätze würden insbesondere im digitalen Wirtschaftsbereich nicht immer der wettbewerblichen Bedeutung des Unternehmens gerecht, da eine erfolgreiche Markteinführung mit einer großen Zahl von Nutzern und Netzwerkeffekten oft durch unentgeltliche oder preiswerte Angebote erreicht werde. Das Umsatzpotenzial entfalte sich oft erst nach der Übernahme, weswegen bereits etablierte Unternehmen mit internetbasierten Geschäftsmodellen versuchten, potenzielle Wettbewerber aufzukaufen.

Wenn die beteiligten Unternehmen weltweit insgesamt mehr als 500 Mio. Euro Umsatz erzielt haben, muss nur eines der beteiligten Unternehmen im letzten Geschäftsjahr vor dem Zusammenschluss Umsatzerlöse von mehr als 25 Mio. Euro erwirtschaftet haben. Die anderen Unternehmen dürfen im Inland Umsatzerlöse von 5 Mio. Euro nicht überschritten haben und mindestens eines muss im Inland tätig sein oder voraussichtlich tätig werden. Wenn dann der Transaktionswert (Kaufpreis zuzüglich etwaiger Verbindlichkeiten) mehr als 350 Mio. Euro beträgt, kann eine Fusionskontrolle stattfinden, siehe § 35 Abs. 1a, § 38 Abs. 4a GWB-E. Nach den im Referentenentwurf genannten Zahlen zu den wichtigsten Start-up-Übernahmen im letzten Jahr hätte nur eine Übernahme im einschlägigen Bereich gelegen. Für die Anwendung der Vorschrift werden daher auch nur Fälle im einstelligen Bereich erwartet.[137]

Datenschutz 4.0

„Dateninhaber" als Datensouverän des persönlichen Gehalts und der wirtschaftlichen Verwertbarkeit der Daten

Datensouveränität muss im Lichte des Rechts auf informationelle Selbstbestimmung und der digitalen Privatautonomie zwei Kernpunkte umfassen:

- *die Hoheit über den persönlichen Gehalt der Daten und*
- *die Hoheit über die wirtschaftliche Verwertbarkeit.*

Rechtlich relevante Formen der Nutzung von Daten sind vor allem die Nutzung personenbezogener Daten sowie von Daten, die mit Rechten Dritter wie Urheberrechten, Rechten des Datenbankherstellers, Recht am eigenen Bild oder gewerblichen Schutzrechten verknüpft sind, Daten aus verschiedenen Quellen und das Sammeln zunächst unstrukturierter Datenmengen (data lakes), zumeist unter Nutzung großer Datenmengen (Big Data). Der Wert der Daten zur ökonomischen Nutzung steigt in der Regel mit der Menge der Nutzer und/oder der Granularität der Datenbestände. Die bisherigen Prinzipien des Datenschutzes kollidieren hier hinsichtlich Datensparsamkeit, Datenminimierung und kurzer Speicherdauer mit der Entwicklung innovativer Produkte und Dienstleistungen durch Nutzung von Big Data über längere Zeitreihen. „Volume" (große Datenmengen), „Velocity" (hohe Frequenz einströmender Daten) und „Variety" (Mischung aus strukturierten und unstrukturierten Daten) sind zur Auswertung der Daten erforderlich.[138] Diese kollidierenden Rechte sind im Sinne einer Datability[139], eines nachhaltigen und verantwortungsvollen Umgangs mit Daten, in Einklang zu bringen.[140]

Daten haben einen ***ökonomischen Wert.*** Sie können als Substitut für eine Zahlung behandelt werden, wenn sie als Entgelt in einem vertraglichen Austauschverhältnis dienen. Mit dem Vorschlag einer ***„Richtlinie zu vertragsrechtlichen Aspekten bei der Bereitstellung digitaler Dienste"***[141] liegt ein erster Umsetzungsvorschlag zur rechtlichen Anerkennung der Funktion von Daten als **Entgeltsubstitut** vor. Diese liegt nach dem Richtlinienvorschlag bei aktivem Bereitstellen von Informationen wie Name, E-Mail-Adresse oder Foto vor. Cookies oder IP-Adressen, die nur anlässlich eines Kundenkontaktes eingesetzt oder erhoben werden,

sollen nach dem Entwurf kein Äquivalent für ein Entgelt darstellen, da sie nicht aktiv bereitgestellt würden. Das Abgrenzungskriterium der aktiven Bereitstellung erscheint fraglich, da sich hiernach nicht der ökonomische Wert von Daten bemisst. Dieser sollte aber Leitlinie zur Bestimmung eines potenziellen vertraglichen Austauschverhältnisses sein.

Unabhängig von der Diskussion der Einordnung des „Rechts an Daten“ oder „Rechts des Zugangs zu Daten“ als Inhaberschaft, Quasieigentum oder leistungsschutzähnliches Recht[142] bleibt die Frage, wem die Entscheidung über die Verwertung, d. h. die wirtschaftliche Nutzung von Daten, zufallen soll: Kann der Einzelne im Sinne des Rechts auf informationelle Selbstbestimmung aktiv über die Nutzung seiner Daten bestimmen oder muss er im Sinne eines überwiegenden Schutzrechts vor dem Eingriff Dritter geschützt werden? Im Grünbuch wird hier eine deutliche Perspektive zur wirtschaftlichen Nutzung von Daten eingenommen. „Datensouveränität“ und „digitale Privatautonomie“ stärken die Stellung des Dateninhabers als Verfügungsbefugter über „seine“, insbesondere die personenbezogenen, Daten in Anlehnung an das Prinzip der Vertragsautonomie im deutschen Zivilrecht, das die Inkongruenz der Informationsstände und beherrschbaren Sphären für den Einzelnen durch besondere Verbraucherschutzrechte auflöst.

Die Hoheit über den persönlichen Gehalt der Daten erfordert wie beim Urheberrecht das Verbleiben eines **höchstpersönlichen, unveräußerlichen Kerngehaltes** beim Dateninhaber. Dieser Kerngehalt beinhaltet die Umkehrbarkeit bestimmter Entscheidungen zur Nutzung der Daten (Reversibilität)[143] wie das Recht auf Vergessen[144], die Widerruflichkeit der Überlassung der Daten an Dritte, den Anspruch auf Information über die gespeicherten Daten und den Anspruch auf Löschung.[145] Im Übrigen stellt sich die Frage, ob das Nutzerverhalten großer Nutzergruppen von sozialen Medien wie Tinder, Instagram oder Snapshot ein wirkliches Schutzbedürfnis offenbart. Hier wird der Zugriff auf personenbezogene Daten und Bilder freiwillig einer Vielzahl von Nutzern gewährt. Teile des privaten Lebens und damit der Privatsphäre werden auf digitalen Plattformen gelebt. Wenn aber von einer Vielzahl von Nutzern Teile ihrer persönlichen Sphäre im Internet gelebt werden, sind personenbezogene Daten erforderlich. Die Prinzipien der Datensouveränität und der digitalen Privatautonomie erfordern, dieses Nutzerverhalten auf rechtmäßiger Basis möglich zu machen, unter Beachtung des unveräußerlichen Kerngehaltes der eigenen Daten.

Beide Bereiche, die Hoheit über den persönlichen Gehalt der Daten und die Hoheit über deren wirtschaftliche Verwertbarkeit, erfordern eine **selbstbestimmte und ausdrückliche Einwilligung** in die Nutzung der Daten und eine realistische Entscheidungsalternative zur Angabe der Daten. Soweit für den Bereich der wirtschaftlichen Verwertung die Daten als Entgeltsubstitut eingesetzt werden, begibt sich der Dateninhaber in ein Austauschverhältnis, auf das die **allgemeinen Regeln für Schuldverhältnisse** anzuwenden sind. Der Widerruf der Einwilligung zur Nutzung von Daten ist hierbei an die allgemeinen Regeln zur Beendigung von Verträgen je nach Rechtsnatur durch Kündigung, Aufhebung, Widerruf oder Rücktritt vom Vertrag gebunden. Hierbei sind Ansprüche auf Schadensersatz der Gegenseite denkbar. Zum anderen muss eine Beendigung von langlaufenden Verträgen, d. h. die Lösung aus einem Dauerschuldverhältnis gem. § 314 BGB, immer möglich sein. Das Beispiel Amazon Underground zeigt, wie komplex eine Rückabwicklung sein kann.[146]

Verbraucherschutz als Lösung der Informationsasymmetrien

Herstellung von Privatautonomie und Durchsetzung von Verbraucherrechten heißt nicht Verhinderung von innovativen Geschäftsmodellen durch Verbot der Nutzung von Daten. Mehr Kommerzialisierung durch Unternehmen erfordert aber mehr individuelle Kontrolle und Information der Verbraucher durch den Ausgleich von Informationsasymmetrien. Hierzu sollten standardisierte Einwilligungserklärungen für bestimmte Geschäftsmodelle und One-Pager erprobt werden.

Bei der Nutzung von Big Data können eine Vielzahl von Daten beteiligter und unbeteiligter Personen erhoben werden, die hierauf keinen Einfluss haben. Insbesondere Verbraucher haben oft keinerlei Einflussmöglichkeiten, die Datenerhebung und-verarbeitung zu verhindern, da die Datenerhebung für sie oftmals im Verborgenen, d. h. ohne die Kenntnis der Betroffenen, geschieht oder weil es äußert schwierig bis unmöglich ist, sich einer Überwachung zu entziehen. Verbraucherschutz im Wettbewerbsrecht soll bei unübersichtlichen Angeboten einen Überblick und bei komplexen Marktbedingungen Durchblick schaffen.[147] *„Datenschutz war schon immer verbraucherrelevant.“*[148] *„Es gab noch nie eine Zeit, in der Daten so sehr der Gegenstand von Geschäftsmodellen geworden sind, deshalb wird Datenschutzrecht immer stärker Verbraucherschutzrecht werden.“*[149]

Nach dem Grünbuch soll für die Zulässigkeit der Datennutzung **der vom Unternehmen kommunizierte Zweck** im Mittelpunkt stehen.[150] Hierzu ist eine Diskussion der **Hierarchie der Nutzungszwecke** erforderlich. Die Erhebung und Verarbeitung von Big Data auf digitalen Plattformen können zum einen öffentlichen Interessen dienen, z. B. im Katastrophenschutz.[151] Gleichzeitig zielen die Anwendungen im zivilen Bereich überwiegend auf gewerbliche oder sonstige private Interessen. Diese unterschiedlichen Interessenlagen sind mit dem Recht auf informationelle Selbstbestimmung, dem Recht am eigenen Bild und vielen anderen Rechten in Einklang zu bringen. Die im Grünbuch geforderte „Transparenz und Information“ von Kunden sollte insbesondere bei Verbrauchern daran gemessen werden, wie viele Informationen erforderlich sind, damit die Souveränität und Kontrolle über die eigenen Daten gewahrt und die Entscheidungsfreiheit im Marktgeschehen nicht unlauter beeinträchtigt wird. Bei einer Hierarchisierung der Nutzungszwecke kann ***mehr Kommerzialisierung mehr individuelle Kontrolle und Information*** erfordern. Diese Restriktion dient der Aufrechterhaltung eines fairen Leistungswettbewerbs. Nicht Verbot der Nutzung ist dann das Ziel, sondern Herstellung von Privatautonomie bei der Nutzung und Schutz des Verbrauchers bei einer Informations- und Kontrollinadäquanz. Unternehmen dürfen dann mehr kommerzialisieren, d. h. mehr Daten für unternehmerische Zwecke einsetzen, wenn sie dem Kunden mehr Transparenz und Kontrolle über seine Daten und deren Verwendung einräumen.

Neben einer Hierarchisierung der Nutzungszwecke bietet sich als Wertungsmaßstab auch die **Klassifizierung von Nutzungssphären** an. Leitlinie des Identity-Managements kann eine gestufte Einwilligung nach betroffenen Sphären sein. Die bisherigen Abgrenzungen des Öffentlichkeitsbegriffs, z. B. für Leistungsschutzrechte, taugen hierfür nur teilweise. Danach wird keine Öffentlichkeit hergestellt, wenn ein geschlossener, überschaubarer Nutzerkreis bzw. eine persönliche Verbundenheit besteht.[152] Soziale Netzwerke wie Facebook basieren zwar im Prinzip auf der Geschlossenheit der Nutzergruppe und dem Erfordernis der Anmeldung. Überschaubar ist die Zahl der Nutzer im Rechtssinne aber schon lange nicht mehr. Ein taugliches Abgrenzungskriterium in Bezug auf Transparenz und Kontrolle sind jedoch die ***freiwillige Anmeldung zu einem Dienst*** und die ***aktive Zustimmung zu Nutzungsbedingungen***, unabhängig von der Problematik der Durchsetzung bereits geltenden Rechts.[153]

Klarheit und Wahrheit im Wettbewerb

Das UWG bietet bei konsequenter Anwendung ausreichende Regelungen zum Schutz vor Irreführung im Wettbewerb bei digitalen Geschäftsmodellen.

Durch das UWG sollen Wettbewerber, sonstige Marktteilnehmer, Verbraucher und der Wettbewerb an sich

nach den Maßstäben eines fairen Leistungswettbewerbs geschützt werden.[154] Das Gebot der Klarheit und Wahrheit von Werbung, die Transparenz der angebotenen Waren und Dienstleistungen und der Schutz des Verbrauchers vor einem Informationsungleichgewicht sind grundlegende Prinzipien des Wettbewerbsrechts. Regelungen zur Verwendung von Daten finden sich u. a. hinsichtlich der Zulässigkeit von Werbung im Direktmarketing[155], des Anbietens von Diensten im Internet[156] und der Transparenz von Preisen[157]. Diese Regelungen sind auch Maßstab für neue Formen von Werbung und Datennutzung sowie -analyse bei digitalen Geschäftsmodellen.

So muss sich das Tracking von Nutzerverhalten zur Feststellung der individuellen Preisbereitschaft und zum **Anbieten von individuellen Preisen** an den Prinzipien der Klarheit und Wahrheit der Preise und der Preisfindung sowie der Offenlegung der diesbezüglichen Kriterien messen lassen. Soweit der Nutzer in die Verwendung seiner Daten einwilligt, ist die Datenanalyse nicht per se unzulässig, sondern genügt den Anforderungen des UWG, wenn die Kriterien der Preisfindung für den Nutzer offengelegt werden und so eine Irreführung ausgeschlossen werden kann.[158] Die zweite Grenze könnte die Schutzbedürftigkeit bestimmter Nutzergruppen wie z. B. geschäftlich unerfahrene Kunden, Kinder und Jugendliche sowie Menschen in Zwangssituationen sein, und die bewusste Ausnutzung dieser Situationen, siehe § 4a Abs. 1, Abs. 2 S. 1 Nr. 3 und S. 2 UWG. Diese Zwangssituationen sind bei Massentracking in der Regel kaum feststellbar. Ein Verstoß wird daher eher an der konkreten Handlung, der Art der beworbenen Produkte und Dienstleistungen sowie der sonstigen Kriterien des § 4a Abs. 2 UWG festzumachen sein.

Für das Anbieten von Diensten über **Plattformen** ist die Herstellung von Transparenz hinsichtlich Rolle, Produkten und Dienstleistungen, Preisen und Bedingungen erforderlich. Bezüglich der Rolle ist zunächst festzustellen, ob eigene oder fremde Dienste angeboten werden und ob auf das Angebot der Plattform überhaupt Einfluss genommen werden kann. Nur dann liegt ein Diensteanbieter vor.[159] Dann sollte eine Angabe in Bezug auf das Anbieten von eigenen Diensten oder das bloße Vermitteln gemacht werden. Ein ausdrücklicher Hinweis im Sinne einer ***Mitteilung*** ist bei gesetzlichen Mitteilungspflichten wie denen von Versicherungsmaklern erforderlich, siehe z. B. § 11 VersVmG. „Mitteilen“ ist nach dem LG München I mehr als „Bereithalten“ (unter einem Button „Erstinformation“), es bedeutet vielmehr aktives Präsentieren, ohne dass der Kunde danach suchen muss.[160] Für Dienste ohne besondere Mitteilungspflichten sehen §§ 5, 6 TMG allerdings nur ein ***Bereithalten*** der Informationen vor (leicht erkennbar, unmittelbar erreichbar und ständig verfügbar). Hierfür ist das Bereithalten unter einem Button „Impressum“ oder „Kontakt“ ausreichend.[161]

Impulse für den Rechtsrahmen 4.0

Ob Recht 4.0 Innovationsmotor oder -hemmnis sein wird, hängt von der Kohärenz und Stringenz bei der Gestaltung der gesetzlichen Regelungen ab. Die folgenden Regelungen sind zur Konkretisierung der Rechtsrahmens für digitale Plattformen erforderlich:

- Klarstellung des ökonomischen Wertes von Daten und des Charakters als Entgelt substitutierende Gegenleistung in Austauschverhältnissen;
- bei Daten als Gegenleistung im Austauschverhältnis: Qualifizierung des Rückrufs der datenschutzrechtlichen Einwilligung als Kündigung, Rücktritt oder Widerruf des Vertragsschlusses;
- technische Konkretisierung der Verpflichtung zur Bereitstellung von Daten und Formaten;
- Ausnahmeregelungen für Start-ups und KMU bei der Erfüllung der technischen Standards mit den Anknüpfungskriterien Nutzerzahlen, Netzwerkeffekte etc.;
- Schutz der Investition in eine Datenbank durch Klarstellung der Trennung der Rechte an Daten von den Rechten des Datenbankherstellers;
- Verpflichtung der Kennzeichnung der Anbieter von Plattformen als Anbieter, Vermittler von Diensten oder Aufbereiter von Informationen;
- Zulässigkeit neuer Geschäftsmodelle ohne diskriminierende Kennzeichnungen, aber mit konsequenter Anwendung der Kriterien der Irreführung des UWG durch
  - Klarstellung der Zulässigkeit individueller Preise,
  - unter Beachtung der Kriterien des § 19 AGG und Grenze des § 4a UWG bei besonders schutzbedürftigen Kundengruppen sowie Verpflichtung zur
    - Information über Preisbestandteile und-kriterien,
    - Informationen über Quellen und dem Algorithmus zugrunde liegende Wertungs- und Ordnungskriterien bei der Aufbereitung von Informationen,
    - Information über Provisionen für die Platzierung bei Suchmaschinen oder Vergleichsportalen;
- konsequente Anwendung des Prinzips der Trennung von redaktionellem Inhalt und Werbung;
- Experimentierklauseln für bestimmte digitale Plattformen
  - zur Nutzung von Big Data aus verschiedenen Quellen und/oder
  - zu sich verändernden Zwecken,
  - bei Einsatz von standardisierten, übersichtlichen und transparenten Einwilligungserklärungen zum Ausgleich der Informationsasymmetrie und zur Kompensation der besonderen Einsatzrisiken, bei deren Einsatz sich der Nutzer auf bestimmte rechtliche Qualitätskriterien verlassen kann;
- standardisierte Einwilligungserklärungen für bestimmte Geschäftsmodelle durch Gesetz oder Branchenvereinbarung (vergleichbar der Widerrufserklärung im Fernabsatz), ggf. verbunden mit Zertifizierungsmodellen;
- Voranstellen eines One-Pagers[162] vor jede ausführliche Information zum Datenschutz.

Smart-Data-Lösungskonzepte zur technischen Durchsetzung der Zweckbindung

Datennutzungskontrolle

Von Matthias Huber, FZI Forschungszentrum Informatik

Werden personenbezogene Daten erhoben oder verarbeitet, muss der Grundsatz der Zweckbindung beachtet werden. Die verantwortliche Stelle[163] ist verpflichtet die erhobenen Daten nur für die bei der Erhebung festgelegten Zwecke[164] zu verarbeiten – sofern nicht ein gesetzlicher Ausnahmetatbestand greift. In der Praxis kann die Zweckbindung mit Mechanismen zur ***Datennutzungskontrolle (Data Usage Control)*** unterstützt werden. Hierbei wird technisch erzwungen, dass Daten nur gemäß vorab festgelegten Sicherheitsrichtlinien –sogenannten ***Policies*** – verwendet werden.

Mehr als Zugriffskontrolle

Datennutzungskontrolle ist eine Erweiterung der Zugriffskontrolle (Access Control), die regelt, wer auf welche Daten zugreifen darf. Technisch wird Zugriffskontrolle mit sogenannten Zugriffskontrollpunkten, die Zugriffsanfragen überprüfen und aufgrund einer Sicherheitsrichtlinie Zugang gewähren oder verwehren, realisiert.[165] Nachdem der Zugriff auf Daten gewährt wurde, hat das Zugriffskontrollsystem keinen weiteren Einfluss auf die Verarbeitung und Weitergabe der Daten.

An dieser Stelle bietet Datennutzungskontrolle einen Mehrwert. Mit Datennutzungskontrolle kann nicht nur geregelt werden, wer auf welche Daten zugreifen darf, sondern auch ob und wie die Daten nach erfolgtem Zugriff verarbeitet oder weitergegeben werden dürfen.[166] Somit kommt die Datennutzungskontrolle einer Realisierung der Zweckbindung deutlich näher als reine Zugriffskontrolle.

Bei der Datennutzungskontrolle wird während der Verarbeitung der Daten überprüft, ob diese erlaubt ist, und die Verarbeitung gegebenenfalls unterbunden. Technisch lässt sich beispielsweise mittels Verschlüsselung unterbinden, dass eine nicht angepasste Anwendung, die sich potenziell nicht an die Sicherheitsrichtlinie hält, die Daten verarbeiten kann. Je nach konkreter Umsetzung können Daten auch nur an angepasste Anwendungen weitergegeben oder Daten im Sinne einer Anonymisierung modifiziert werden.

Chancen und Grenzen

Eine Herausforderung bei der Datennutzungskontrolle ist die Überprüfung, ob eine Anwendung Daten potenziell verarbeiten darf. Hierfür sind Remote-Attestation-Protokolle[167] geeignet. Mit diesen können Eigenschaften eines Zielsystems, u. a. auch über dessen Software, nachgewiesen werden. Für verlässliche Beweise benötigt Remote Attestation jedoch eine vertrauenswürdige Software- und Hardware-Basis unterhalb der Ebene, über die Nachweise geführt werden sollen. Hierbei kann ein Trusted Plattform Module (TPM)[168] als Vertrauensanker dienen.

Darüber hinaus existiert, wie auch beim Digital Rights Management (DRM), die sogenannte ***analoge Lücke***. Beispielsweise können auf einem Bildschirm angezeigte Daten abgeschrieben oder abfotografiert werden. Gerade für große Datenmengen ist dies jedoch in der Regel nicht praktikabel.

Je nach Realisierung bietet Datennutzungskontrolle also nicht den stärksten theoretisch denkbaren Schutz vor unautorisierter Datenverarbeitung. Sie verhindert jedoch unabsichtliche nichtkonforme Verarbeitung und kann absichtliche nichtkonforme Verarbeitung verhindern, womit das Vertrauen und die Akzeptanz der Betroffenen erhöht werden kann.

Da auch die Benutzung von nicht personenbezogenen Daten kontrolliert werden kann, kann Datennutzungskontrolle darüber hinaus auch eingesetzt werden, um geistiges Eigentum zu schützen. Dies soll beispielsweise im Automatisierungsumfeld im Rahmen des Smart-Data-Projekts PRO-OPT erprobt werden.

Datennutzungskontrolle bei Smart Data

Werden bei Smart-Data-Anwendungen personenbezogene Daten erhoben, ist eine zu klärende Frage, wer die Sicherheitsrichtlinien spezifiziert. Dies hängt u. a. auch von der Komplexität der Notation (beispielsweise XACML) bzw. von der Benutzbarkeit des Tools ab, mit dem die Sicherheitsrichtlinien definiert und angewandt werden können. Werden Daten auf Grundlage einer Einwilligung des Betroffenen erhoben, ergibt sich die Herausforderung, dass die Policy die Einwilligung widerspiegeln muss: Die Policy darf höchstens jene Datennutzungen erlauben, in die der Betroffene wirksam eingewilligt hat. Ist dies der Fall, könnte ein durchgehendes System zur Datennutzungskontrolle Datenschutz-Audits und Risikofolgenabschätzungen erleichtern, da dank der Policys der Zweck formal festgelegt ist und technisch auf deren Einhaltung hingewirkt wird. Dies setzt jedoch ein geschlossenes System und eine durchgehende Integration von Benutzungskontrollmechanismen voraus. Durch Frameworks wie das im nächsten Beitrag vorgestellte IND²UCE wird eine solche Integration erleichtert.

Neben der technischen Sicherstellung der Zweckbindung ist es denkbar, die Rechte der Betroffenen auch durch technisch ermöglichte Transparenzsteigerung besser durchzusetzen. Mittels geeigneter Techniken zur Nachvollziehbarkeit der Datenflüsse, beispielsweise durch Watermarking (ein digitales Äquivalent zum Wasserzeichen) der personenbezogenen Daten in Verbindung mit Detektionstechniken, könnten Betroffene besser nachvollziehen, wer die Daten wie verwendet. Wie bei der Datennutzungskontrolle müssen solche Methoden jedoch von der verantwortlichen Stelle in deren Systeme integriert werden. Eine verbesserte Nachvollziehbarkeit in Bezug darauf, zu welchen Zwecken Daten tatsächlich verwendet werden, kann zu einer erhöhten Akzeptanz der Datenverarbeitung durch die Betroffenen führen. Daher könnte der Einsatz dieser Technik auch einen Erfolgsfaktor für neue Smart-Data-Innovationen darstellen.

Von IT-Sicherheitslösungen zu technischen Datenschutz

Fazit

Datennutzungskontrolle leistet mehr als reine Zugriffskontrolle und schützt Daten auch, nachdem der initiale Zugriff gewährt wurde. Somit wird ein Schutz auch während der Verarbeitung gewährleistet. Sie stellt einen sinnvollen Ansatz dar, die zweckgebundene Datenverarbeitung sicherzustellen, auch wenn ein absoluter Schutz derzeit nicht garantiert werden kann. Mit ihr können geistiges Eigentum, Betriebsgeheimnisse wie auch personenbezogene Daten geschützt werden. Sie kann als technische Maßnahme zur Sicherstellung der Zweckbindung beitragen. Bei Smart-Data-Anwendungen kann Datennutzungskontrolle die Akzeptanz und das Vertrauen Betroffener in die Verarbeitung ihrer personenbezogenen Daten erhöhen. Als technische Maßnahme zur Minimierung der Betroffenenrisiken bietet Datennutzungskontrolle gleichzeitig für Betreiber Vorteile, wie beispielsweise einfachere Risikoanalysen, Audits oder Folgeabschätzungen. Da Verstöße nach der kommenden Datenschutzgrundverordnung mit teils empfindlichen Sanktionen belegt werden können, dürfte dem Einsatz von Datenschutzkonformität unterstützenden Techniken eine bedeutende Funktion zukommen. In diesem Sinne fordert die Datenschutzgrundverordnung explizit, dass die verantwortliche Stelle nach einer Risikoabwägung geeignete technische und organisatorische Maßnahmen trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen. Zu diesen Grundsätzen gehört auch der Zweckbindungsgrundsatz.

Datennutzungskontrolle mit IND²UCE

Von Christian Jung und Denis Feth, Fraunhofer-Institut für Experimentelles Software Engineering (IESE)

Das Fraunhofer IESE befasst sich seit 2008 mit dem Forschungsfeld der Datennutzungskontrolle (englisch „Data Usage Control“). Datennutzungskontrolle ergänzt klassische Zugriffskontrollmechanismen (englisch „Access Control“) und erweitert diese mit zusätzlichen Steuerungs- und Kontrollmöglichkeiten zur Nutzungszeit. Die zugrundeliegende Idee: Der Berechtigte soll selbst bestimmen, wie seine Daten nach Zugriff genutzt werden.

Das am Fraunhofer IESE entwickelte Sicherheitsframework IND²UCE (Integrated Distributed Data Usage Control Enforcement) macht Datennutzungskontrolle für die praktische Anwendung nutzbar.

Mit Hilfe von IND²UCE können Sicherheitsrichtlinien zur Kontrolle der Datennutzung spezifiziert werden. Diese Richtlinien regeln, welche Daten von welcher Firma geöffnet, kopiert oder überhaupt genutzt werden dürfen. Zudem ist eine situationsbedingte Einschränkung möglich, beispielsweise indem Informationen innerhalb eines gesicherten Firmengeländes eingesehen werden können und außerhalb der Firma der Detailgrad der dargestellten Informationen reduziert wird.

Der Berechtigte kann also mit Hilfe von Sicherheitsrichtlinien die gewünschte Datennutzung präzise und feingranular kontrollieren. Dabei kann er einstellen, welche seiner Daten unter welchen Bedingungen wie oft gelesen, verändert, kopiert oder weitergeleitet werden dürfen. Es bestehen Möglichkeiten, spezielle (personenbezogene) Daten automatisiert zu anonymisieren, Nutzungen nur auf bestimmten Geräten oder Geräteklassen (z. B. Dienstgeräte des Dateneigentümers) zu erlauben und die Örtlichkeit bei der Datennutzung einzuschränken (z. B. nur innerhalb eines bestimmten Gebäudes oder innerhalb der Landesgrenzen). Beispielsweise müssen einzelne Datenfelder je nach Datenempfänger oder Nutzungssituation eingeblendet oder ausgeblendet werden. Dies ermöglicht es, Daten nutzer- oder geschäftsmodellspezifisch bereitzustellen und zu verarbeiten. Des Weiteren können ausgewählte Daten nach einer genau definierten Anzahl von Tagen gelöscht bzw. unbrauchbar gemacht werden, was den Missbrauch von Daten reduzieren kann.

IND²UCE-Framework

IND²UCE ermöglicht dies durch die Erweiterung der klassischen Zugriffskontrolle und steuert die Nutzung der Daten. Ein essenzieller Punkt zur Erreichung dieser Ziele sind die Analyse und der Eingriff in Datenströme, um die Verwendung der Daten je nach Nutzungssituation kontrollieren zu können. Abbildung 1 zeigt das komponentenbasierte IND²UCE-Framework, das die relevanten Komponenten zur technischen Durchsetzung von Datennutzungskontrolle beinhaltet. Es wird in die drei Schichten „Manage“, „Decide“ und „Enforce“ untergliedert.

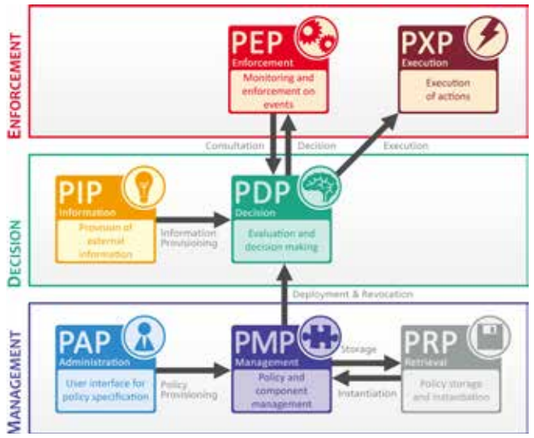


Abbildung 1: IND²UCE-Framework

Management-Layer

Policy Administration Point
Wir unterscheiden für die Spezifikation und Verwaltung der Sicherheitsrichtlinien zwei Komponenten: den Policy Management Point (PMP) und den Policy Administration Point (PAP). Der PAP ist eine Benutzerschnittstelle, die dazu dient, Sicherheitsrichtlinien auf benutzerfreundliche Art und Weise zu spezifizieren. PAPs müssen an den Wissenstand der Endanwender und die Sicherheitsbedürfnisse der Anwendungsdomäne angepasst werden. Die Sicherheitsrichtlinien werden schlussendlich in eine maschinenlesbare Form überführt.
Policy Management Point
Der PMP übernimmt die Verwaltung der spezifizierten Sicherheitsrichtlinien. Dazu gehört das Aushandeln, Aktivieren, Modifizieren und Zurückziehen von Sicherheitsrichtlinien.
Policy Retrieval Point
Der Policy Retrieval Point (PRP) bietet einen gesicherten Speicher für Sicherheitsrichtlinien. Dieser muss gegen bösartige oder versehentliche Veränderung geschützt werden. Die einzigen Komponenten mit Zugriff auf diesen Speicher sind der Policy Decision Point (PDP), um Sicherheitsrichtlinien zu beziehen, und der Policy Management Point (PMP), um Sicherheitsrichtlinien zu verwalten.

Decision-Layer

Policy Decision Point
Im Zentrum des Frameworks steht eine generische und technologieunabhängige Entscheidungskomponente (Policy Decision Point, PDP), die anhand von Sicherheitsrichtlinien über die Legitimität von sicherheitsrelevanten Ereignissen (beispielsweise Datenoperationen) entscheidet. Diese Sicherheitsrichtlinien basieren auf dem Event-Condition-Action-Paradigma und erlauben die Verwendung der Obligation Specification Language (OSL). Mit Hilfe von OSL können Verbindlichkeiten (englisch „Obligations“) spezifiziert werden (beispielsweise „Personenbezogene Daten müssen innerhalb von 14 Tagen gelöscht werden“ oder „Ohne Genehmigung des Vorgesetzten dürfen nur 10 Akten pro Stunde geöffnet werden“).
Policy Information Point
Als weitere Komponente ist der Policy Information Point (PIP) zu nennen. Diese Komponente stellt zusätzliche Informationen bereit, die für die Entscheidungsfindung im PDP benötigt werden und im Systemereignis nicht vorliegen. Zusätzliche Informationen können Daten über Informationsflüsse oder kontextabhängige Daten, wie etwa die aktuelle Lokation oder die Wi-Fi-Konnektivität eines Endgeräts, sein. Kontextsensitivität erlaubt es, Sicherheitsmechanismen nur dann scharf zu schalten, wenn diese in der Situation angebracht sind. Dies ermöglicht beispielsweise, allgemeine Verbote aufzulockern, zu denen Unternehmen sonst gezwungen sind. Aus dem allgemeinen Verbot „Smartphones sind im Unternehmen verboten, da Fotos von geheimen Informationen gemacht werden könnten“ kann eine kontextsensitive Sicherheitsrichtlinie entstehen, wie zum Beispiel „Fotos, die mit einem Smartphone innerhalb des Unternehmens aufgenommen wurden, dürfen auch nur dort angesehen werden“.

Enforcement-Layer

Policy Enforcement Point
Durchsetzungskomponenten, sogenannte Policy Enforcement Points (PEPs), sind Kontrollpunkte, die in bestehende Systeme integriert werden, um Informationsflüsse gemäß den spezifizierten Sicherheitsrichtlinien kontrollieren zu können. PEPs erfassen relevante Ereignisse auf verschiedenen Systemebenen und lassen sie (je nach Sicherheitsvorgabe) zu, modifizieren oder verwerfen sie. Hierbei können Modifikationen, wie beispielsweise Anonymisierungen oder Aggregationen von Daten, sehr feingranular und situationsbedingt gesteuert werden. PEPs müssen auf das jeweilige System angepasst werden und sind somit technologieabhängige Komponenten.

Policy Execution Point
Policy Execution Points (PXPs) können zusätzliche Aktionen wie das Löschen von Daten, das Protokollieren von Operationen oder das Versenden von Benachrichtigungen durchführen. Die Minimalkonfiguration des IND²UCE-Frameworks zur Durchsetzung von Sicherheitsrichtlinien erfordert einen PDP für die Entscheidungsfindung und einen PEP zum Durchsetzen der Entscheidung.

Das dynamische Laufzeitverhalten des Frameworks und sein komponentenbasierter Ansatz erlauben eine einfache Integration von Datennutzungskontrolle in existierende System- und Softwarelandschaften.

Anwendungsbeispiele

Wir möchten hier auf zwei Beispiele für die Anwendung von Datennutzungskontrolle eingehen, die in zwei Forschungsprojekten untersucht wurden. Dabei handelt es sich um den Einsatz im Finanzwesen und in der Cloud.

Datennutzungskontrolle mit IND²UCE im Finanzwesen

Im Finanzwesen stellen Portfoliodaten der Kunden ein höchst schützenswertes Gut dar. Im Alltagsgeschäft (z. B. bei Kundengesprächen) benötigen Anlageberater Zugriff auf diese Daten. Zunehmend findet die Beratung beim Kunden vor Ort statt und es werden mobile Endgeräte eingesetzt. Dennoch müssen die Daten angemessen geschützt werden. Die mobilen Endgeräte müssen sich deshalb an die jeweilige Nutzungssituation anpassen und Datenzugriffe entsprechend regeln. In dieser Situation essenziell sind eine automatische Erkennung der Umgebung sowie Maßnahmen zur Bestimmung der Anwesenheit des Kundenberaters und des Kunden, bevor eine Freigabe sensibler Daten erfolgt.

Im Rahmen des Software-Cluster-Projekts „SINNODIUM“[169] wurde der Demonstrator „Anlageberatung“ vom Fraunhofer IESE und von der vwd Vereinigte Wirtschaftsdienste GmbH entwickelt. IND²UCE ermöglicht es im vwd portfolio manager, mobile kontextabhängige Sicherheitsrichtlinien zu steuern.

Die Sicherheitseinstellungen des portfolio managers mobile verhalten sich unterschiedlich in Abhängigkeit von der Nutzungssituation: Im sicheren Bankenumfeld sind die Sicherheitsrichtlinien weniger restriktiv als außerhalb der Bank. Beispielsweise erfordert eine Sicherheitsrichtlinie beim Abruf von Kundendaten außerhalb der Bank die Eingabe einer MobileTAN durch den Kunden. Abbildung 2 zeigt die Anonymisierung von Kundeninformationen, die stattfindet, wenn sich der Anlageberater nicht in der Bank befindet (potenziell unsicherer Bereich) und keine oder eine falsche MobileTAN eingegeben wurde.

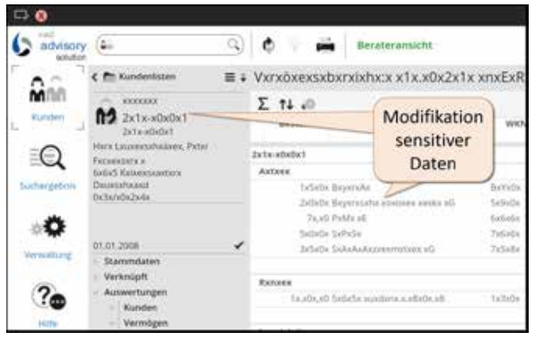


Abbildung 2: IND²UCE im Finanzwesen

Datennutzungskontrolle mit IND²UCE für die Cloud

Cloud Computing stellt für kleine und mittelständische Unternehmen eine Alternative zum eigenen Rechenzentrum dar. Allerdings bedingt die Verwendung externer Ressourcen einen Kontrollverlust in Bezug auf die eigenen IT-Anwendungen und Daten. Zudem müssen bei der Verarbeitung personenbezogener Daten rechtliche Vorgaben erfüllt werden, wie die der Speicherung von Daten im europäischen Rechtsraum. Datennutzungskontrolle bietet die Möglichkeit, Regelverletzungen aufzudecken und zu verhindern.

Im EU-Projekt SECCRIT[170] (SEcure Cloud computing for CRitical infrastructure IT) wurden seitens des Fraunhofer IESE die Erhebung und Spezifikation von Sicherheitsrichtlinien sowie deren Durchsetzung in Cloud-Umgebungen untersucht. Beispielsweise wird mit Hilfe von Sicherheitsrichtlinien in das Cloud-Management eingegriffen, um virtuelle Maschinen innerhalb der Cloud-Virtualisierung zu separieren oder den Zugriff auf Daten, z. B. von außerhalb Europas, zu regulieren. Abbildung 3 zeigt ein beispielhaftes Sicherheitsrichtlinientemplate, das im Rahmen des Projekts erhoben wurde.

ID	Policy		Asset
SU1	Data declassification on service user level		classified data
Architectural Level	Policy Creator	Security Principles	Life Cycle Phase
user level	CI service user	confidentiality	deployment, runtime

Policy Template Syntax: If <classified data> is to be sent to [<service under a specific jurisdiction> | <service outside a specific jurisdiction>], [notify <entity> | inhibit data transmission | [encrypt | anonymize | pseudonymize | remove] <sensitive attributes> from <classified data> before transmission]*.

Description: To prevent leakage of classified data, the policy enforces downgrading of the data's sensitivity or inhibition of data transmission. Where required, additional transformation mechanisms can be added to the security policy template. Examples can be found in the Sections 3.3.4 and 3.3.8 in the SECCRIT deliverable "D2.2 - Legal fundamentals" [BP13].

Threat: Unintended information leakage ([Ins13a]: VBH_WTI.5).

Exemplary Instantiation: If person-identifiable information is to be sent to a CI service outside the European Union, notify the service user and inhibit data transmission.

Abbildung 3: IND²UCE-Policy.Template aus dem EU-Projekt SECCRIT

Fazit und Ausblick

Das IND²UCE-Framework setzt Konzepte der Datennutzungskontrolle praktisch um und erlaubt es dem Dateneigentümer, feingranulare Sicherheitsrichtlinien zur Steuerung der Datennutzung zu definieren. Der modulare Aufbau des Frameworks erlaubt eine einfache Integration in bestehende Software- und Systemlandschaften.

Zukünftige Herausforderungen im Bereich der Datennutzungskontrolle umfassen u. a. die zunehmende Verwendung mobiler Endgeräte. Hierdurch wird es möglich, in unterschiedlichen Situationen auf Daten zuzugreifen. Die Sicherheitseinstellungen sollten sich dabei je nach Bedarf anpassen, um immer den bestmöglichen Schutz gewährleisten zu können. Die Eigenschaft „Kontextsensitivität“ wird für die Effizienz künftiger Sicherheitstechnologien entscheidend sein. Bei sicherheitskritischen Entscheidungen muss die Kontexterkennung mit einer gewissen Präzision erfolgen, um die Sicherheit in der jeweiligen Situation zu gewährleisten.

Eine weitere Herausforderung stellen die Erhebung und Spezifikation von Sicherheitsrichtlinien dar. Das IND²UCE-Framework verarbeitet eine maschinenlesbare Sicherheitsrichtlinie in XML-Notation. Der Spezifikationsprozess dieser XML-Dateien ist jedoch fehleranfällig und kann oft nur von Experten durchgeführt werden. Aktuelle Forschungsvorhaben am Fraunhofer IESE befassen sich deshalb mit der Erstellung von benutzerfreundlichen Schnittstellen zur Sicherheitsrichtlinienspezifikation. Ziel ist es, dass auch weniger qualifizierte Benutzer ihre Sicherheitsanforderungen adäquat und fehlerfrei spezifizieren können.

Ein weiterer wichtiger Punkt ist die Auswirkung von Sicherheitseinstellungen und-maßnahmen auf die Nutzbarkeit des Systems. Unter Umständen sind die Sicherheitsrichtlinien zu restriktiv und machen ein System unbrauchbar. Andererseits möchte man Sicherheitseinstellungen nicht zu freizügig gestalten. Das Finden der richtigen Balance zwischen Sicherheit und Nutzbarkeit und die Schaffung von Transparenz für den Endnutzer sind daher essenziell für die Gebrauchstauglichkeit des Systems.

Weitere Informationen zum Forschungsgebiet Datennutzungskontrolle und verschiedene Anwendungsvideos sind auf der Website[171] des Fraunhofer IESE zu finden.

Datenschutz durch maschinenlesbare Zertifizierung mittels XBRL

Michael Lang, Technische Universität München[172], NGCert sowie Christoph Pflügler, Maximilian Schreieck, Dr. Manuel Wiesche, Prof. Dr. Helmut Krcmar, Technische Universität München, ExCELL

Geschäftsprozesse in Unternehmen und im öffentlichen Sektor werden heute in immer komplexeren IT-Landschaften realisiert. Um einen bestimmten Geschäftsprozess umzusetzen, werden oft viele verschiedene Dienste kombiniert. Hierbei ist nicht gewährleistet, dass alle diese Dienste durch dieselbe Organisation bereitgestellt werden – im Zuge von Outsourcing-Maßnahmen bietet es sich an, Dienste externer Anbieter in Anspruch zu nehmen, um Teile ‚eines Geschäftsprozesses zu realisieren. Da hierbei gegebenenfalls sensible Daten weitergegeben werden, sollten in Frage kommende externe Anbieter besonders den Datenschutz analysieren und sicherstellen. Zertifizierungen durch dritte Parteien, wie beispielsweise Regulierungsbehörden, können die Auswahl vertrauenswürdiger Anbieter erheblich erleichtern und außerdem als rechtliche Grundlage für eine Auswahl dienen.[173]

Besonders in komplexen Dienstlandschaften mit vielen externen Anbietern ist jedoch eine manuelle Kontrolle aller Zertifikate nur mit hohem Zeitaufwand möglich. Eine Automatisierung dieses Prozesses könnte durch maschinenlesbare Zertifikate realisiert werden. Diese Zertifikate, kontrolliert durch staatlich akkreditierte Zertifizierungsstellen (vgl. Art. 43 DSGVO), können datenschutztechnische Aspekte, wie den Speicherstandort der Daten oder die verwendete Verschlüsselung, garantieren. Durch automatisierte Routinen können die Zertifikate vor jeder Inanspruchnahme eines externen Dienstes auf ihre Eignung für den jeweiligen Geschäftsprozess überprüft werden. Während eine technische Realisierung solcher Zertifikate bereits möglich ist, existiert bis heute noch kein standardisiertes einsatzfähiges Konzept zur Übermittlung der Zertifikatsinhalte. Dieser Beitrag soll die Grundzüge eines solchen Konzepts mit Hilfe des Datenübertragungsformats XBRL (eXtensible Business Reporting Language) aufzeigen. Das Konzept entstand in einer Zusammenarbeit zwischen dem Projekt ExCELL des Smart-Data-Förderprogramms und dem Projekt NGCert des Förderprogramms „Sicheres Cloud Computing“ des Bundesministeriums für Bildung und Forschung (BMBF).

Als Illustrationsbeispiel wird der physische Speicherstandort verarbeiteter Daten verwendet. Datenschutztechnisch ist dies ein relevantes Thema – so ist es beispielsweise im Zuge des sogenannten Patriot Acts der US-amerikanischen Regierung möglich, in den USA gespeicherte kundenbezogene Daten einzusehen, selbst wenn die Kunden keine US-amerikanischen Staatsbürger sind und sich auch nicht auf US-amerikanischem Territorium aufhalten. Aus diesem Grunde legt ein großer Teil deutscher Unternehmen Wert darauf, dass sensible Daten in Deutschland oder zumindest einem Land der europäischen Union gespeichert werden. Natürlich kann der Datenspeicherstandort allein keine Einhaltung aller unternehmensspezifischen Datenschutzrichtlinien garantieren. Er kann jedoch durchaus die Auswahl eines externen Diensteanbieters beeinflussen – weitere Aspekte, wie beispielsweise die verwendete Verschlüsselung oder Zugriffskontrollen, können analog zu dem illustrierten Konzept umgesetzt werden.

XBRL als Datenübertragungsformat

XBRL ist eine frei verfügbare, XML-basierte Sprache, die einen automatisierten Austausch von Daten mit Hilfe von standardisierten elektronischen Dokumenten ermöglicht. In der Praxis wird XBRL vor allem im Rahmen der Finanzberichterstattung eingesetzt. Die Grundlage aller XBRL-Dokumente bildet die XBRL-Spezifikation.[174] Sie beschreibt die Regeln und die Syntax zur Erstellung XBRL-basierter Artefakte, sogenannter Instanzen und Taxonomien. XBRL-Spezifikationen sind Erweiterungen der XML-Spezifikation, wobei jedes XBRL-Dokument auch ein valides XML-Dokument darstellt. Ein XBRL-Instanzdokument stellt eine Sammlung verschiedener Sachverhalte dar, im Beispiel dieses Artikels also den konkreten Datenspeicherstandort oder

die verwendete Verschlüsselung. Um die Vergleichbarkeit verschiedener Instanzdokumente zu ermöglichen, werden Metadaten zu den verwendeten Sachverhalten benötigt. Diese Metadaten werden in XBRL-Taxonomien gespeichert – hier wird festgelegt, welche Bedeutung den Sachverhalten zukommt, welche konkreten Werte diese annehmen können oder welche Beziehungen zwischen verschiedenen Sachverhalten bestehen. Die Deklaration eines Sachverhalts in einer Taxonomie wird auch als Konzept bezeichnet. Aus technischer Sicht ist eine XBRL-Taxonomie gleichwertig mit einem XML-Schema.

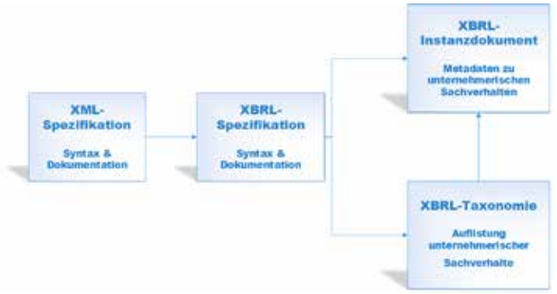


Abbildung 4: XBRL-Aufbau

Code 1, „Beispielhafte XBRL-Taxonomie“, beschreibt eine Taxonomie für den aufgezeigten Anwendungsfall. Aus Gründen der Lesbarkeit wird im Folgenden in allen Code-Beispielen auf die Deklaration der verwendeten Namespaces verzichtet.

Das Element, das den Datenspeicherstandort repräsentiert, trägt den Namen „RechenzentrumStandort“ und wird als eine Sequenz von Subelementen definiert, die die Adresse genauer beschreiben. Durch die Verwendung des Werts „stringItemType“ für das Attribut „type“ wird definiert, dass all diese Elemente durch Zeichenketten repräsentiert werden. Standardmäßig bietet XBRL zudem Unterstützung für Geldeinheiten („monetaryItemType“) sowie Zahlen- und Prozentwerte („decimalItemType“) an. Die Spezifikation erlaubt es Entwicklern außerdem, eigene Datentypen

```
<?xml version=“1.0“ encoding=“US-ASCII“?>
<xs:schema targetNamespace=
„http://www.example.com/ServiceCert“>
<!-- Aus Gründen der Lesbarkeit verzichten wir hier auf die
Deklaration der verwendeten Namespaces -->
 <xs:element name=“RechenzentrumStandort“
  id=“ServiceCert_RechenzentrumStandort“
  substitutionGroup=“xbrli:tuple“
  abstract=“false“>
   <xs:complexType>
    <xs:sequence>
     <xs:element ref=
      „ServiceCert:Street“/>
     <xs:element ref=
      „ServiceCert:BuildingNumber“/>
     <xs:element ref=
      „ServiceCert:PostalCode“/>
     <xs:element ref=
      „ServiceCert:TownCity“/>
     <xs:element ref=
      „ServiceCert:Country“/>
    </xs:sequence>
   </xs:complexType>
 </xs:element>
 <xs:element name=“Street“ id=
  „ServiceCert_Street“
  substitutionGroup=“xbrli:item“
  type=“xbrli:stringItemType“
  xbrli:periodType=“instant“/>
 <xs:element name=“BuildingNumber“ id=
  „ServiceCert_BuildingNumber“
  substitutionGroup=“xbrli:item“
  type=“xbrli:stringItemType“
  xbrli:periodType=“instant“/>
 <xs:element name=“PostalCode“ id=
  „ServiceCert_PostalCode“
  substitutionGroup=“xbrli:item“
  type=“xbrli:stringItemType“
  xbrli:periodType=“instant“/>
 <xs:element name=“TownCity“ id=
  „ServiceCert_TownCity“
  substitutionGroup=“xbrli:item“
  type=“xbrli:stringItemType“
  xbrli:periodType=“instant“/>
 <xs:element name=“Country“ id=
  „ServiceCert_Country“
  substitutionGroup=“xbrli:item“
  type=“xbrli:stringItemType“
  xbrli:periodType=“instant“/>
</xs:schema>
```

Code 1, „Beispielhafte XBRL-Taxonomie“

zu definieren. Das Attribut „periodType“ gibt den zeitlichen Kontext an, für den der Sachverhalt gültig ist – hier kann es sich um einen spezifischen Zeitpunkt („instant“) oder um eine Zeitspanne („duration“) handeln. Die konkreten Zeitdaten werden im Instanzdokument festgelegt.

Auf Basis dieser Taxonomie kann anschließend ein Instanzdokument erstellt werden. Das vollständige Ergebnis ist dem Code 2, „Beispielhaftes XBRL-Instanzdokument“, zu entnehmen. Auch an dieser Stelle wird wieder auf die Angabe der verwendeten Namespaces verzichtet.

```
<?xml version=“1.0“ encoding=“UTF-8“?>
<!-- Aus Gründen der Lesbarkeit verzichten wir hier auf die
Deklaration der verwendeten Namespaces -->
<xbrli:xbrl>
 <link:schemaRef xlink:type=“simple“
  xlink:href=“ServiceCert.xsd“/>
 <ServiceCert:RechenzentrumStandort>
  <ServiceCert:Street contextRef=
   „Anbieter1“>Cloudstrasse</ServiceCert:Street>
  <ServiceCert:BuildingNumber contextRef=
   „Anbieter1“>1</ServiceCert:BuildingNumber>
  <ServiceCert:PostalCode contextRef=
   „Anbieter1“>80331</ServiceCert:PostalCode>
  <ServiceCert:TownCity contextRef=
   „Anbieter1“>Muenchen</ServiceCert:TownCity>
  <ServiceCert:Country contextRef=
   „Anbieter1“>Germany</ServiceCert:Country>
 </ServiceCert:RechenzentrumStandort>
 <xbrli:context id=“Anbieter1“>
  <xbrli:entity>
   <xbrli:identifier scheme=
    „http://www.services.com“>
    Service Provider 1
   </xbrli:identifier>
  </xbrli:entity>
  <xbrli:period>
   <xbrli:instant>2016-01-01</xbrli:instant>
  </xbrli:period>
 </xbrli:context>
</xbrli:xbrl>
```

Code 2, „Beispielhaftes XBRL-Instanzdokument“

Zunächst wird auf die zuvor definierte Taxonomie referenziert und das dort bereitgestellte Konzept mitsamt seinen Unterkonzepten instanziiert. Über XBRL-spezifische Validierungssoftware kann jederzeit sichergestellt werden, dass das Instanzdokument den Regeln der Taxonomie folgt und beispielsweise die korrekten Datentypen verwendet werden. Im Instanzdokument wird zudem ein sogenannter Context definiert, der mit dem RechenzentrumStandort-Element verknüpft wird, um weitere Metadaten anzugeben. Hierzu gehört eine Entity, eine Organisation oder ein Individuum, auf die sich das Element bezieht und die in diesem Beispiel den Diensteanbieter darstellt. Außerdem kann der bereits erwähnte Zeitraum angegeben werden, für den der berichtete Sachverhalt gültig ist. Wie bereits in der Taxonomie definiert, handelt es sich hier um einen spezifischen Zeitpunkt, nämlich den 1. Januar 2016.

Um weitere Informationen zu unseren bereits definierten Konzepten bereitzustellen oder um Beziehungen zwischen verschiedenen Konzepten zu definieren, bietet XBRL sogenannte Linkbases an. Hierbei handelt es sich um zusätzliche XML-Dateien, die der XLink-Spezifikation folgen und in fünf Kategorien unterteilt werden: Label, Definition, Presentation, Reference und Calculation. Über die Label-Linkbase können menschenlesbare Zeichenketten als Bezeichner für bestimmte Konzepte definiert werden. Diese Bezeichner können dann in grafischen Oberflächen angezeigt werden – hiermit lassen sich Konzepte auch internationalisieren, da je Sprache verschiedene Bezeichner gewählt werden können. Mit Hilfe der Definition-Linkbase können verschiedene Beziehungen zwischen jeweils zwei Konzepten erstellt werden. Hierzu gehören hierarchische Strukturen (Parent-Child-Beziehungen) oder auch Spezialisierungen bzw. Generalisierungen. In der zuvor dargestellten Taxonomie wird beispielsweise das generische Konzept „Postal Code“ verwendet. Eine mögliche Spezialisierung für den geografischen Standort Deutschland könnte ein neues Element „Postleitzahl“ darstellen, für das wiederum besondere Validierungsregeln gelten könnten. Über die Reference-Linkbase lassen sich Verweise auf relevante Gesetzestexte oder Kommentare in externen Dokumenten wie Internetseiten oder Gesetzbüchern hinterlegen. Presentation-Linkbases beziehen sich ähnlich wie Labels auf die grafische Darstellung der Elemente. Hier können hierarchische Strukturen für die verwendeten Elemente definiert werden, die dann in grafischen Oberflächen für die Darstellung der Instanzdokumente verwendet werden können. Calculation-Linkbases zielen auf Anforderungen der Finanzbranche ab. Sie definieren vereinfacht gesagt Rechenregeln zwischen verschiedenen monetären Elementen und werden hier nicht genauer erläutert.

Das Instanzdokument kann anschließend zusammen mit der verwendeten Taxonomie sowie den gegebenenfalls benötigten Linkbase-Dateien einer staatlich akkreditierten Zertifizierungsstelle signiert und vom dazugehörigen Diensteanbieter bereitgestellt werden. Eine automatisierte Prüfung der Informationen oder ein Vergleich mit anderen Anbietern kann durch spezialisierte Software erfolgen. Auch eine manuelle Einsicht oder Kontrolle der übertragenen Daten wird durch entsprechende Software ermöglicht – da die grafische Repräsentation allein durch die standardisierten Label- und Presentation-Linkbases definiert wird, lässt sich insbesondere für diesen Anwendungsfall bereits existierende XBRL-Software verwenden.

Fazit und Ausblick

Die Eigenschaften und Konzepte der Sprache XBRL eignen sich hervorragend als Grundlage für die Übertragung maschinenlesbarer Zertifikate zum automatischen Abgleich servicerelevanter Anforderungen. Taxonomien, die von unabhängigen, vertrauenswürdigen Instanzen wie Regulierungsbehörden erstellt werden können, sorgen für Konsistenz und durchgehende Validierbarkeit der übertragenen Zertifikatsdaten und stellen somit auch die Grundlage für maschinelle Auswertung und Weiterverarbeitung dar. Auch wenn eine solche Standardisierung heute noch aussteht, würde sie die Entwicklung von Analyse- und Vergleichssoftware begünstigen. Da Zertifikate verschiedener Anbieter denselben Taxonomien folgen, können diese einfach und automatisiert miteinander verglichen werden. Bestehende Taxonomien können außerdem für Spezialfälle um zusätzliche Konzepte erweitert werden.

Durch die weite Verbreitung von XBRL im Bereich der Finanzberichterstattung existieren bereits viele Programme zur Verarbeitung von XBRL-Dokumenten. Gerade im Bereich der grafischen Darstellung gibt es hier ein großes Potenzial für eine Wiederverwendung. Aber auch bei Neuentwicklungen kann von der Popularität des XBRL durch die Verwendung von bereits existierenden und praxiserprobten Programmierschnittstellen profitiert werden. Für die Konzeption und die Entwicklung eines Bereitstellungsmechanismus für signierte Instanzdokumente und Taxonomien lohnt sich ein Blick auf das Online-Portal EDGAR Online.[175] Über EDGAR Online lassen sich Finanzberichte vieler verschiedener Unternehmen im XBRL-Format suchen und herunterladen. Eine ähnliche Plattform wäre für unsere XBRL-basierten Zertifikate denkbar – Benutzer hätten damit eine zentrale Anlaufstelle zur Verfügung, die sie für die Suche nach einem geeigneten und zertifizierten Diensteanbieter verwenden könnten.

Eine der größten Herausforderungen auf organisatorischer Ebene stellen sicherlich die Entwicklung und Einigung auf einen XBRL-basierten Datenübertragungsstandard dar, der einheitliche Taxonomien und Linkbase-Definitionen einschließt. Hier wird es wichtig sein, Diensteanbieter und Dienstekonsumenten, aber auch den Gesetzesgeber, aktiv in Entscheidungen und Diskussionen einzubeziehen, um einen übersichtlichen und nachhaltigen Datenübertragungsstandard zu entwickeln, der die Anforderungen und Bedürfnisse aller beteiligten Nutzer abdeckt.

Über die Autoren

DR. JOHANNES DREPPER

Dipl. Psych. Dr. rer. nat. Johannes Drepper, seit 2005 als wissenschaftlicher Referent in der Geschäftsstelle der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. tätig und verantwortlich für die Bereiche Datenschutz und IT. Er unterstützt die entsprechenden Arbeitsgruppen und ist an diversen IT-Projekten aus diesen Bereichen beteiligt (z. B. SAHRA-Projekt des BMWi).

DENIS FETH

... arbeitet beim Fraunhofer-Institut für Experimentelles Software Engineering (IESE) in der Abteilung Security Engineering. Seine Forschungsschwerpunkte liegen im Bereich der Datennutzungskontrolle mit Fokus auf einer benutzerfreundlichen Umsetzung von Sicherheitslösungen.

VALÉRIE GLÄSS LL.M.

Ass. jur. Valérie Gläß LL.M., seit 2015 als wissenschaftliche Referentin der Geschäftsstelle der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. im Bereich Recht und Datenschutz tätig. Als Juristin berät sie verschiedene interdisziplinäre IT-Projekte bei der rechtssicheren Nutzung von Gesundheitsdaten für die wissenschaftliche Forschung (z. B. SAHRA-Projekt des BMWi).

DR. MATTHIAS HUBER

... ist Abteilungsleiter im FZI Forschungszentrum Informatik. 2009 Abschluss des Studiums der Informatik am KIT mit anschließender Promotion. Von 2009 bis 2013 wissenschaftlicher Mitarbeiter am KIT. Seit 2013 als Abteilungsleiter im FZI. Forschungsschwerpunkte: Kryptographie und nachvollziehbare IT-Sicherheit, sichere Software-Architekturen, Datenschutz durch Technik, sicheres Datenbank-Outsourcing, Anonymitätsbegriffe und Datenbankanonymisierung.

CHRISTIAN JUNG

... leitet die Abteilung Security Engineering am Fraunhofer-Institut für Experimentelles Software Engineering (IESE) in Kaiserslautern, Deutschland. Er ist verantwortlich für das Forschungsfeld Datennutzungskontrolle, das sich mit der Durchsetzung von Sicherheitsrichtlinien zur flexiblen Steuerung der Datennutzung befasst.

PROF. DR. HELMUT KRCMAR

... ist Inhaber des Lehrstuhls für Wirtschaftsinformatik der Technischen Universität München. Seine Forschungsschwerpunkte liegen auf dem Gebiet des Informationsmanagements, der IT-ermöglichten Wertschöpfungsnetze, des Dienstleistungsmanagements, der Computer Supported Cooperative Work und der Informationssysteme für IT-Service-Provider, im Gesundheitswesen sowie im öffentlichen Bereich.

MICHAEL LANG

... ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik der Technischen Universität München und arbeitet im vom BMBF geförderten Forschungsprojekt „Next Generation Certification“ (NGCert). Herr Lang besitzt einen Master of Science with Honors in Finanz- und Informationsmanagement der Technischen Universität München und Universität Augsburg.

CHRISTOPH PFLÜGLER

... ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik der Technischen Universität München und arbeitet im vom BMWi geförderten Forschungsprojekt „ExCELL“. Herr Pflügler besitzt einen Master of Science with Honors in Finanz- und Informationsmanagement der Technischen Universität München und Universität Augsburg.

PD DR. OLIVER RAABE

... ist Leiter der Forschungsgruppe „Informationsrecht für technische Systeme und Rechtsinformatik“ am Karlsruher Institut für Technologie (KIT) und Direktor am FZI Forschungszentrum Informatik in Karlsruhe. Als habilitierter Informatiker und Jurist befasst er sich im Schwerpunkt mit der rechtlichen Beurteilung von komplexen IKT-Infrastrukturen und Fragen der Formalisierung des Rechts (Rechtsinformatik). Im Rahmen der Smart-Data-Begleitforschung leitet er gemeinsam mit Manuela Wagner die Fachgruppe Rechtsrahmen.

MAXIMILIAN SCHREIECK

... ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik der Technischen Universität München und arbeitet im vom BMWi geförderten Forschungsprojekt „ExCELL“. Herr Schreieck besitzt einen Master of Science in Technologie- und Managementorientierter Betriebswirtschaftslehre der Technischen Universität München.

PETER SCHAAR

... ist Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz und war von 2003 bis 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Er wurde mit diversen Preisen ausgezeichnet, u. a. dem Preis der Friedrich-Ebert-Stiftung „Das politische Buch“, dem Sonderpreis der deutschen Internetwirtschaft des eco Forums 2008, als erster Preisträger mit dem GDD-Datenschutzpreis und dem Louis D. Brandeis Privacy Award.

MAXIMILIAN VON GRAFENSTEIN LL.M.

... ist seit 2010 Rechtsanwalt und seit 2013 Doktorand am Humboldt Institut für Internet und Gesellschaft (HIIG). Dort leitet er im Rahmen der Forschungsgruppe Internet Entrepreneurship die Startup Law Clinic, in der junge Unternehmen aus der Internetbranche ihre Produkte und Geschäftsmodelle unter rechtlichen Gesichtspunkten analysieren und weiterentwickeln können.

MANUELA WAGNER

..., Ass. iur. Sie ist Promovendin am Zentrum für Angewandte Rechtswissenschaft des Karlsruher Instituts für Technologie (KIT). Als Mitglied der von PD Dr. Raabe geleiteten Forschungsgruppe „Informationsrecht für technische Systeme und Rechtsinformatik“ betreut sie Forschungsprojekte zu den rechtlichen Themenschwerpunkten Datenschutz- und Energierecht. Im Rahmen der Smart-Data-Begleitforschung leitet sie gemeinsam mit PD Dr. Oliver Raabe die Fachgruppe Rechtsrahmen.

PROF. DR. BEATRIX WEBER

Die Mission „Innovative Technologien rechtlich möglich machen“ lebt Frau Prof. Dr. Beatrix Weber als Leiterin der Forschungsgruppe „Recht in Nachhaltigkeit, Compliance und IT am Institut für Informationssysteme (iisys) der Hochschule für Angewandte Wissenschaften Hof. Sie forscht mit ihrem Team in interdisziplinären Projekten an der Schnittstelle zwischen Recht und IT zu Rechtsfragen der Digitalisierung, Industrie 4.0, Internet of Things und Datenschutz.

DR. THILO WEICHERT

..., Jurist und Politologe, Netzwerk Datenschutzexperte, Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e. V. (DVD), seit 1982 Tätigkeiten als Rechtsanwalt, Politiker, Hochschuldozent, Justiziar und Publizist in Freiburg i.Br., Stuttgart, Dresden und Hannover. Von 2004 bis Juli 2015 Datenschutzbeauftragter von Schleswig-Holstein und damit Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD) in Kiel.

DR. MANUEL WIESCHE

... ist Forschungsgruppenleiter am Lehrstuhl für Wirtschaftsinformatik der Technischen Universität München. Herr Wiesche schloss sein Studium der Wirtschaftsinformatik an der Westfälischen Wilhelms-Universität in Münster ab und promovierte anschließend in Wirtschaftsinformatik an der Technischen Universität München.

Mitglieder der Fachgruppe Recht

Bretfeld, Jürgen
Advaneo GmbH

Bretthauer, Sebastian
Johann Wolfgang Goethe-Universität Frankfurt am Main, Projekt Smart Regio

Bunk, Patrick
Ubermetrics GmbH, Projekt Smart Data Web

Drepper, Dr. Johannes
Leiter Arbeitsgruppe Datenschutz der Fachgruppe Rechtsrahmen, TMF e. V., Projekt SAHRA

Duisberg, Dr. Alexander
Leiter der Arbeitsgruppe Daten als Wirtschaftsgut, Bird & Bird

Eckhardt, Dr. Jens
Derra, Meyer und Partner Rechtsanwälte PartGmbB

Elteste, Thomas
DB-Systel, Projekt SD4M

Fasching, Peter
UK Erlangen, Projekt KDI

Freitag, Gerald
DB-Systel, Projekt SD4M

Fröhlich, Sven
Technische Universität Dresden, Projekt ExCELL

Gläß, Valérie LL.M.
Leiterin Arbeitsgruppe Datenschutz der Fachgruppe Rechtsrahmen, TMF e. V., Projekt SAHRA

Guzman, Liliana
Fraunhofer IESE, Projekt PRO-OPT

Hilber, Dr. Marc LL.M.
Oppenhoff & Partner

Ibbeken, Dr. Arne LL.M.
Siemens, Projekt KDI

Janneck, Kai
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Projekt iTesa

Jeske Henning
Technische Universität Dresden, Projekt ExCELL

Klein, Achim
Universität Hohenheim, Projekt InnOplan

Lenk, Dr. Alexander
BMW Group

Maier, Florian
Fraunhofer IAO, Projekt Smart Energy Hub

Meiers, Thomas
Fraunhofer HHI, Projekt sd-kama

Oppermann, Henrik
USU Software AG, Projekt SAKE

Premm, Marc
Universität Hohenheim, Projekt InnOplan

Runde, Dr. Detlef
Fraunhofer HHI, Projekt sd-kama

Schallaböck, Jan
iRights.Law Rechtsanwälte, Projekt Smart Data Web

Schlisske, Andreas
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Projekt iTesa

Spiecker genannt Döhmann, Prof. Dr. Indra LL.M.
Johann Wolfgang Goethe-Universität Frankfurt am Main, Projekt Smart Regio

Stecher, Björn
Initiative D 21

Steffen, Dr. Matthias
Bayer AG, Projekt Sidap

Stock, Sophy
FZI Forschungszentrum Informatik

Troemel, Marc
Vico research, Projekt Smart Data Web

Ursinus, Sven
BITMi Bundesverband IT-Mittelstand e. V.

von Grafenstein, Maximilian LL.M.
Alexander von Humboldt Institut für Internet und Gesellschaft

Wachovius, Juliane
Hochschule für Angewandte Wissenschaften Hof, Institut für Informationssysteme der Hochschule Hof (iisys)

Wacker, Richard
YellowMap AG

Weber, Prof. Dr. Beatrix MLE
Leiterin der Arbeitsgruppe Daten als Wirtschaftsgut, Hochschule für Angewandte Wissenschaften Hof, Projekt sd-kama

Weitzmann, John
iRights.Law Rechtsanwälte, Projekt Smart Data Web

Willkomm, Dr. Marlene
Stellvertretende Leiterin der Hochwasserschutzzentrale Köln, Projekt sd-kama

Xu, PD Dr. habil Feiyu
DFKI Deutsches Forschungszentrum für Künstliche Intelligenz, Projekt SD4M

Mitglieder der Fachgruppe Sicherheit

Gärtner, Dietmar
Software AG, Projekt sd-kama

Bogot, Kersting
Fraunhofer HHI

Eitel, Andreas
Fraunhofer IESE, Projekt PRO-OPT

Fichte, Dr. Johannes
data experts, Projekt SAHRA

Folmer, Jens
TU München, Projekt SIDAP

Freitag, Gerald
DB Systel GmbH, Projekt SD4M

Gebhardt, Dr. Marie
data experts, Projekt SAHRA

Geiß, Christian
DLR, Projekt sd-kama

Guzman, Liliana
Fraunhofer IESE, Projekt PRO-OPT

Hyka, Rüdiger
Fraunhofer IVI, Projekt iTESA

Klaes, Michael
Fraunhofer IESE, Projekt PRO-OPT

Korf, Roman
USU Software AG, Projekt SmartRegio

Maier, Florian
Fraunhofer IAO, Projekt SmartEnergyHub

Moucha, Cornelius
Fraunhofer IESE, Projekt PRO-OPT

Müller-Quade, Prof Dr. Jörn
Leiter Fachgruppe Sicherheit der Smart Data Begleitforschung, FZI

Norman Spangenberg
Universität Leipzig, Projekt InnOPlan

Pflügler, Christoph
TU München, Projekt ExCELL

Pilipchuk, Roman
Smart Data Begleitforschung, FZI

Putz, Wolfgang
Fraunhofer IESE, Projekt PRO-OPT

Rauschert, André
Fraunhofer IVI, Projekt iTESA

Sariyar, Murat
TMF e. V., Projekt SAHRA

Schwarzer, Ingo
DB Systel GmbH, Projekt SD4M

Troemel, Marc
VICO Research & Consulting GmbH, Projekt Smart Data Web

Wacker, Richard
YellowMap AG, Projekt SmartRegio

Wohlfrom, Andreas
Fraunhofer IAO, Projekt SmartEnergyHub

Fußnoten

1 Roßnagel, ZD 2013, 562; Weichert, ZD 2013, 251; Martini, DVBl 2014, 1481.

2 Mertz u. a., Studie „Digitale Selbstbestimmung“, Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres), 2016; Vodafone Institute for Society and Communication, BIG DATA – a European survey on the opportunities and risks of data analytics.

3 Hornung/Goeble, CR 2015, 265; Schwartmann/Hentsch, RDV 2015, 221; Hansen, DuD 2015, 435; Ullrich, DuD 2014, 696.

4 Kamp/Rost, DuD 2013, 80 (82); Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, S. 91; Seidel, ZG 2014, 153 (155).

5 Huber, Datennutzungskontrolle, S. 42; Jung, Datennutzungskontrolle mit Ind2uce, S.45.

6 https://www.w3.org/P3P/.

7 Bergt, ZD 2015, 365; Brink/Eckhardt, ZD 2015, 205; Hammer/Knopp, DuD 2015, 503.

8 Schneider/Enzmann/Stopczynski/Waidner, Web-Tracking-Report 2014; Karg/Thomsen, DuD 2012, 729.

9 Schefzig, K&R 2014, 772.

10 Bundestags-Drs. 14/4329 v. 13.10.2000, S. 24.

11 Bundesministerium für Wirtschaft und Energie, Leitplanken Digitaler Souveränität, 2015, S. 5, https://www.bmwi.de/BMWi/Redaktion/PDF/IT-Gipfel/it-gipfel-2015-leitplanken-digitaler-souveraenitaet,property=pdf,bereich=bmwi2012,-sprache=de,rwb=true.pdf, Abruf 16.8.2016.

12 Bundesverfassungsgericht, Urteil zum Volkszählungsgesetz v. 15.12.1983, 1. Leitsatz, BVerfGE 65, 1, S. 1.

13 Bundesverfassungsgericht, a.a.O., S. 42.

14 ebd.

15 Vgl. Matthias Huber, Datennutzungskontrolle, in dieser Publikation, S. 42 ff.

16 Thilo Weichert, Big Data – eine Herausforderung für den Datenschutz, in: Heinrich Geiselberger, Tobias Moorstedt (Red.), Big Data – Das neue Versprechen der Allwissenheit, Berlin 2013, S. 133.

17 President’s Council of Advisors on Science and Technology (PCAST), BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE, May 2014, S. 2.

18 R. Hes, John Borking, Privacy-Enhancing Technologies: The Path to Anonymity, Leiden 1995, vgl. auch: Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder (AK Technik), Datenschutzfreundliche Technologien, Schwerin 1998.

19 Vgl. Bruce Schneier, Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World, New York, London 2015, S. 199.

20 Vgl. http://www.w3.org/P3P/.

[21] Christian Jung, Denis Feth, Datennutzungskontrolle mit IND2UCE, in dieser Broschüre, S. 45.

[22] BMWi, Leitplanken Digitaler Souveränität, https://www.bmwi.de/BMWi/Redaktion/PDF/IT-Gipfel/it-gipfel-2015-leitplanken-digitaler-souveraenitaet,property=pdf,bereich=bmwi2012,-sprache=de,rwb=true.pdf, S. 5.

[23] Hansen, https://www.datenschutzzentrum.de/artikel/1000-Die-Zukunft-der-informationellen-Selbstbestimmung-mit-Datensparsamkeit-UND-digitaler-Souveraenitaet.html.

[24] BVerfGE 65, 1.

[25] Weichert/Schuler, „Datenschutz contra Wirtschaft und Big Data?“, http://www.netzwerk-datenschutzexpertise.de/autor/dr-thilo-weichert, S. 9.

[26] Ausführlich Buchner, „Informationelle Selbstbestimmung im Privatrecht“, 2006, S. 52 ff.

[27] Weichert/Schuler (Fn. 25), S. 9.

[28] BVerfGE 65, 1.

[29] BVerfGE 65, 1.

[30] Voigt in „Smart Data Geschäftsmodelle“, http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SmartData_Positionspapier_Geschaeftsmodelle.html, S. 13.

[31] Vodafone Institute for Society and Communication, „BIG DATA – a European survey on the opportunities and risks of data analytics”, Januar 2016, http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-Big-Data-Highlights-de.pdf.

[32] Vodafone (Fn. 31), S. 14.

[33] Vodafone (Fn. 31), S. 19.

[34] Wolff in Wolff/Brink, BeckOK Datenschutzrecht, Syst A. Prinzipien, Rn. 13.

[35] Artikel-29-Datenschutzgruppe, WP 203 S. 3.

[36] Wolff in Wolff/Brink (Fn. 34), Syst A., Rn. 18.

[37] Der Übersetzung als „eindeutig“ fehlen die Aspekte „ausdrücken“ und „erklären“: Artikel-29-Datenschutzgruppe, WP 203, S. 17 (Fn. 42).

[38] Artikel-29-Datenschutzgruppe, WP 203, S. 12.

[39] Wolff in Wolff/Brink (Fn34), Syst A., Rn. 19.

[40] Bizer DuD 2007, S. 350 (353).

[41] Siehe Scholz in Simitis, BDSG (8. Aufl. 2014), § 3a Rn. 51–56.

[42] BVerfGE 65, 1.

[43] Vgl. Artikel-29-Datenschutzgruppe, WP 203, S. 4.

[44] z.B. § 4 Abs. 3 Nr. 2 BDSG, § 13 Abs. 1 S. 1, § 93 Abs. 1 S. 1 TKG.

[45] Scholz/Sokol in Simitis (Fn. 41) § 4 Rn. 42.

[46] Artikel-29-Datenschutzgruppe, WP 203, S. 13.

[47] Artikel-29-Datenschutzgruppe, WP 203, S. 17.

[48] Vgl. Meldepflicht §§ 4e Nr. 4, 4d BDSG.

[49] Taeger in Taeger/Gabel, Kommentar zum BDSG (2010) § 28 BDSG, Rn. 111.

[50] Vgl. Anlage zu § 9 S. 1 BDSG.

[51] Analysis and impact study on the implementation of Directive EC 95/46 in Member States, http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf, S. 8, Wolff in in Wolff/Brink (Fn. 34) Syst A. Rn. 14.

[52] Wolff in Wolff/Brink (Fn. 34) § 28 Rn. 1.

[53] § 28 Abs. 1 S. 2 BDSG.

[54] Kramer in Auernhammer, BDSG (4. Aufl. 2014) § 28 Rn 37f.; Wolff in Wolff/Brink (Fn. 34), § 28 Rn. 17.

[55] Gola/Klug/Körffer in Gola/Schomerus, BDSG (12. Aufl. 2015) § 28, Rn. 14; Bergmann/Möhrle/Herb, BDSG (Jan. 2014) § 28 BDSG, Rn. 17–225.

[56] Simitis in Simitis, (Fn. 41), § 28 Rn. 112; Taeger in Taeger Gabel, (Fn 49), § 28 BDSG, Rn. 56.

[57] Kramer in Auernhammer, (Fn. 54) § 28 Rn. 65; Simitis in Simitis, (Fn. 41), § 28 Rn. 104–105; Taeger in Taeger/Gabel (Fn. 49) § 28 BDSG, Rn. 55.

[58] Simitis in Simitis (Fn. 41), § 28 Rn. 99.

[59] Taeger in Taeger/Gabel (Fn. 49) § 28 BDSG, Rn. 57.

[60] Simitis in Simitis (Fn. 41), § 28 Rn. 145; eine zweckungebundene Verwendungsmöglichkeit nimmt Weichert ZD 2013, 251 (255) an.

[61] Wie weit sich Beschränkungen, die an diese Kategorisierung ohne weitere Abwägung anknüpfen, im Lichte von Art. 7 (f) RL 95/46/EG halten lassen, steht angesichts des Schlussantrags des Generalanwalts Sánchez-Bordona in der Rechtssache C-582/14 (Breyer gegen BRD) erneut in Frage (siehe bereits ECJ C-468/10 und C-469/10-ASNEF gegen FECEMD).

[62] In Art. 6 (1) (b) und (c) RL 95/46/EG und Art. 5 (1) (b) und (c) DSGVO.

[63] Artikel-29-Datenschutzgruppe, WP 203, S. 4.

[64] Artikel-29-Datenschutzgruppe, WP 203, S. 1.

[65] Analysis and impact study on the implementation of Directive EC 95/46 in Member States, (Fn. 51) S. 9.

[66] Vgl. Scholz/Sokol in Simitis, (Fn. 41), § 4 Rn. 42; Bizer DuD 2007, S. 350 (352); a. A. Härting NJW 2015, 3284.

[67] Vgl. §§ 14 Abs. 2; 28 Abs. 2 und 3 BDSG. Nach § 31 BDSG dürfen Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, Datensicherung oder Betriebsführung gespeichert werden, keiner Weiterverwertung zugeführt werden, siehe Bizer DuD 2007, S. 350 (353).

[68] § 28 Abs. 2 Nr. 2 BDSG: Simitis in Simitis (Fn. 41) § 28 Rn. 182; Taeger in Taeger/Gabel (Fn. 49) § 28 BDSG Rn.137; a. A. Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 288.

[69] Im Einzelfall auch gegen den Willen des Betroffenen: Taeger in Taeger/Gabel (Fn. 49) § 28 BDSG Rn.134.

[70] Simitis in Simitis (Fn. 41) § 28 Rn. 126; Kramer in Auernhammer (Fn. 54) § 28 BDSG Rn. 71; Taeger in Taeger/Gabel (Fn. 49) § 28 BDSG Rn. 62f.

[71] Vgl. Kramer in Auernhammer (Fn. 54) § 28 BDSG Rn. 72 ff.; Taeger in Taeger/Gabel (Fn. 49) § 28 BDSG Rn. 74 ff.; Bermann/Möhrle/Herb, BDSG, § 28 Rn. 239, 243.

[72] Vgl. Moos in Taeger/Gabel, (Fn. 49), § 12 TMG Rn. 20; Schreibauer in Auernhammer (Fn. 54), § 12 TMG, Rn. 13; Spindler/Nink in Spindler/Schuster, Recht der elektronischen Medien (3. Aufl. 2015) § 12 TMG, Rn. 7.

[73] Moos in Taeger/Gabel, (Fn. 49), § 12 TMG Rn. 20; Schreibauer in Auernhammer (Fn. 54, § 12 TMG, Rn. 13; Spindler/Nink in Spindler/Schuster, (Fn. 72) § 12 TMG, Rn. 7.

[74] Siehe §§ 14, 15 TMG, § 28 Abs. 2, 3 BDSG.

[75] Z. B. § 28 Abs. 2 Nr. 1, Nr. 2 Buchst. a) BDSG.

[76] Artikel-29-Datenschutzgruppe, WP 203, S. 24, mit dem Hinweis, die Aufzählung der wesentlichen Faktoren sei weder erschöpfend noch vollständig, sondern gebe einen Überblick. Weitere Abwägungskriterien sind somit nicht ausgeschlossen.

[77] Artikel-29-Datenschutzgruppe, WP 203, S. 24 f.

[78] Artikel-29-Datenschutzgruppe, WP 203, S. 26.

[79] Artikel-29-Datenschutzgruppe, WP 203, S. 27.

[80] Taeger in Taeger/Gabel (Fn. 49) § 28 BDSG Rn. 123; Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 285.

[81] Weichert/Schuler (Fn. 25), S. 11.

[82] Norton Cybercrime Report 2011 http://us.norton.com/cybercrimereport/promo; Karger „Selbstdatenschutz Online: Die Deutschen sind die eifrigsten Schwindler", http://blog.beck.de/2010/09/13/selbstdatenschutz-online-die-deutschen-sind-die-eifrigsten-schwindler.

[83] Vodafone (Fn. 31).

[84] https://www.bmwi.de/BMWi/Redaktion/PDF/IT-Gipfel/it-gipfel-2015-leitplanken-digitaler-souveraenitaet,property=pdf,bereich= bmwi2012,-sprache=de,rwb=true.pdf.

[85] Das Grundrecht wurde vom BVerfG in folgenden Urteilen entwickelt: BVerfG-Urteil vom 15. Dezember 1983, Aktenzeichen: 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, BVerfGE 65, 1 ff. Auf europäischer Ebene bieten Art. 8 der Charta der Grundrechte der EU und Art. 16 AEUV denselben Schutz.

[86] Generische Datenschutzkonzepte für die Forschungsnetze in der Medizin, C.-M. Reng, P. Debold, Ch. Specker, K. Pommerening.

[87] Erst willigt der Patient in das beschriebene Verfahren zur weiteren Nutzung seiner Daten ein und dann wird jedes künftige Forschungsprojekt von einem Ausschuss Datenschutz geprüft und ggf. bewilligt.

[88] http://dgepi.de/fileadmin/pdf/leitlinien/GEP_mit_Ergaenzung_GPS_Stand_24.02.2009.pdf, letzter Zugriff am 05.07.2016; vgl. auch K. Pommerening, J. Drepper, K. Helbig, T. Ganslandt, Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, Generische Lösungen der TMF 2.0, S. 39 ff.

[89] http://nako.de/wp-content/uploads/2016/03/NAKO_Einwilligungserkla%CC%88rung_Level-1_v2.1.2_2016-02-09.pdf, letzter Zugriff am 05.07.2016.

[90] http://www.ak-med-ethik-komm.de/index.php?option=com_content&view=article&id=145&Itemid=154&lang=de, letzter Zugriff am 30.06.2016.

[91] Art. 9 Abs. 2 lit. a

[92] Molnár-Gábor/Korbel: Verarbeitung von Patientendaten in der Cloud – Die Freiheit translationaler Forschung und der Datenschutz in Europa, ZD 2016, S. 274.

[93] Art. 5 Abs. 1 b) EU-DSGVO: „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung")."

[94] Erwägungsgrund 50 der EU-DSGVO.

[95] Art. 89 Abs. 1 EU-DSGVO: „Die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt."

[96] Art. 6 Abs. 1 b) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr: „für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedsstaaten geeignete Garantien vorsehen."

[97] Article 29 Data Protection Working Party – Opinion 03/2013 on purpose limitation, S. 28.

[98] Vgl. Schantz: Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841, 1844.

99 Artikel-29-Datenschutzgruppe, opinion 03/2013 on purpose limitation, S. 11.

100 Eifert, Innovationsfördernde Regulierung, in: Hoffmann-Riem und Eifert (Hrsg.), Innovation und Recht II – Innovationsfördernde Regulierung, 2009, S. 11/12.

101 Siehe zum Stand der Diskussion Grafenstein DuD 2015, 789 (789).

102 Artikel-29-Datenschutzgruppe, opinion 03/2013 on purpose limitation, S. 20 ff.

103 Vgl. die wenigen Ansätze in der Literatur, die sich bisher auf den öffentlichen Sektor und dabei auf die Aufgaben der öffentlichen Verwaltung beziehen, etwa Hofmann, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes, S. 76 ff., Forgó/Krügel/Rapp, Zwecksetzung und informationelle Gewaltenteilung, S. 35 f. m. w. N.; Albers, Umgang mit personenbezogenen Informationen und Daten, in: Neue Verwaltungsrechtswissenschaft, Rz. 124, die darauf hinweist, dass die Aufgabenzuweisung nicht mit der Zweckbestimmung gleichzusetzen ist; so jetzt auch klarstellend BVerfG, 20. April 2016, 1 BvR 966/09 und 1 BvR 1140/09 (Bundeskriminalamtgesetz), Rn. 178–281; siehe aber auch Buchner, Informationelle Selbstbestimmung im Privatrecht, S. 261 ff., der im Zusammenhang mit dem Freiwilligkeitserfordernis bei der Einwilligung zumindest teilweise auf Vorschriften des BGB zurückgreift.

104 Forgó, Krügel, Rapp, Zwecksetzung und informationelle Gewaltenteilung, S. 34.

105 Vgl. Eifert, Zweckvereinbarkeit statt Zweckbindung als Baustein eines modernisierten Datenschutzes, in: Rechtswissenschaft im Wandel, Tübingen 2007, S. 151, der zumindest auf dem öffentlichen Sektor „angesichts des eng verstandenen Gesetzesvorbehalts und der Zweckbindung ein relativ gutes Abbild der Informationsströme zwischen den Verwaltungen“ für möglich hält.

106 Vgl. den Ansatz bei Albers, Umgang mit personenbezogenen Informationen und Daten, in: Neue Verwaltungsrechtswissenschaft, sowie Britz, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Offene Rechtswissenschaft, die den Datenschutz auch an anderen Freiheitsrechten ausrichten.

107 Siehe nur zum risikobasierten Ansatz in den EU-Datenschutzregimen Artikel-29-Datenschutzgruppe, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218.

108 Siehe zusammenfassend den Meinungsstand zum Verhältnis von Artikel 7 und 8 der Grundrechte-Charta, Eichenhofer, Privatheit im Internet als Vertrauensschutz, Der Staat 2016, S. 61, m. w. N.

109 Grafenstein und Schulz, The Right to be forgotten in data protection law: a search for the concept of protection, International Journal for Public Law and Policy 2015, S. 264/265.

110 Zum fehlenden Maßstab etwa Kuner, Cate, Millard, Svantesson, Lynskey, Editorial – Risk management in data protection, International Data Privacy Law, 2015, Vol. 5, No. 2; zu den aufmerksamkeitsökonomischen Gesichtspunkten v. a. Hallinan and Friedewald, Public Perception of the Data Environment and Information Transactions – A selected-survey analysis of the European public's views on the data environment and data transactions, S. 72–74.

111 Siehe etwa die Ofcom-Studie „Personal Data and Privacy“ zur Einwilligung, zuletzt heruntergeladen am 01.08.2016 unter http://www.wik.org/fileadmin/Studien/2015/Personal_Data_and_Privacy.pdf.

112 Zum Schutzbereich siehe Grafenstein DuD 2015, 789 (791).

113 Grafenstein und Schulz, a. a. O., S. 264/265.

114 Vgl. Britz, a. a. O., S. 274 ff.

115 Siehe zur Anforderung aus Artikel 6 Abs. 1 b) der Datenschutzrichtlinie 95/46/EC, die Zwecke „eindeutig“ festzulegen (bzw. nach der englischen Fassung „explizit“ zu machen), Artikel-29-Datenschutzgruppe, opinion 03/2013 on purpose limitation, S. 17 ff.

116 So auch Art. 13 Abs. 3 und Art. 14 Abs. 4 der DSGVO (EU) 2016/679.

117 Vgl. Albers, a. a. O., Rn. 124, siehe etwa auch Däubler/Klebe/Welde/Weichert, BDSG, § 4a Rn. 18.

118 Vgl. zur höheren Rechtsunsicherheit beim Einsatz rechtlicher Prinzipien allgemein etwa Eifert, Regulierungsstrategien, in: Hoffmann-Riem, Schmidt-Aßmann, Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation“, 2012, Rn. 25 und 26; Franzius, Claudio, Modalitäten und Wirkungsfaktoren der Steuerung durch Recht, in: Hoffmann-Riem, Schmidt-Aßmann, Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation“, 2012, Rn. 7, 17 und 81–103.

119 Instruktiv Eifert, a. a. O., Rn. 52 ff.; jetzt auch umfassend vorgesehen in den Artikeln 40–43 der DSGVO (EU) 2016/679.

120 Vgl. u. a. Art. 24 Abs. 3 der DSGVO (EU) 2016/679.

121 Vgl. Art. 46 Abs. 2 f) der DSGVO (EU) 2016/679.

122 Grünbuch, S. 56.

123 Grünbuch, S. 34.

124 Grünbuch, S. 32, 58.

125 Grünbuch, S. 15, 57, 60.

126 Grünbuch, S. 34.

127 Entwurf eines Neunten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen (9. GWB-ÄndG), Referentenentwurf, Bearbeitungsstand: 01.07.2016, S. 36 f., 40.

128 Entwurf RiLi COM(2015) 634 final der EU-Kommission vom 09.12.2015; Grünbuch S. 32, 58.

129 Referentenentwurf, Begründung S. 48.

130 Kritik der Monopolkommission, Hauptgutachten XXI, Wettbewerb 2016 vom 20.09.2016, S. 11.

131 Haucap, Justus: Ordnungspolitik und Kartellrecht im Zeitalter der Digitalisierung, in: Ordnungspolitische Perspektiven Nr. 77, S. 13.

132 Art. 3 Abs. 1 VO 330/2010, Art. 5 VO 461/2010 (Kfz-GVO), Kfz-Leitlinien Nr. 62–64.

133 § 20a Abs. 3 EnWG, § 20 StromGVV und GasGVV.

134 § 46 TKG.

135 Monopolkommission: Hauptgutachten XXI, Wettbewerb 2016 vom 20.09.2016, S. 11.

136 Art. 20 DSGVO: Nach ErwGr (68) sollen interoperable Formate entwickelt werden.

137 Referentenentwurf, Begründung S. 75 f.; die Monopolkommission hatte sogar einen Transaktionswert von 500 Mio. Euro empfohlen: Sondergutachten 68, Wettbewerbspolitik: Herausforderung digitale Märkte vom 01.06.2015, Tz. 461.

138 Deutscher Bundestag, Wissenschaftlicher Dienst, Horvath, Sabine: Big Data, Nr. 37/13 vom 06.11.2013, S. 1; Handelsblatt Research Institute: Big Data und Datenschutz, Studie erstellt für die Deutsche Telekom, S. 3, 10/2013.

139 Zusammengesetzt aus Dataprotection und Sustainability, siehe CeBIT 2014, www.cebit.de/de/news-trends/trends/datability/, Stand: 31.03.2014.

140 § 3a BDSG: Datenvermeidung, Art. 25 Abs. 1 DS-GVO: Datenminimierung.

141 RiLi COM(2015) 634 final der EU-Kommission vom 09.12.2015.

142 Siehe hierzu: Duisberg, Alexander: „Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Recht an Datensammlungen“, wird demnächst veröffentlicht.

143 Picot, Arnold: „Recht auf Ökonomisierung der eigenen Daten – Privatheit, Freiheit und Reversibilität“, Vortrag beim Workshop Begleitforschung Recht zu „Innovations from Smart Data“ am 08.09.2016, www.gi.de/smart-data-begleitforschung/workshops-2016/3-workshop-der-fg-recht.html.

144 EuGH-Urteil vom 13.05.2014, Rs C-131/12 und Art. 17 DSGVO.

145 Art. 20, 21 DSGVO.

146 www.amazon.de/Amazon-com-Amazon-Underground/dp/B004GJDQT8, Stand: 30.09.2016.

147 Leitbild der Bundesverbraucherzentrale, abrufbar unter: www.verbraucherzentrale.de/wir-ueber-uns, Stand: 09.10.2015.

148 Dr. Thilo Weichert, „Datenschutzrecht für den Verbraucher“, Vortrag auf der Computas-Fachkonferenz DuD 2001 am 23. und 24.04.2001 in Berlin.

149 Heiko Maas: Für den Datenschutz in der digitalen Gesellschaft – Modernes Recht aus Brüssel und Berlin!, Vortrag beim 16. Datenschutzkongress, 06.05.2015, Berlin; www.bmjv.de/SharedDocs/Reden/DE/2015/20150506_Datenschutzkongress.html.

150 Grünbuch, S. 57.

151 Siehe Programm des BMWi „Innovations from Smart Data“, Projekt sd-kama.

152 § 15 Abs. 3 UrhR, Ahlberg/Götting, in: UrhR, BeckOK, Stand: 01.07.2016, Rdn. 25.

153 Siehe den oben geschilderten Stand zu WhatsApp/Facebook.

154 § 1 und § 3 UWG.

155 § 7 Abs. 2 und 3 UWG.

156 Telemedien: §§ 5, 6, 11 f. und 13 ff. TMG.

157 § 1 ff. PAnGVO, § 3 Abs. 1 i. V. m. § 5 Abs. 1 UWG.

158 § 3 Abs. 1 i. V. m. § 5 Abs. 1 Nr. 2 bzw. § 5a Abs. 2 und 3 Nr. 3 UWG.

159 LG Heidelberg, Urteil vom 30.12.2015, Az 12 O 21/15, BeckRS 2016/04060.

160 LG München I, Urteil vom 13.07.2016, Az 37 O 152 68/15 für Versicherungsmakler mit Verpflichtung aus § 11 VersVmG.

161 BGH-Urteil vom 20.07.2006, MMR 2007, 40 f., noch für TDG: Erreichbarkeit über zwei Klicks.

162 www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2015/11192915_Vorstellung_OnePager.html.

163 Vgl. BDSG § 3 (7).

164 Vgl. Abschnitt 1.

165 Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad; Security Patterns: Integrating Security and Systems Engineering

166 A. Pretschner, M. Hilty, D. Basin, C. Schaefer, T. Walter; Mechanisms for Usage Control.

167 George Coker, Joshua Guttman, Peter Loscocco, Amy Herzog, Jonathan Millen, Brian O‘Hanlon, John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen; Principles of Remote Attestation.

168 http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/.

169 Förderkennzeichen: 01IC12S01F (BMBF).

170 SECCRIT, http://www.seccrit.eu, grant agreement no 312758.

171 Usage Control, Fraunhofer IESE, http://s.fhg.de/UC.

172 Projekt NGCert, Förderkennzeichen: 16KIS0078 (BMBF).

173 Art. 42 f. DSGVO sehen die Möglichkeit vor, mittels Zertifizierung die Einhaltung der Datenschutzvorgaben nachzuweisen. Die Zertifizierung kann sich grundsätzlich auf sämtliche datenschutzrechtlich relevanten Verarbeitungsvorgänge beziehen. So sind, wie in diesem Dokument angeregt, auch die Standardisierung und Zertifizierung von Verarbeitungszwecken denkbar, siehe Grafenstein, S. 27.

174 Vgl. https://specifications.xbrl.org/work-product-index-group-base-spec-base-spec.html

175 Vgl. http://www.edgar-online.com/.