Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

3
K&R

18. Jahrgang März 2015 Seiten 145 – 216

dfv Mediengruppe · Frankfurt am Main

Kommunikation & Recht

K&R 3/2015

RA Dr. Thomas Helbing, München*

Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung

Big Data bezeichnet die Auswertung großer Datenmengen in hoher Geschwindigkeit mit dem Ziel, diese nutzbar zu machen, meist in wirtschaftlicher Hinsicht. Die ursprünglich aus Vertragsverhältnissen oder als Metadaten angefallenen Informationen werden dabei aus ihrem Zusammenhang gerissen, neu strukturiert und mit geänderter Zielrichtung ausgewertet. Dem kann der datenschutzrechtliche Grundsatz der Zweckbindung entgegenstehen. Der Beitrag erläutert den Zweckbindungsgrundsatz gemäß der EU-Datenschutzrichtlinie, stellt deren Umsetzung im deutschen Recht dar, untersucht auf dieser Grundlage typische Fallgruppen von Big Data Anwendungen und zeigt Möglichkeiten wirtschaftlicher Nutzung.

I. Big Data und das Datenschutzrecht

1. Hintergrund und Merkmale von Big Data

Die Grundlage von Big Data bildet zum einen die enorme Menge an Daten, die heute tagtäglich anfällt und exponentiell wächst. Smartphones, Sensoren in Fahrzeugen, Stromzähler, RFID-Chips, Videokameras und die Aktivitäten von Nutzern in sozialen Netzen generieren bereits eine immense Datenflut. Zum anderen erlauben verbesserte Techniken, etwa bei Datenbanken, eine schnellere Auswertung und Analyse der Datenberge. Cloud Services ermöglichen auch kleinen Unternehmen kurzfristig bedarfsabhängig Rechner- und Speicherkapazitäten für Auswertungszwecke anzumieten.

Nach dem oben umrissenen Verständnis von Big Data zeichnet sich dieses durch vier Merkmale aus:[1]

- Datenmenge: Es werden sehr große Datenmengen verarbeitet, z. B. alle E-Mail Postfächer eines Mailanbieters, sämtliche Sensordaten einer Autoflotte, die punktgenauen historischen Positionsdaten von Handys oder alle Artikeleinkäufe einer Kaufhauskette.
- Datenvielfalt: Die Daten stammen aus unterschiedlichen Quellen und sind unstrukturiert, z. B. Texte, Stamm- und Transaktionsdaten aus Datenbanken oder Wetterdaten.
- Geschwindigkeit: Die Auswertung erfolgt in hoher Geschwindigkeit, ggf. in Echtzeit, z. B. werden Staus anhand von Handy-Bewegungsdaten erkannt oder potentielle Betrugsfälle noch während der Abwicklung einer Online-Zahlung identifiziert.
- Auswertung: Aus den Daten werden Zusammenhänge und Muster erkannt, um Vorhersagen zu treffen, z. B. anhand des Telefonierverhaltens eines Handynutzers wird das Risiko ermittelt, dass dieser zum Tarif eines Konkurrenten wechselt oder es wird die Affinität von Kunden für bestimmte Produkte anhand ihrer Online-Aktivitäten ermittelt.

Big Data Lösungen können Unternehmen helfen, fundiertere Entscheidungen zu treffen, weil sich Marktpotentiale und das Kundenverhalten besser abschätzen lassen. Dem Marketing und Vertrieb erlaubt Big Data eine bessere Kundensegmentierung und -ansprache und so Streuverluste bei Werbung zu reduzieren. Der Logistik und Warenverteilung kann Big Data helfen, Abläufe und Prozesse zu optimieren und so Kosten zu senken. Schließlich können Big Data Anwendungen der Betrugsprävention und dem Erkennen sonstiger Unternehmens-Risiken dienen.

2. Datenschutzrechtliche Herausforderungen bei Big Data

In einer repräsentativen Befragung von Unternehmen in Deutschland gaben 48 % datenschutzrechtliche Bestimmungen als Einsatzhemmnis für ihre Big Data Projekte an.[2]

Das Ergebnis überrascht nicht. Im Zusammenhang mit Big Data sind vielfältige datenschutzrechtliche Fragen zu beantworten:[3] Liegen überhaupt personenbezogene Daten vor? Was ist die Rechtsgrundlage der Verarbeitung? Dürfen Daten „auf Vorrat" gespeichert werden? Wie lange? Wie können Auskunftsrechte und Transparenzanforderungen umgesetzt werden?

Zur Untersuchung der datenschutzrechtlichen Zulässigkeit ist ein Big Data Projekt in die verschiedenen Phasen der Datenerhebung, Verarbeitung und Nutzung zu zerteilen. Für jede Phase ist zu fragen, ob personenbezogene Daten vorliegen und ob eine Einwilligung der Betroffenen vorliegt oder sonstige Erlaubnisnormen die Datenverwendung gestatten. Je nach Art und Herkunft der Daten können unterschiedliche Regelungsbereiche einschlägig sein, etwa das Telemediengesetz für Daten aus Apps oder von Webseiten, das Telekommunikationsgesetz für Verbindungsdaten von Smartphones oder das BDSG für Daten aus Kaufverträgen mit Kunden. Sondervorschriften bestehen zudem für besondere Arten von Daten, die Nutzung von

* Mehr über den Autor erfahren Sie auf S. VIII.

1 BITKOM, „Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte" (2012) S. 19, 21, abrufbar unter http://www.bitkom.org/files/documents/BITKOM_LF_big_data_2012_online%281%29.pdf (15. 2. 2015).

2 BITKOM, „Potenziale und Einsatz von Big Data", 5. 5. 2014, S. 16, abrufbar unter http://www.bitkom.org/files/documents/Studienbericht_Big_Data_in_deutschen_Unternehmen.pdf.

3 Siehe etwa *Weichert*, ZRP 2014, 168; *Roßnagel*, ZD 2013, 562; *Weichert*, ZD 2013, 251; *Katko/Babaei-Beigi*, MMR 2014, 360; *Ohrtmann/Schwiering*, NJW 2014, 2984.

Daten für Werbezwecke, dem Scoring und automatisierten Einzelfallentscheidungen.

Vorliegender Beitrag untersucht das Thema Big Data indes auf Basis des Zweckbindungsgrundsatzes. Die datenschutzrechtliche Besonderheit bei Big Data Projekten liegt nämlich in erster Linie darin, dass Daten aus ihrem ursprünglichen Zusammenhang gerissen werden und für „neue Zwecke" verarbeitet werden sollen.

II. Der Zweckbindungsgrundsatz auf Europäischer Ebene

Art. 6 Abs. 1 Buchstabe b) der EU-Datenschutzrichtlinie 95/46/EG legt den Zweckbindungsgrundsatz als grundlegendes Prinzip jeder Datenverarbeitung fest.[4] Der Zweckbindungsgrundsatz hat nach dem Wortlaut der Vorschrift zwei Aspekte. Personenbezogene Daten dürfen

1) nur „für festgelegte eindeutige und rechtmäßige Zwecke erhoben" werden (Zweck-Festlegung), und

2) „nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden" (kompatible Nutzung).

In den Mitgliedstaaten wurden diese Bestimmungen teils sehr unterschiedlich ausgelegt, weshalb die Art. 29-Arbeitsgruppe 2013 ihre Auffassung zum Zweckbindungsgrundsatz in einer 70-seitigen, bisher nur in Englisch veröffentlichten Stellungnahme ausgedrückt hat.[5] Die Art. 29-Arbeitsgruppe ist ein unabhängiges Beratungsgremium auf EU Ebene, in dem Vertreter der nationalen Datenschutzbehörden sitzen. Die Stellungnahme ist zwar nicht bindend, hat aber grundlegende Relevanz für alle Big Data Projekte und bisher nicht die ihr gebührende Resonanz und Auseinandersetzung gefunden.

1. Zweck-Festlegung

Die Festlegung des Zwecks der Datenverarbeitung bildet den Maßstab für die Einhaltung weiterer Datenschutzgrundsätze: Nur wenn der Zweck der Datenverwendung feststeht, können die Anforderungen an eine angemessene Verwendung, die Datenqualität, die Aufbewahrungsfristen und sonstige Schutzmaßnahmen bestimmt werden.

Gemäß dem Grundsatz der Zweck-Festlegung dürfen personenbezogene Daten nur für „festgelegte eindeutige und rechtmäßige Zwecke" erhoben werden.

Der Zweck ist nach der Auslegung der Art. 29-Arbeitsgruppe festgelegt, wenn er so klar definiert ist, dass sich daraus die notwendigen Schutzmaßnahmen ableiten lassen.[6] Die verantwortliche Stelle muss sich also vor der Erhebung überlegen, wofür sie die Daten verwenden will und dies mit einem Detailgrad dokumentieren, der später eine Prüfung der Zulässigkeit der Verarbeitung und etwaiger Schutzmaßnahmen ermöglicht. Allgemeine Bestimmungen wie die „Verbesserung des Nutzungserlebnisses", „IT-Sicherheit" oder „zukünftige Untersuchungen" sollen nicht ausreichen.[7] Die Festlegung kann zum Beispiel in Datenschutzhinweisen erfolgen.

Eindeutig ist der Zweck nach Ansicht der Arbeitsgruppe, wenn er unmissverständlich und deutlich festgelegt ist und nach außen hin zum Ausdruck gebracht wurde.[8] Innere Absichten, Vorstellungen und Wünsche der verantwortlichen Stelle sollen keine „eindeutig" festgelegten Zwecke darstellen.

Maßgeblich ist der Betroffenenhorizont: Für den durchschnittlich Betroffenen muss absehbar sein, wofür die Daten verwendet werden und wofür nicht. Es dürfen keine Zweifel bestehen. Mehrdeutige Auslegungen sind auszuschließen. Dem Betroffenen soll eine informierte Entscheidung möglich sein, ob er seine Daten der verantwortlichen Stelle anvertraut.

Wurden die Zwecke nicht kommuniziert oder sind sie missverständlich oder undeutlich, so sollen alle tatsächlichen Begebenheiten, das allgemeine Verständnis sowie die generellen Erwartungen der Betroffenen zur Zweckbestimmung herangezogen werden.[9]

Rechtmäßig ist der Zweck schließlich, wenn er mit dem Recht vereinbar ist. Das umfasst nicht nur das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt. Vielmehr müssen die Verwendungszwecke auch mit sonstigem Recht im Einklang stehen, etwa Antidiskriminierungs-Gesetzen, Verbraucherschutzgesetzen und dem Arbeitsrecht.[10]

2. Kompatible Nutzung

Der Grundsatz der kompatiblen Nutzung besagt: Daten dürfen nach ihrer Erhebung nicht in einer mit der ursprünglichen Zweckbestimmung unvereinbaren Weise weiterverarbeitet werden. Die späteren Nutzungszwecke müssen also mit der ursprünglichen Zweckfestlegung kompatibel sein. Vergleichsmaßstab ist die Zweckbestimmung bei der Erhebung, das heißt der allerersten Phase der Datenverwendung.

In der Datenschutzrichtlinie ist der Grundsatz der kompatiblen Nutzung als doppelte Verneinung formuliert. Es heißt sinngemäß: „inkompatible Nutzungen sind verboten", statt „es sind nur kompatible Nutzungen zulässig". Dies kann nach Auffassung der Art. 29-Arbeitsgruppe dahingehend verstanden werden, dass eine gewisse Flexibilität bei der Zweckänderung gewährt wird.[11] Der Zweckbindungs-Grundsatz bindet die spätere Nutzung also nicht strikt an den ursprünglichen Zweck. Änderungen können durchaus zulässig sein. Besser wäre daher die Bezeichnung „Zweckbeschränkungsgrundsatz".

Anhand der nationalen Datenschutzgesetze und der Verwaltungspraxis in den Mitgliedstaaten hat die Art. 29-Arbeitsgruppe einen Kriterienkatalog aufgestellt:[12]

a) Kriterium 1: Zusammenhang zwischen dem ursprünglichen und dem späteren Verwendungszweck

Im Rahmen dieses Prüfkriteriums ist zu fragen, ob der spätere Verwendungszweck bei der Erhebung mehr oder weniger schon impliziert war, die Verwendung für den späteren Zweck also einen absehbaren nächsten Schritt darstellt. In diesem Fall ist der Verwendungszweck kompatibel. Wenn sich der spätere Verwendungszweck nicht oder nur in Randbereichen mit dem ursprünglichen deckt, soll dies dagegen eine Inkompatibilität indizieren.

Vergleichsmaßstab für die Kompatibilitätsprüfung ist dabei der bei Erhebung festgelegte Zweck, nicht der Zweck, für den die Daten tatsächlich zuerst verwendet wurden.

4 Die Zweckbestimmung als wesentliche Voraussetzung der Datenverarbeitung hat bereits das BVerfG im Volkszählungsurteil erkannt, BVerfG, 15. 12. 1983 – 1 BvR 209/83, BVerfGE 65, 43.
5 Art. 29-Arbeitsgruppe, „Opinion 03/2013 on purpose limitation" (WP 203), 2. 4. 2013.
6 Art. 29-Arbeitsgruppe, WP 203, S. 15.
7 Art. 29-Arbeitsgruppe, WP 203, S. 16.
8 Art. 29-Arbeitsgruppe, WP 203, S. 17.
9 Art. 29-Arbeitsgruppe, WP 203, S. 19.
10 Art. 29-Arbeitsgruppe, WP 203, S. 19 f.
11 Art. 29-Arbeitsgruppe, WP 203, S. 21.
12 Art. 29-Arbeitsgruppe, WP 203, S. 23 ff.

Abzustellen ist nicht formal auf den Wortlaut der Zweck-Festlegung, sondern auf die tatsächlichen Begebenheiten und das allgemeine Verständnis der Beteiligten zum Erhebungszeitpunkt.

b) Kriterium 2: Kontext, in dem die personenbezogenen Daten ursprünglich erhoben wurden und die vernünftigen Erwartungen der Betroffenen

Entscheidend bei diesem Kriterium soll die Frage sein, ob ein durchschnittlicher Betroffener mit der Verwendung für den späteren Zweck zum Zeitpunkt der Erhebung gerechnet hat. Ist der spätere Verwendungszweck üblich und allgemein akzeptiert, so spricht dies für eine Kompatibilität. Eine wichtige Rolle spielt dabei die Transparenz, nämlich ob und wie der Betroffene bei der Erhebung oder auch später über die Nutzungszwecke informiert wurde.

Auch ein etwaiges Ungleichgewicht zwischen den Betroffenen und der verantwortlichen Stelle soll berücksichtigt werden. Wenn der Betroffene zur Preisgabe seiner Daten bei der Erhebung gesetzlich verpflichtet war oder faktisch keine Alternative hatte, so sind neue Nutzungszwecke tendenziell als inkompatibel anzusehen. Beruht dagegen die spätere Datenverwendung auf einer gesetzlichen Verpflichtung, so soll eher von einer Kompatibilität ausgegangen werden dürfen.

c) Kriterium 3: Die Art der Daten und die Auswirkungen der neuen Verwendung auf die Betroffenen

Je sensibler die Daten sind, desto eher soll eine spätere Verwendung für einen anderen Zweck mit dem ursprünglichen Zweck inkompatibel sein. Dies gelte insbesondere bei besonderen Arten von Daten, biometrischen oder genetischen Daten, Kommunikationsdaten und Standortdaten.

Daneben sind die Auswirkungen der neuen Zweckverwendung für die Betroffenen zu berücksichtigen und zwar positive wie negative. Negative Auswirkungen können etwa ein Ausschluss von Leistungen, die Diskriminierung oder selbst eine emotionale Beeinträchtigung durch den Verlust der Kontrolle über personenbezogene Daten sein.

Relevant ist vor allem die Art der späteren Datenverwendung. Erfolgt diese durch eine andere verantwortliche Stelle, werden Daten veröffentlicht oder mit unvorhersehbaren Folgen weiterverarbeitet oder werden große Datenmengen miteinander kombiniert, so soll dies tendenziell gegen eine kompatible Nutzung sprechen. Auch alternative Formen der Datenverarbeitung, die die Zwecke der verantwortlichen Stelle in gleicher Weise erfüllen aber für den Betreffenden schonender sind, müssen berücksichtigt werden.

d) Kriterium 4: Von der verantwortlichen Stelle getroffene Schutzmaßnahmen zur Verhinderung unangemessener Datenverwendungen und nachteiliger Auswirkungen auf die Betroffenen

Schließlich sind bei der Kompatibilitäts-Prüfung Maßnahmen zu berücksichtigen, die die verantwortliche Stelle zum Schutz der Betroffenen ergriffen hat. Solche Maßnahmen sind gemäß Art. 29-Arbeitsgruppe typischerweise eine Anonymisierung oder Pseudonymisierung oder das Aggregieren von Daten. Auch eine erhöhte oder nachgeholte Transparenz der Datenverarbeitung kann berücksichtigt werden, ebenso, wenn dem Betroffenen ein Widerspruchsrecht eingeräumt wird oder die Zustimmung zur Nutzung für den neuen Zweck eingeholt wird. Als Schutzmaßnahme kommt auch eine funktionale Trennung in Betracht, bei der durch interne Maßnahmen sichergestellt wird, dass die Daten nicht für personenbezogene Maßnahmen oder Entscheidungen genutzt werden.

Der Kompatibilitäts-Test besteht aus einer Berücksichtigung und Gewichtung aller oben genannter Faktoren. Im Ergebnis können also geeignete Schutzmaßnahmen durchaus auch größere oder überraschende Zweckänderungen legitimieren.

III. Der Zweckbindungsgrundsatz im deutschen Recht

Im Folgenden wird die Verankerung des Zweckbindungsgrundsatzes im deutschen Recht aufgezeigt.[13]

1. Der Grundsatz der Zweck-Festlegung im deutschen Recht

Der Grundsatz der Zweck-Festlegung kommt im BDSG und TMG an verschiedenen Stellen zum Ausdruck: Nach § 28 Abs. 1 S. 2 BDSG sind bei der Erhebung personenbezogener Daten die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, „konkret festzulegen". Nach § 4 Abs. 3 S. 1 Nr. 2 BDSG ist der Betroffene bei der Erhebung der Daten von der verantwortlichen Stelle unter anderem über die Zweckbestimmungen zu unterrichten, wenn er nicht bereits auf andere Weise Kenntnis davon erlangt hat. Daneben hat die Zweck-Festlegung zum Beispiel in § 4 a Abs. 1 S. 2 BDSG (Zweckfestlegung bei Einwilligungen) und § 33 Abs. 1 S. 1 (Unterrichtung des Betroffenen bei erstmaliger Datenspeicherung ohne Kenntnis) Niederschlag gefunden. Diese Anforderungen sind im Lichte der Art. 29-Arbeitsgruppe auszulegen, insbesondere muss der Zweck nach außen deutlich werden.

Im Anwendungsbereich des TMG müssen Dienstanbieter die Nutzer zu Beginn des Nutzungsvorgangs über die Zwecke der Erhebung und Verwendung personenbezogener Daten informieren, § 13 Abs. 1 S. 1 TMG.

2. Der Grundsatz der kompatiblen Nutzung im deutschen Recht

Der zweite Aspekt des Zweckbindungsgrundsatzes, die kompatible Nutzung, kommt im deutschen Recht weniger deutlich zum Ausdruck. Nach § 28 Abs. 1 S. 1 Nr. 1 BDSG dürfen Daten aus einem Vertragsverhältnis grundsätzlich nur zweckgebunden genutzt werden, soweit dies für Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Eine Übermittlung oder Nutzung für andere Zwecke ist gemäß § 28 Abs. 2 BDSG zulässig im Falle einer positiven Interessenabwägung (Nr. 1), zur Wahrung berechtigter Interessen eines Dritten (Nr. 2 a), zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten (Nr. 2 b) sowie zur Durchführung wissenschaftlicher Forschung (Nr. 3). Das deutsche Recht erlaubt damit eine Zweckänderung auf Basis einer recht vage geregelten Abwägung von Interessen in Erlaubnisnormen.

13 Zum Zweckbindungsgrundsatz siehe: *Zezschwitz*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, 2019 ff.; *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, Einl. Rn. 113; *Heckmann*, in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 14 Rn. 22; *Roggenkamp*, in: Plath, BDSG, 2013, § 14 Rn. 20.

Wie die Art. 29-Arbeitsgruppe jedoch mehrfach betont, handelt es sich beim Zweckbindungsgrundsatz und dem Grundsatz des Verbots mit Erlaubnisvorbehalt um zwei unterschiedliche, voneinander getrennt zu beachtende Vorgaben.[14] Alleine aus dem Umstand, dass für eine Datenverarbeitung eine Einwilligung oder Erlaubnisvorschrift vorliegt, kann also nicht gefolgert werden, dass auch der Zweckbindungsgrundsatz gewahrt ist.

Der Grundsatz der „kompatiblen Nutzung" ist im BDSG nicht als generelle Anforderung der Datenverarbeitung festgelegt. Es gibt keine Vorschrift, wonach Daten nur für Zwecke verwendet werden, die mit dem bei der Erhebung festgelegten kompatibel sind. Man muss deshalb den Grundsatz der kompatiblen Nutzung mit den Maßgaben der Art. 29-Arbeitsgruppe als ungeschriebene Merkmale einschränkend aber nach hier vertretener Auffassung auch erweiternd in die entsprechenden Erlaubnisvorschriften etwa des BSDG oder TMG hineinlesen und dort bei der Auslegung der unbestimmten Rechtsbegriffe, insbesondere der Erforderlichkeitsprüfung und Interessenabwägung beachten.[15]

IV. Anwendung des Zweckbindungsgrundsatzes auf Big Data

Im Folgenden wird für zwei typische Fallkonstellationen von Big Data die Zulässigkeit nach dem Zweckbindungsgrundsatz behandelt.

1. Nutzung Makro-Ebene

In vielen Big Data Anwendungen werden personenbezogene Daten auf „Makro-Ebene" genutzt, um allgemeine Trends und Korrelationen zu erkennen und besser fundierte Geschäftsentscheidungen zu treffen. So könnte zum Beispiel eine Einzelhandelskette alle Verkaufsdaten der Vergangenheit aus ihren Läden und Online-Shops sowie sämtliche Besucher-Daten der Webseiten, Aktivitäten auf den Facebook-Fanpages des Unternehmens sowie die Nennung der Marken auf Twitter und im Internet samt verfügbaren Standortdaten zusammenführen und auf Muster und Korrelationen hin auswerten. Auf Basis der Ergebnisse werden dann Ladenstandorte ausgewählt, Sortimente umstrukturiert, Online-Shops überarbeitet oder Fernsehwerbung zielgruppenorientierter konzipiert.

Erstes Wesensmerkmal dieser Fallgruppe ist, dass zwar personenbezogene Daten Grundlage der Analyse sind, die Ergebnisse und Auswertungen aber keinen Personenbezug haben. Auch wenn unmittelbar personenidentifizierende Merkmale wie Namen, Bankverbindung oder E-Mail Adresse gelöscht werden, so dürfte häufig weiterhin eine Re-Identifikation nachträglich möglich sein und deshalb Personenbeziehbarkeit vorliegen.[16] Das Datum und die Zusammensetzung von Einkaufskörben dürften zum Beispiel bereits so markant sein, dass diese durch das Unternehmen anhand von archivierten Daten leicht wieder dem Kunden zugeordnet werden können.

Zweites Kernmerkmal der Fallgruppe ist, dass negative Auswirkungen für den Betroffenen nicht vorhanden, gering oder dem „allgemeinen Lebensrisiko" zuzurechnen sind (das im Laden kaum gekaufte Produkt wird nur noch online angeboten, Fernsehspots richten sich an berufstätige Großstädter).

Maßgeblich für die Zulässigkeit der neuen Nutzung für den neuen Zweck erscheint in dieser Fallgruppe, ob ausreichende Schutzmaßnahmen getroffen wurden, um zu verhindern, dass die Daten personenbezogen genutzt werden.[17] Solche Schutzmaßnahmen zur funktionalen Trennung können sein:

- Die Auswertung erfolgt in einem technisch getrennten und sicheren System (eigene Datenbank und eigene Rechner) sowie organisatorisch[18] getrennt (z. B. Echtdaten und Auswertungen erfolgen durch unterschiedliche Teams).
- Die Auswertung wird von einem externen Dienstleister oder einer eigens gegründeten IT-Servicegesellschaft durchgeführt.
- Zwischen der verantwortlichen Stelle und der auswertenden Gesellschaft wird ein Vertrag mit strenger Zweckbindung, Wiederverknüpfungsverbot, Vertragsstrafen und ggf. Publizitätspflichten bei Verstößen geschlossen.
- Die Einhaltung der Anforderungen wird durch einen unabhängigen Dritten regelmäßig auditiert.

Sind die Schutzmaßnahmen ausreichend streng, kann nach hier vertretener Auffassung eine Zweckänderung auch dann zulässig sein, wenn der neue Zweck ursprünglich weder explizit festgelegt, noch für die Betroffenen transparent oder absehbar war und die Betroffenen der neuen Verwendung auch nicht widersprechen können.

Denn eine Persönlichkeitsrechts-relevante negative Auswirkung für einzelne Betroffene ist nicht ersichtlich. Das Restrisiko einer unzulässigen Rückführung auf eine Einzelperson macht die Zweckänderung nicht unzulässig, solange ausreichend Schutzvorkehrungen getroffen wurden. In vielen Fällen dürfte der Zweck einer umfassenden Auswertung zwar ursprünglich nicht festgelegt gewesen sein. Der Zweckbindungsgrundsatz erlaubt aber gerade auch eine Nutzung für neue, kompatible Zwecke, wobei die Kompatibilität anhand eines Kriterienkatalogs zu bestimmen ist, bei dem Schutzmaßnahmen zu berücksichtigen sind. Zudem kann der neue Nutzungszweck auch nachträglich transparent gemacht werden.

Tatsächlich werden vergleichbare Fälle derzeit primär in Bezug auf die Frage erörtert, wann und für wen Daten Personenbezug haben.[19] Das führt häufig zu schwarz-weiß Ergebnissen, bei denen entweder alles erlaubt oder (fast) alles verboten ist. Sinnvoller wäre, die Thematik im Rahmen des Zweckbindungsgrundsatzes zu erörtern, der anhand seines Kriterienkatalogs abgestufte Ergebnisse zulässt. Problematisch bleibt dann allerdings, dass die datenschutzrechtlichen Erlaubnisnormen zum Teil statische und wenig ausgeglichene Grenzen ziehen. So dürfen etwa online erfasste Nutzungsdaten nur zur „bedarfsgerechten Gestaltung" des Online-Dienstes genutzt werden, § 15 Abs. 3 TMG, nicht aber für den Offline-Bereich. Bei sensiblen Daten (z. B. Kauf von Medikamenten) werden § 28 Abs. 6 bis 9 BDSG als abschließende Erlaubnisnormen angesehen[20] und gestatten im Rahmen ihrer engen Tatbestands-

14 Art. 29-Arbeitsgrupp, WP 203, S. 3, 12, 3.
15 Zur Ähnlichkeit der Kriterien einer Zweckänderung und Interessenabwägung vergleiche Art. 29-Arbeitsgruppe, „Opinion 06/2014 on the Nation of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" (WP 217), 9. 4. 2014, S. 23 ff.
16 Art. 29-Arbeitsgruppe, WP 203, S. 30 f.
17 Art. 29-Arbeitsgruppe, WP 203, S. 30 ff., 46.
18 Funktionale Trennung bei Datenauswertungen fordert auch *Hackenberg*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 2014 (39. EL), Ziff. 16.7 Rn. 65.
19 Etwa *Kühling/Klar*, NJW 2013, 3611; *Roßnagel*, ZD 2013, 562, 563; *Weichert*, ZD 2013, 257.
20 *Simitis*, BDSG, 8. Aufl. 2014, § 28 Rn. 298.

merkmale kaum, die differenzierten Kriterien des Zweckbindungsgrundsatzes zu berücksichtigen, obwohl die Art der Daten richtigerweise nur eines von mehreren Kriterien darstellen sollte. Hier bliebe nur, die Tatbestände im Sinne des Zweckbindungsgrundsatzes erweiternd auszulegen.[21]

2. Individualisierte Werbung

Ein weiteres Anwendungsgebiet von Big Data ist die Auswertung personenbezogener Daten mit dem Zweck, Einzelpersonen zielgerichtet zu bewerben. Im Online-Bereich ist dies klassischerweise die Einblendung von geeigneten Werbeanzeigen, wobei zuvor die demographischen Daten und potentiellen Interessen des Nutzers anhand bereits besuchter Webseiten ermittelt werden. Bei Big Data Projekten können hier Daten aus weiteren Quellen hinzukommen, etwa aus Laden-Einkäufen, Anfragen beim Kundenservice, aus Rücksendungen, der Teilnahme an Rabattaktionen oder über WLAN oder Apps ermittelte Standortdaten. Eine kleine Gruppe von Kunden wird dann mit entsprechender Einwilligung und gegebenenfalls gegen Vergütung auf ihre Vorlieben und Interessen hin befragt. Eine Software ermittelt im Anschluss anhand der Gesamtdaten statistische Zwillinge und kann so über verborgene Gemeinsamkeiten die potentiellen Vorlieben und Interessen der nicht befragten Kunden ermitteln. Diese erhalten dann passgenaue Werbung oder Vertragskonditionen.

Nach hier vertretener Auffassung ist die damit einhergehende Zweckänderung im Grundsatz zulässig, wenn die Datenverwendung ausreichend transparent gemacht wird, der Betroffene widersprechen kann und eine funktionale Trennung erfolgt.[22]

Für die Transparenz ist eine deutliche Information über die Datenarten, die Quellen und die Zusammenführung nötig. Zudem sind die Zwecke und Methoden der Auswertung mit einfachen Worten darzustellen, der bloße Begriff „Werbung“ oder „Marketing“ genügt dabei als Zweckbeschreibung nicht.[23] Eine Detaildarstellung der Algorithmen und Entscheidungskriterien erscheint dagegen in der Regel weder möglich noch für den Betroffenen hilfreich.[24] Auskunft über „berechnete“ Interessen und Vorlieben ist dem Betroffenen gemäß § 34 Abs. 1 S. 1 Nr. 1 BDSG zu gewähren. Soll die Transparenz nachträglich hergestellt werden, erscheint eine separate Kommunikation oder deutliche Hervorhebung nötig (z. B. gesonderte E-Mail, Hinweistext auf Rabattgutschein, Popup-Fenster in der App). Wurde der Zweck ausreichend konkret festgelegt und kommuniziert, kann dies auch eine längerfristige Speicherung rechtfertigen. Diese erfolgt dann gerade nicht „auf Vorrat“, sondern zweckgebunden.

Zudem ist dem Betroffenen ein Widerspruchsrecht einzuräumen. Über dieses, dessen Ausübung und die Folgen ist der Betroffene zu informieren.

Die Auswertung und Zusendung von Werbung muss darüber hinaus von der Verarbeitung für den ursprünglichen Zweck funktional getrennt sein. So kann zum Beispiel die verantwortliche Stelle dem Dienstleister A. zur Auswertung pseudonymisierte Daten, bei denen die unmittelbar identifizierenden Merkmale durch eine Kennzahl (Kundennummer) ersetzt sind, übermitteln. Das Auswertungsergebnis samt Pseudonym („Kunde 123 mag vermutlich Produkt X“) liefert Dienstleister A. an Dienstleister B. Von der verantwortlichen Stelle erhält Dienstleister B. nur das Pseudonym und die Kontaktdaten (Anschrift von Kunde 123). Dienstleister B. liefert dann die entsprechende Werbung aus (Werbebroschüre für Produkt X an Anschrift von Kunde 123). Verantwortliche Stelle und Dienstleister müssen ergänzend die oben genannten Vereinbarungen zur funktionalen Trennung treffen. Bei entsprechender Organisation könnten Dienstleister A. und B. auch interne Stellen innerhalb der verantwortlichen Stelle sein.[25]

Die beschriebenen Anforderungen entsprechen im Grundsatz dem, was bei online erfassten Nutzungsdaten für die Erstellung von „Profilen“ für Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien nach § 15 Abs. 3 TMG verlangt wird.

Die Beeinträchtigung durch die Passgenauigkeit der Werbung ist in der Regel gering, der Nutzungszweck der Daten transparent und ein Widerspruch jederzeit möglich. Missbrauch wird durch die Schutzmaßnahmen der funktionalen Trennung vermieden. Für die werbliche Ansprache selbst (E-Mail, Anruf) bleiben natürlich die Anforderungen des UWG und BDSG zu beachten.

Nach geltendem Recht steht einer Big Data Analyse von Daten in Deutschland jedoch potentiell § 28 Abs. 3 BDSG im Wege. Danach dürfen personenbezogene Daten für Zwecke der Werbung grundsätzlich nur mit einer Einwilligung verarbeitet werden. Letztlich enthält die Norm damit ein Zweckänderungsverbot in Bezug auf Werbung, das kein Spiegelbild in der EU Datenschutzrichtlinie hat. Der Begriff der Werbung wird im Rahmen des § 28 Abs. 3 BDSG sehr weit ausgelegt. Erfasst sind alle Formen der Ansprache potenzieller oder tatsächlicher Kunden.[26] Im kommerziellen Bereich soll Werbung bereits bei jedem Anpreisen von Waren und Dienstleistungen oder Unternehmenszielen vorliegen.[27] Die bloße Auswertung von Daten zur Ermittlung von Interessen für kundenspezifische Werbung, ohne den Kunden überhaupt zu kontaktieren, fiele damit wohl bereits unter den Einwilligungsvorbehalt.[28]

Zwar erlaubt das Listenprivileg des § 28 Abs. 3 S. 2 BDSG eine Nutzung auch ohne Einwilligung, jedoch gehen bei Big Data Analysen die einfließenden Daten bei weitem über die in § 28 Abs. 3 S. 2 BDSG aufgezählten Datenfelder hinaus.

Einzige Lösungsmöglichkeit bietet dann § 28 Abs. 3 S. 3 BDSG, wonach die verantwortliche Stelle für Zwecke der Werbung für eigene Angebote zu den Listendaten weitere Daten „hinzuspeichern“ darf.

In der Gesetzesbegründung heißt es hierzu: „Nach Absatz 3 S. 3 darf die verantwortliche Stelle für Zwecke der Werbung für eigene Angebote (…) zu den in S. 2 Num-

21 Für einen Rückgriff auf § 28 Abs. 2 BDSG im Rahmen des Anwendungsbereichs des TMG wohl *Arning/Moos*, ZD 2014, 242, 244.

22 A. A. wohl die Art. 29-Arbeitsgruppe, WP 203, S. 46, wonach die Nutzung für die persönliche Ansprache „nahezu immer“ einer Einwilligung bedürfe.

23 *Büllesbach*, CR 2000, 11, 14; zur Zweckfestlegung in den AGB von Apple, siehe auch LG Berlin, 30. 4. 2013 – 15 O 92/12, ZD 2013, 451.

24 Zur Transparenz des Algorithmus bei Big Data wohl anderer Ansicht Art. 29-Arbeitsgruppe, WP 203, S. 47.

25 Kritisch zur Pseudonymisierung innerhalb der verantwortlichen Stelle: *Selk*, in: Conrad/Grützmacher (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, 2014, § 30 Rn. 143 ff.

26 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 4. Aufl. 2014, § 28 Rn. 89.

27 Vgl. *Wedde*, (Fn. 26), § 28 Rn. 89; *Wolff*, in: Wolff/Brink, BDSG, 2013, § 28 Rn. 116; *Ehmann*, in: Simitis, BDSG, 7. Aufl. 2011, § 29 Rn. 80.

28 Das erscheint im Hinblick auf eine fehlende europarechtliche Stütze für das „Werbeverbot“ und aufgrund der Tatsache, dass jede unternehmerische Datenverarbeitung letztlich dem Vertrieb von Waren und Dienstleistungen dient, fragwürdig. Einschränkend *Schirmbacher/Schätzle*, WRP 2014, 1143, 1143 f.

mer 1 genannten Daten (…), die sie beim Betroffenen nach Absatz 1 S. 1 Nummer 1 erheben muss, weitere Daten hinzuspeichern. Die Beschränkung auf das ‚Hinzuspeichern' stellt klar, dass die verantwortliche Stelle die weiteren Daten gestützt auf eine andere Befugnis rechtmäßig erhoben, z. B. nach Absatz 1 S. 1 Nummer 3, oder rechtmäßig übermittelt bekommen haben muss. (…) Absatz 3 S. 3 soll es der verantwortlichen Stelle ermöglichen, einen eigenen Datenbestand, der direkt beim Betroffenen erhoben wurde, für Zwecke der Eigenwerbung (…) zu selektieren, um die bestehenden Kunden gezielter ansprechen zu können."[29]

Vor dem Hintergrund dieser gesetzgeberischen Absicht ist das Hinzuspeichern weit auszulegen und als „Hinzunutzen" zu verstehen. Auch bei einer Big Data Analyse erfolgt letztlich eine Selektion von Kunden zur gezielten Ansprache. Die Besonderheit liegt darin, dass alle Merkmale in die Selektion einbezogen werden und die Gewichtung durch Algorithmen erfolgt. Im Rahmen von § 28 Abs. 3 S. 3 BDSG kann eine Selektion jedoch richtigerweise auch anhand von mehreren Merkmalen erfolgen.[30]

Sind also die in die Auswertung einbezogenen Daten von der verantwortlichen Stelle irgendwie[31] in zulässiger Weise erhoben oder ihr rechtmäßig übermittelt worden, steht der Einwilligungsvorbehalt des § 28 Abs. 3 BDSG der Datenauswertung zur Ermittlung von Kundeninteressen nicht entgegen.[32] Einzige Zusatzanforderung ist, dass das Unternehmen die Daten für eigene Angebote nutzt. Der Betroffene bleibt durch sein gesetzliches Widerspruchsrecht nach § 28 Abs. 4 BDSG und den Vorbehalt der entgegenstehenden Interessen gemäß § 28 Abs. 3 S. 6 BDSG geschützt.

V. Fazit und Schlussbemerkung

Bei Big Data werden Daten aus ihrem ursprünglichen Zweckzusammenhang gerissen, aus verschiedenen Bereichen zusammengeführt, strukturiert, ausgewertet und neuen Nutzungen zugeführt. Der datenschutzrechtliche Zweckbindungsgrundsatz bildet dabei einen zentralen Prüfungsmaßstab für die datenschutzrechtliche Zulässigkeit. Die Art. 29-Arbeitsgruppe hat hierzu einen Katalog von Kriterien entwickelt, mit dessen Hilfe für die unterschiedlichsten Bereiche, egal ob online oder offline und unabhängig von Datenherkunft und Art, sachgerechte Ergebnisse erzielt werden können, da insbesondere Schutzmaßnahmen ausgleichend berücksichtigt werden können. In Deutschland ist der Zweckbindungsgrundsatz dagegen teilweise nicht als allgemeines Prinzip verankert und deshalb in die datenschutzrechtlichen Erlaubnisnormen hineinzulesen.

Der Autor plädiert dafür, auf Basis der Zweckbindungs-Kriterien übergreifende Maßstäbe für die Zulässigkeit von Big Data Anwendungen zu entwickeln und die unbestimmten Rechtsbegriffe in den Erlaubnisnormen in diesem Sinne auszulegen. Der Beitrag hat hierzu für die Auswertung von personenbezogenen Daten auf Makro-Ebene und zur personalisierten Werbung einen ersten Schritt geleistet. In Bezug auf personalisierte Werbung vertritt der Autor, dass die einhergehende Zweckänderung gerechtfertigt werden kann, wenn die Datenverwendung ausreichend transparent gemacht wird, der Betroffene widersprechen kann und eine funktionale Trennung erfolgt. Bei einer Werbung für eigene Angebote steht dem dann auch § 28 Abs. 3 BDSG nicht entgegen.

29 BT-Drs. 16/12011, S. 32.
30 So auch LG Augsburg, 19. 8. 2011 – 3 HK O 2827/11, ZD 2012, 476, 477; andere Ansicht zuvor OLG Köln, 19. 11. 2010 – 6 U 73/10, NJW 2012, 3312, dort unter II. 1. b); offen: Düsseldorfer Kreis, „Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke", Dezember 2013, S. 6 f.
31 LG Augsburg, 19. 8. 2011 – 3 HK O 2827/11.
32 Kritisch zur Regelung des § 28 Abs. 3 BDSG bei Kundenprofilen auch *Ohrtmann/Schwiering*, NJW 2014, 2986, 2985.

RA Dr. Uwe Schlömer und RA/FA GewRS/FA IT-Recht Jörg Dittrich, LL.M. oec., Hamburg*

eBay & Recht – Rechtsprechungsübersicht zum Jahr 2014

Der nachfolgende Beitrag setzt die Rechtsprechungsübersicht zum Jahr 2013 (Schlömer/Dittrich, K&R 2014, 228 ff.) fort. Mehrfach hatte sich die Judikatur mit der Frage zu befassen, unter welchen Voraussetzungen eine Online-Auktion vorzeitig beendet werden kann. Welche Folgen der unberechtigte Abbruch einer Online-Auktion haben kann, zeigen hierzu ergangene Urteile des BGH. Für Rechtssicherheit konnte der BGH auch bei der Frage sorgen, ob die Pflicht zur Grundpreisauszeichnung weiterhin Bestand hat. Eine neue Frage zur Haftung von eBay selbst hat das LG Köln aufgeworfen, soweit es um Pflichtangaben geht, die zwar in den Artikelangeboten der eBay-Mitglieder erscheinen, nicht jedoch in den von eBay veranlassten Werbeanzeigen für diese Angebote.

I. Vertragsabschluss und Leistungsstörungen

1. Handeln bei eBay unter fremdem Namen

Gelegentlich entsteht zwischen eBay-Mitgliedern Streit darüber, wer tatsächlich Vertragspartei geworden ist – so z. B. dann, wenn der Inhaber eines Mitgliedskontos einwendet, das Angebot nicht selbst bei eBay eingestellt zu haben. Das OLG Celle verwies auf die höchstrichterliche Rechtsprechung, der zufolge die Regelungen über die Stellvertretung gem. §§ 164 ff. BGB und die hierzu entwickelten Grundsätze entsprechende Anwendung finden, wenn bei der Nutzung eines fremden Namens der Anschein erweckt wird, es solle ein Geschäft mit dem Namensträger

* Mehr über die Autoren erfahren Sie auf S. VIII.