Verbraucher-Scoring aus Sicht des Datenschutzrechts

Domurath, I.; Neubeck, I.

Publication date
2018
Document Version
Final published version
License
Unspecified

WORKING PAPER

Verbraucher-Scoring aus Sicht des Datenschutzrechts

Irina Domurath und Irene Neubeck

SVRV Sachverständigenrat für Verbraucherfragen

Zitierhinweis für diese Publikation:
Domurath, I. & Neubeck, I. (2018). Verbraucher-Scoring aus Sicht des Datenschutzrechts.
Veröffentlichungen des Sachverständigenrats für Verbraucherfragen.
Berlin: Sachverständigenrat für Verbraucherfragen.

Berlin, Oktober 2018
Veröffentlichungen des Sachverständigenrats für Verbraucherfragen
ISSN: 2365-919X

Herausgeber:
Sachverständigenrat für Verbraucherfragen
beim Bundesministerium der Justiz und für Verbraucherschutz
Mohrenstraße 37
10117 Berlin
Telefon: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525

E-Mail: info@svr-verbraucherfragen.de
Internet: www.svr-verbraucherfragen.de

Gestaltung: Atelier Hauer+Dörfler GmbH, Berlin
Druck: bud

WORKING PAPER

Verbraucher-Scoring aus Sicht des Datenschutzrechts

Irina Domurath und Irene Neubeck

Dr. Irina Domurath ist wissenschaftliche Mitarbeiterin an der Universität von Amsterdam, Rechtswissenschaftliche Fakultät, Abteilung Privatrecht, Valckenierstraat 59, 1018 XE Amsterdam. Zuvor war sie wissenschaftliche Mitarbeiterin in der Geschäftsstelle des Sachverständigenrats für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, Mohrenstraße 37, 10117 Berlin.

Irene Neubeck hat diesen Artikel während ihrer Zeit als Mitarbeiterin in der Geschäftsstelle des Sachverständigenrats für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, Mohrenstraße 37, 10117 Berlin, erarbeitet.

Die Autorinnen danken Hans-W. Micklitz, Helga Zander-Hayat und Johannes Gerberding für hilfreiche Anmerkungen.

Mitglieder und Mitarbeitende des SVRV

Mitglieder des SVRV

Prof. Dr. Lucia Reisch (Vorsitzende)
Professorin für Interkulturelle Konsumforschung und europäische Verbraucherpolitik an der Copenhagen Business School

Dr. Daniela Büchel (stellv. Vorsitzende)
Bereichsvorstand Handel Deutschland REWE Group, Geschäftsführerin REWE Markt GmbH und Penny Markt GmbH

Prof. Dr. Gerd Gigerenzer
Direktor des Harding-Zentrums für Risikokompetenz am Max-Planck-Institut für Bildungsforschung in Berlin

Helga Zander-Hayat
Mitglied der Geschäftsleitung der Verbraucherzentrale Nordrhein-Westfalen

Prof. Dr. Gesche Joost
Professorin für das Fachgebiet Designforschung an der Universität der Künste

Prof. Dr. Hans-Wolfgang Micklitz
Professor für Wirtschaftsrecht am Europäischen Hochschulinstitut in Florenz

Prof. Dr. Andreas Oehler
Professor für Finanzwirtschaft an der Universität Bamberg und Direktor der Forschungsstelle Verbraucherfinanzen und Verbraucherbildung

Prof. Dr. Kirsten Schlegel-Matthies
Professorin für Haushaltswissenschaft an der Universität Paderborn

Prof. Dr. Dr. h.c. Gert G. Wagner
Max Planck Fellow am MPI für Bildungsforschung (MPIB) Berlin, Research Associate beim Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG) Berlin, und Senior Research Fellow bei der Längsschnittstudie Sozio-oekonomisches Panel (SOEP) am DIW Berlin

Mitarbeitende des SVRV

Leiter der Geschäftsstelle:
Thomas Fischer, M.A.

Wissenschaftlicher Stab der Geschäftsstelle:
Johannes Gerberding
Dr. Christian Groß
Dr. Ariane Keitel
Sarah Sommer, M.A.

Inhalt

I Einleitung

1. Kontext

Die Praxis des Scoring hat in den letzten Jahren immer mehr und global an Bedeutung gewonnen. Zuletzt hat die chinesische Regierung mit seinem umfassenden „Sozialkredit"-System für Aufregung gesorgt. Das Sozialkreditsystem ist ein bis 2020 fertigzustellendes Programm, das alle Bürger und Unternehmen Chinas mit einem individuellen Score versehen soll, der Ausdruck ihrer sozialen und politischen Verhaltensweisen und damit der persönlichen Reputation des Bürgers sein soll. Ziel des Programms ist, so sagt es die chinesische Regierung offen, die Förderung sozialistischer Werte und die entsprechende Honorierung von „Aufrichtigkeit" und die Bestrafung von „Unaufrichtigkeit".[1]

Aber auch außerhalb Chinas sind Scoringpraktiken bekannt und etabliert. Vor allem in der Kreditwirtschaft wird die Bonität von Kunden schon lange und routinemäßig gescort. Gesetzliche Krankenversicherungen teilen Patienten in sog. Morbiditätsgruppen ein.[2] Auch wenn verhaltensbasierte Kriterien für Krankenkassen bisher keine Rolle spielen, ist in anderen Bereichen verhaltensbasiertes Scoring durchaus bekannt. Beispielsweise haben Kfz-Versicherungen mit verhaltensbasierten Telematiktarifen Scoringpraktiken eingeführt.

Diese Entwicklungen werden durch die kontinuierlich steigenden Möglichkeiten, große Mengen personenbezogener Daten auswerten zu können (sogenannte Big-Data-Analysen) beschleunigt.[3] Big-Data-Analysen sollen Zusammenhänge erkennen, um damit umfangreichere Informationen und umfassendere Verhaltensmuster über Kunden liefern zu können. Für junge technikaffine Unternehmen sind die Möglichkeiten von Big-Data-Analysen inzwischen integraler Bestandteil neuer Geschäftsmodelle.[4]

Scoring ist spezialgesetzlich in § 10 Abs. 2 KWG für das Kreditwesen geregelt. Branchenübergreifend ist Scoring hauptsächlich im Datenschutzrecht erfasst. Im Bundesdatenschutzgesetz (BDSG)[5] stand bislang das klassische Kreditscoring im Mittelpunkt. Die Einführung der europäischen Datenschutzgrundverordnung (DSGVO) im Mai 2018 bringt Änderungen in der Regulierung des Scoring mit sich.

Konfliktpunkte betreffen oftmals den Ausgleich zwischen unternehmerischen Interessen auf der einen Seite und dem Schutz des Einzelnen vor unrechtmäßiger Nutzung seiner personenbezogenen Daten und vor Diskriminierung im Zugang zu bestimmten Leistungen auf der anderen Seite. Daten werden außerdem als Wirtschaftsgut angesehen.[6] Dies spiegelt sich auch im Datenschutzrecht wider und zieht, wie wir sehen werden, Probleme für den Schutz des Persönlichkeitsrechts des Einzelnen nach sich.

---

1 https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (zuletzt abgerufen am 17.06.2018).

2 Dies ist durch § 268 SGB V gesetzlich geregelt.

3 Siehe z. B. https://www.kreditech.com/what-we-do/ (zuletzt abgerufen am 03.04.2018).

4 Siehe etwa: http://bigdatascoring.com/ (zuletzt abgerufen am 05.04.2018); https://www.welt.de/regionales/hamburg/article108401373/Was-Social-Media-bereits-ueber-Ihre-Bonitaet-verraet.html: https://netzpolitik.org/2017/social-media-analyse-und-profilierung-bei-versicherungen-beeinflussen-nicht-nur-mitgliedsbeitraege/ (zuletzt abgerufen am 09.02.2018).

5 im Folgenden beziehen wir uns auf das BDSG von 2009 als BDSG a. F. und auf das BDSG von 2018 als BDSG n. F.

6 Siehe dazu: Helberger/Borgesius/Reyna, „The Perfect Match? A closer look at the relationship between EU consumer law and data protection law", (2017), Common Market Law Review, Volume 54, Issue 5, S. 2.

2. Problemaufriss und Aufbau des Papiers

Scoring wird als Begriff, insbesondere außerhalb der Rechtswissenschaft, nicht immer einheitlich und häufig auch synonym zum Begriff des Profiling verwendet. Unabhängig von den verschiedenen Herangehensweisen und Definitionen, die bei der Betrachtung von Scoring möglich sind, geht es grundsätzlich immer um die Verarbeitung von Daten. Eine Regulierung der Materie im Datenschutzrecht liegt damit nahe (dazu II.). Die derzeit bestehenden europäischen und deutschen Datenschutzregeln sind also Gegenstand unserer Erörterungen, wobei insbesondere die spezifischere Scoring-Regelung aus § 31 BDSG n. F. in den Blick genommen werden soll.

Im Folgenden unterteilen wir die Problemkreise des Scoring in Probleme der Datenverarbeitung bzw. der Datenbasis. Bei der Datenverarbeitung stellen sich Fragen wie: Welche weiteren Anforderungen werden an eine zulässige Datenverarbeitung gestellt? Müssen Betroffene in die Nutzung ihrer Daten zum Zwecke von Scoring einwilligen oder ist eine Verarbeitung auch ohne Einwilligung möglich (dazu III.)?

Hinsichtlich der Datenbasis ist fraglich, aus welchen Quellen die zur Berechnung von Scores verwendeten Daten bezogen werden dürfen. Von öffentlichen Verzeichnissen, Informationen anderer Unternehmen zu Online-Analysen ist hier vieles denkbar. Welche Voraussetzungen müssen die Daten, die für die Berechnung von Scores verwendet werden, erfüllen? Verhindern die bestehenden Regelungen diskriminierende Effekte? Welche gesetzlichen Anforderungen bestehen, um die Richtigkeit der Daten sicherzustellen? Wie weit darf die Datenbasis eines Scoringverfahrens reichen? Sind etwa Social-Media-Daten oder der Wohnort einer Person tatsächlich erheblich für die Feststellung ihrer Bonität (dazu IV.)? Weitere, im Zusammenhang mit automatisierter Datenverarbeitung grundsätzlich relevante Fragen, etwa zur Aufsicht, bleiben in diesem Papier außen vor.[7]

Schlussendlich wird deutlich, dass das Scoring größere gesellschaftspolitische Fragen aufwirft, in denen das Datenschutz nur *eine* Rolle in einem Netzwerk von anwendbaren Regeln spielen kann (dazu V.).

7 Außer Betracht bleibt auch die Diskussion um die Unionsrechtskonformität des neuen Scoringparagraphen § 31 BDSG n. F. und der beim deutschen Gesetzgeber verbleibenden Regelungskompetenz. Weitergehend zu dieser Debatte, s. Martini, Datenschutz-Grundverordnung, Paal/Pauly (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 8 zu Art. 22 DSGVO.

II Scoring im Datenschutzrecht

Das Datenschutzrecht ist ab dem Moment auf Scoringverfahren anwendbar, ab dem personenbezogene Daten i. S. d. Art. 4 Abs. 1 DSGVO verarbeitet werden. Liegt ein Personenbezug vor, ist die Verarbeitung der Daten nur dann zulässig, wenn ein Erlaubnistatbestand erfüllt ist, also entweder eine gesetzliche Erlaubnis (wie z. B. die Erlaubnis der Datenverarbeitung gem. Art. 6 Abs. 1 S. 1 lit. b) DSGVO) oder die Einwilligung des Betroffenen gem. Art. 6 Abs. 1 S.1 lit. a) DSGVO.[8]

1. Personenbezogene Daten im Scoring

In Art. 4 Nr. 1 DSGVO werden personenbezogene Daten definiert als Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, wie Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Die Frage, inwiefern beim Scoring ein Personenbezug der Daten gegeben sein muss, muss für verschiedene Prozesse und Daten voneinander getrennt betrachtet werden. Die Analyse von Datenbeständen zur Identifizierung von Korrelationen zwischen bestimmten Merkmalen und dem durch das Scoring zu prognostizierenden Verhalten ist nicht darauf gerichtet, Aussagen über einen Einzelnen, sondern zunächst nur allgemeine Feststellungen zu treffen, weshalb hier noch keine Bezüge zu Personen erforderlich sind.[9] Häufig werden hierfür Datensätze mit anonymen bzw. anonymisierten oder aggregierten Daten verwendet, die nicht in den Anwendungsbereich des Datenschutzes fallen.[10] Dass eine Deanonymisierung technisch möglich wäre, kann außer Betracht bleiben, weil ein solcher Umgang mit den Datenbeständen weder erwünscht noch wahrscheinlich ist.[11]

Sofern allerdings Datenbestände mit Personenbezug für die Analysen verwendet werden, findet das Datenschutzrecht Anwendung und ein spezieller Erlaubnistatbestand zur Verarbeitung der Daten wird erforderlich. Grundsätzlich zu unterscheiden sind dabei zum einen die Daten, die der Entwicklung der Formel dienen, mit der die Scores später berechnet werden (Scorecard), und Daten, die zur Errechnung des späteren Scorewerts einer konkreten Person verwendet werden.

Obschon die Erstellung der Scorecard selbst nicht die Verarbeitung personenbezogener Daten betrifft und damit das Datenschutzrecht auf diesen Teil des Prozesses grundsätzlich nicht anwendbar ist, unterwirft sie der Gesetzgeber dennoch Rechtmäßigkeitsanforderungen. Insbesondere hat der Verantwortliche gem. § 31 Abs. 1 Nr. 1 BDSG n. F. nachzuweisen, dass die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind.

Der Personenbezug, der die Anwendbarkeit des Datenschutzrechts begründet, ergibt sich erst durch die Errechnung des Scorewertes einer individuellen Person. Datenschutzrechtlich relevant sind dabei die Erhebung der personenbezogenen Daten des zu scorenden Betroffenen, sowie der Scorewert selbst.[12] Dass der kalkulierte Scorewert ein personenbezogenes Datum im

---

8 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 25.1 zu § 28b BDSG a. F.

9 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 23 zu § 28b BDSG a. F.

10 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 25 zu § 28b BDSG a. F.; Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 129 zu Art. 6 DS-GVO.

11 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 129 zu Art. 6 DS-GVO.

12 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 23 zu § 28b BDSG; Der Streit um die Personenbezogenheit der in Scoringverfahren genutzten Daten hat weiterhin eine gewisse Relevanz in den Bereichen, die nicht von § 31 BDSG n. F. erfasst werden. Dazu gehört insbesondere das nicht vertragsbezogene Scoring, also die interne Bewertung von Forderungen und Sicherheiten, siehe von Lewinski, Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017.

Sinne des Datenschutzrechts darstellt, ist inzwischen anerkannt.[13] Dies bedeutet, dass der persönlichkeitsrechtlich relevanteste Teil von Scoring ab der Anwendung der Scoring-Formel auf die einzelne Person vom Datenschutzrecht erfasst ist. Auf die vorgelagerte Analyse von Datenbeständen ohne Personenbezug, die zur Entwicklung der Scorecard führt, findet das Datenschutzrecht dagegen keine Anwendung.

2. Scoringparagraph § 31 BDSG n. F.: Schutz des Wirtschaftsverkehrs

Am 25.05.2018 trat das BDSG n. F. zusammen mit der DSGVO in Kraft. Es setzt die europäischen Vorgaben um und konkretisiert und ergänzt sie an verschiedenen Stellen. In Bezug auf Scoring stellt § 31 BDSG n. F. unter der Überschrift „Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften" Voraussetzungen für Scoring auf. Die Neuregelung in § 31 Abs. 1 BDSG n. F. stellt eine Legaldefinition von Scoring auf. Sie lautet, wenig abweichend von § 28b BDSG a. F.:

> Die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (Scoring) ist nur zulässig, wenn
> 1. die Vorschriften des Datenschutzrechts eingehalten werden
> 2. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind.
> 3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt wurden und im Fall der Nutzung von Anschriftendaten die betroffene Person vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

Diese Regelung dient, wie schon ihr Titel besagt, dem Schutz des Wirtschaftsverkehrs. Schon dies macht deutlich, dass die Scoring-Regelung nicht in erster Linie mit Datenschutz befasst ist. In der Gesetzesbegründung zu § 31 BDSG n. F. heißt es:

„Die Regelung übernimmt die in § 28b BDSG a. F. festgelegten Voraussetzungen und konkretisiert, welche Voraussetzungen ein von einer Auskunftei ermittelter Score-Wert im Hinblick auf sog. Negativ-Merkmale erfüllen muss, damit er im Wirtschaftsverkehr verwendet werden darf. Für die Verwendung des Score-Wertes wird auf die Kriterien der derzeitigen § 28a Absatz 1 und § 28b zurückgegriffen."[14]

Der gesetzgeberische Wille bei der Einführung von § 28b BDSG bestand darin, für die in der Kreditwirtschaft verwandten Verfahren zur Einschätzung kreditorischer Ausfallrisiken einen gesetzlichen Rahmen zu schaffen, um die bis dahin herrschende Rechtsunsicherheit über die Zulässigkeit von Scoringverfahren zu beseitigen.[15] Mit der Einführung des § 28b BDSG entschied der Gesetzgeber, dass Scoring grundsätzlich erlaubt sein soll, gleichzeitig aber bestimmte Voraussetzungen erfüllen muss.

---

13 Zuvor wurde in Zweifel gezogen, ob der Score sich auf persönliche oder sachliche Verhältnisse einer Person im Sinne der Definition des § 3 Abs. 1 BDSG bezieht. Da es sich bei einem Score um eine zukunftsgerichtete Wahrscheinlichkeitsaussage handelt, wurde von verschiedenen Seiten das Vorliegen eines „Verhältnisses" im Sinne der Vorschrift angezweifelt. Es sei demnach nicht sicher, ob sich die errechnete Gruppenwahrscheinlichkeit bei dem jeweiligen Betroffenen tatsächlich realisiere, weshalb trotz der Zuordnung des Einzelnen zu einer Gruppe der notwendige Rückschluss auf den Einzelnen gerade nicht möglich sei, s. Kamlah, „Das Schufa-Verfahren und seine datenschutzrechtliche Zulässigkeit", (1999), Multi Media und Recht, Heft 7, S. 395–404, S. 401; s. auch: Wuermeling, „Scoring von Kreditrisiken", (2002), Neue Juristische Wochenschrift, Heft 48, S. 3508–3510, S. 3509.

14 BT-Drs. 18/11325, S. 101.

15 Gesetzesbegründung in BT-Drs. 16/10529, S. 15; Zur historischen Entwicklung, s. ULD Schleswig Holstein/GP Forschungsgruppe, *Scoring nach der Datenschutznovelle 2009 und neue Entwicklungen*, (2014), S. 16; 20

Der Bundesrat hatte in seiner Empfehlung zum Gesetzesentwurf des § 28b BDSG gefordert, Scoring-Reglungen nur auf Verträge anzuwenden, bei denen ein kreditorisches Ausfallrisiko besteht, also z. B. Darlehensverträge, Finanzierungshilfe oder Bürgschaften.[16] Damit sollte vermieden werden, dass automatisierte Bewertungsverfahren auf andere Verträge ausgeweitet werden, bei denen kein überwiegendes wirtschaftliches Interesse erkennbar sei, das den weitreichenden mit Scoring verbundenen Eingriff in die Betroffenenrechte rechtfertigen könnte. Die Bundesregierung sah jedoch keine „sachliche Rechtfertigung" für eine solche Einschränkung, da die legitimen Zwecke der Datennutzung durch das geltende Recht ausreichend geschützt seien.[17]

Die Hauptanwendungsfälle von Scoring in § 31 Abs. 1 BDSG n. F. liegen in den Bereichen der Kreditvergabe, des Versandhandels, der Wohnraumvermietung, der Direktwerbung, aber auch im Sicherheitsbereich.[18] Ziel des vorbildgebenden Kreditscorings ist es, die Zahl von Kreditausfällen so gering wie möglich zu halten und dadurch die Kreditkosten für Verbraucher insgesamt zu senken und ein Funktionieren der Kreditwirtschaft zu garantieren.[19] Obschon bei der Entwicklung der Regelungen von Scoring das klassische Kreditscoring als Vorbild fungierte,[20] ist ein weitergehender Anwendungsbereich auch in Bezug auf andere Branchen nicht ausgeschlossen.

Zu den neueren Bereichen zählt beispielsweise das sogenannte Versicherungs-Scoring mit Telematik- bzw. verhaltensbasierten Tarifen. Da in diese Art von Scoring Fälle höherer Gewalt und Fremdeinwirkung in eine Prognoseentscheidung über den Abschluss eines Versicherungsvertrages aufgenommen werden, sollte – so führte die Gesetzesbegründung aus – der bisherige § 28b BDSG keine Anwendung finden.[21] Diese Einschätzung beruht auf der Annahme, dass diese Fälle nicht das „Verhalten" einer natürlichen Person betreffen.[22] Diese Annahme ist inzwischen bei einigen Tarifmodellen in der Versicherungsbranche als hinfällig: es werden zunehmend Businessmodelle ausprobiert, die bestimmte Verhaltensweisen von Betroffenen in den Score einfließen lassen.[23] Dies kann bedeuten, dass bestimmte neue Scoring-Modelle in der Versicherungsbranche durchaus in den Anwendungsbereich des § 31 Abs. 1 BDSG n. F. fallen können.

3. Scoring als automatisierte Einzelentscheidung: Schutz der Entscheidungsfreiheit

Im Datenschutzrecht finden sich weitere Regelungen, die auf Scoring anwendbar sind. Schutzgut sind hier nicht wie bei § 31 BDSG n. F. die Interessen des Wirtschaftsverkehrs, sondern datenbezogene Privatsphäreninteresseninteressen und die Entscheidungsfreiheit des Betroffenen.

Art. 22 DSGVO ist eine allgemeine Regelung für die automatisierte Entscheidung im Einzelfall. Dabei stellt die Vorschrift als einen besonderen Anwendungsfall das sogenannte Profiling ausdrücklich heraus. Gem. Art. 4 Nr. 4 DSGVO wird Profiling definiert als

„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass die personenbezogenen Daten verwendet werden, um bestimmte persönlich Aspekte, die sich auf einer

16 BR-Drs. 548/1/08, S. 11–12.

17 BT-Drs. 16/10581, S.1.

18 Dies war zumindest für § 28b BDSG a. F. der Fall, für die Neuregelung in § 31 Abs. 1 BDSG n. F. dürfte nichts anderes gelten; s. von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 23. Edition 2018, Rn. 2 zu § 28b BDSG a. F.

19 Siehe dazu die Argumentation der Schufa https://www.schufa.de/de/ueber-uns/daten-scoring/scoring/scoring/ (zuletzt abgerufen am, 12.01.2018); Arvato https://finance.arvato.com/de/verbraucher/selbstauskunft/scoring-scorewerte.html (zuletzt abgerufen am 12.01.2018).

20 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 22. Edition, Stand: 01.11.2017, C. H. Beck Verlag, Rn. 8 zu § 28b BDSG a. F.

21 BT-Drs. 16/10529, 10.10.2008, S. 16; gleiches dürfte für § 31 Abs. 1 BDSG n. F. gelten.

22 Siehe ULD Schleswig Holstein / GP Forschungsgruppe, Scoring nach der Datenschutznovelle 2009 und neue Entwicklungen, (2014), S. 21.

23 Dazu zählen z. B. sog. Telematik-Tarife bei Kfz-Versicherungen, bei denen sich der Beitrag zum Teil auch nach dem fahrverhalten des Versicherten bemisst: https://www.allianz.de/auto/kfz-versicherung/telematik-versicherung/ (zuletzt abgerufen am 01.03.2018).

natürlich Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen."

Scoring stellt wiederum einen speziellen Anwendungsbereich des Profiling dar,[24] bei dem der Einsatz des Bewertungsverfahrens der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses dient.

Art. 22 Abs. 1 DSGVO verbietet grundsätzlich Entscheidungen, die auf einer ausschließlich automatisierten Datenverarbeitung beruhen und für den Betroffenen rechtliche Wirkung entfalten oder ihn in ähnlicher Weise erheblich beeinträchtigen.

Damit soll Art. 22 DSGVO Einzelne vor einem Bewertungsautomatismus schützen.[25] Als praxisrelevante Fälle nennt Erwägungsgrund 71 DSGVO die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren.

Auch wenn Art. 22 DSGVO grundsätzlich auf Scoring anwendbar ist, sind viele Scoringmethoden in der Praxis von dem Anwendungsbereich der Norm ausgeschlossen. Erlaubt bleiben solche Entscheidungsprozesse, die nicht vollständig automatisiert sind, bei denen also ein nicht näher definiertes menschliches Eingreifen stattfindet. Dazu kommt, dass in Art. 22 Abs. 2 DSGVO verschiedene Ausnahmen zum Verbot der automatisierten Entscheidung genannt sind. Für Scoring sind insbesondere die in Abs. 2 lit. a und c) DSGVO genannten Ausnahmen relevant, wonach eine automatisierte Entscheidung zulässig ist, wenn sie für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist oder wenn die ausdrückliche Einwilligung der betroffenen Person vorliegt. In diesem Zusammenhang ist fraglich, unter welchen Umständen der Einsatz einer automatisierten Entscheidung als erforderlich für den Abschluss oder die Erfüllung eines Vertrags anzusehen ist. Nach allgemeiner Ansicht dient diese Ausnahme der Ermöglichung von Vertragsschlüssen im Massengeschäft.[26] Ob eine automatisierte Einzelentscheidung erforderlich ist, soll sich demnach aus den jeweiligen Vertragszielen ergeben.

Gefordert wird zum Teil ein unmittelbarer sachlicher Zusammenhang zwischen der Datenverwendung und dem konkreten Vertragszweck, um eine Erforderlichkeit bejahen zu können.[27] Generell bleiben die Voraussetzungen jedoch unklar.

Darüber hinaus stellt § 37 BDSG n. F. eine Ausnahmeregelung vom Verbot der automatisierten Einzelentscheidung für Versicherungsverträge auf. Demnach ist eine automatisierte Einzelentscheidung zulässig, wenn einem Begehren der betroffenen Person stattgegeben wurde (Nr. 1) oder wenn im Falle der (teilweisen) Ablehnung eines individuellen Begehrens angemessene Maßnahmen zur Interessenwahrnehmung durch die Betroffene ergriffen wurden (Nr. 2).

Damit ist der Anwendungsbereich des Datenschutzrechts für Scoring beschränkt. Die umfangreichen und vor allem für Scoring relevanten Ausnahmetatbestände und die Tatsache, dass Scoringverfahren, in denen ein menschlicher Entscheider beteiligt ist, von den Anforderungen der Norm nicht erfasst sind, stehen der Entwicklung eines allgemeinen datenschutzrechtlichen Qualitätsstandards von Scoringsystemen entgegen.

---

24 Schild, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 22. Edition, Stand: 01.11.2017, C. H. Beck Verlag, Rn. 64 zu Art. 4 DSGVO; Martini, Datenschutz-Grundverordnung, Paal/Pauly (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 7 zu Art. 22 DSGVO.

25 Martini, „Big Data als Herausforderung für den Persönlichkeitsschutz", (2014), Deutsches Verwaltungsblatt, Heft 23, S. 1481–1489, S. 1485. Kritiker weisen darauf hin, dass es bei aus dem Anwendungsbereich des Art. 22 DSGVO herausfallenden Systemen für den menschlichen Entscheider kaum möglich sei, mehr als eine Plausibilitätskontrolle der automatisierten und oftmals komplexen Vorentscheidung vorzunehmen. Die menschliche Prüfung sei daher praktisch weitgehend wirkungslos. Sofern aber eine solche, wie auch immer ausgestaltete menschliche Prüfung erfolgt, stellt die DSGVO keine über die normale Datenverarbeitung hinausgehenden Anforderungen. Dabei könnten solche nicht vollkommen automatisierten Entscheidungsverfahren ähnliche Auswirkungen auf den Persönlichkeitsschutz des Einzelnen haben wie vollautomatisierte Systeme.

26 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 29 zu Art. 22 DSGVO; Martini, Datenschutz-Grundverordnung, Paal/Pauly (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 31 zu Art. 22 DSGVO.

27 Martini, Datenschutz-Grundverordnung, Paal/Pauly (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 31 zu Art. 22 DSGVO.

III Problem: Datenverarbeitung

Aber auch in den Bereichen, in denen Scoring vom BDSG erfasst wird, ergeben sich rechtliche Probleme. Im Folgenden sehen wir, dass sich im Bereich der Datenverarbeitung sich einige Schutzlücken durch die neuen Regelungen des BDSG ergeben. Diese betreffen sowohl Erlaubnistatbestände als auch die Einwilligung in die Datenverarbeitung. Auch die allgemeinen Grundsätze des Datenschutzrechts stoßen im Bereich Scoring an ihre Grenzen. Zunächst befassen wir uns mit den gesetzlichen Erlaubnistatbeständen für forderungsspezifische Daten und deren Weiterleitung an Auskunfteien, sowie der Einwilliung der Betroffenen. Danach skizzieren wir die Probleme, die Big-Data-Scoring mit sich bringt.

1. Erlaubnistatbestände

1.1 Einmeldung forderungsbezogener Daten an Auskunfteien

Auskunfteien benötigen zur Berechnung von Scores eine Datenbasis, auf die sie zurückgreifen können. Da in der DSGVO die Datenübermittlung an Auskunfteien, anders als noch im BDSG a. F., nicht explizit geregelt ist, führt der deutsche Gesetzgeber in § 31 Abs. 2 BDSG n. F. die Voraussetzungen für das sogenannte Einmelden forderungsbezogener Daten für das Kreditscoring aus dem § 28a BDSG a. F. fort. Die Einführung der Regelung diente vor allem dazu, den Verantwortlichen mehr Rechtssicherheit und den Betroffenen mehr Transparenz zu gewährleisten.

Die Information, dass eine Forderung nicht beglichen wurde (Negativdaten), fällt unter § 31 Abs. 2 BDSG n. F. und kann unter den dort genannten Voraussetzungen an Auskunfteien weitergegeben werden. Dazu zählt u. a., dass die Forderung tituliert ist, durch den Schuldner ausdrücklich anerkannt wurde, oder das zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen gekündigt werden kann und der Betroffene über die Übermittlung unterrichtet wurde. Alternativ kommt eine Einmeldung auch in Betracht, wenn der Schuldner nach Eintritt der Fälligkeit mindestens zweimal gemahnt wurde, er die Forderung nicht bestritten hat und er über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist. Dies bedeutet, dass ohne Wissen des Schuldners eine Datenübermittlung an Auskunfteien nicht stattfinden kann.

Anders als in § 28a Abs. 2 BDSG a. F. gibt es keine explizite Regelung zur Übermittlung sogenannter Positivdaten an Auskunfteien mehr. Positivdaten sind Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft. Die Übermittlung war grundsätzlich erlaubt, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwog. Diese Regelung ist im BDSG n. F. nicht mehr enthalten. Die Übermittlung von Positivdaten an Auskunfteien sei laut Gesetzgeber durch die Regeln des allgemeinen Datenschutzrechts zur Zulässigkeit der Verarbeitung personenbezogener Daten ausreichend geregelt.[28] Bedenklich ist dies allerdings vor dem Hintergrund, dass die Erlaubnis zur Einmeldung von Positivdaten explizit im BDSG a. F. reguliert worden war, um Rechtssicherheit herbeizuführen.

Im Unterschied zu § 28a Abs. 2 S. 4 BDSG a. F. fehlt im BDSG n. F. zudem auch die Regelung, dass Informationen über Anfragen von Personen zu Kreditkonditionen in die Berechnung ihrer Bonitätsscores nicht einfließen dürfen. Der Bundesrat hatte dies in seiner Stellungnahme kritisiert und darauf hingewiesen, dass es aus Verbrauchersicht sinnvoll sei, vor Abschluss eines Kreditvertrages die Konditionen mehrerer Banken zu vergleichen. Verbraucherinnen und Verbraucher müssten daher befürchten, durch Konditionenanfragen ihren Scorewert zu verschlechtern.[29] Die Regelung des § 28a Abs. 2 S. 4 BDSG a. F. beruhte auf der Erkenntnis, dass die Anfrage von Kreditkonditionen hintereinander bei mehreren Kreditinstituten zu einer stetigen Verschlechterung des Bonitätsscores führte, weil auch die Anfragen bei Banken, die lediglich zur Information über konkrete Konditionen dienten, so behandelt wurden, als handele es sich um Informationen über bereits

28 BT-Drs. 18/11325, S. 101.

29 BR-Drs. 18/11325, S. 18.

gestellte Kreditanträge. Der Häufung solcher Anfragen wurde entnommen, dass der Betroffene dringend Geld bräuchte oder in einen Zahlungsengpass geraten sein könnte.[30] Auch die DSGVO enthält hierzu keine speziellen Regelungen, so dass es nach der neuen Rechtslage zu einer weiteren Schutzlücke für Verbraucher kommt. Nunmehr können solche Daten nach den allgemeinen Vorschriften des Art. 6 DSGVO verarbeiten werden.

Außerdem ist zu bemerken, dass die Voraussetzungen aus § 31 Abs. 2 BDSG n. F. sich ausschließlich auf das Bonitätsscoring beziehen. Sollten forderungsbezogene Negativdaten für die Bestimmung anderer Scores als relevante Merkmale verwendet werden, greift § 31 Abs. 2 BDSG n. F. mit seinen engeren Voraussetzungen nicht. Auch hier sind dann lediglich die allgemeinen Vorgaben des Art. 6 DSGVO zu berücksichtigen.

Es ist unklar, wie die daraus resultierende Schutzlücke geschlossen werden kann. Eine Einwilligung des Betroffenen nach Art. 6 Abs. 1 lit. a) DSGVO würde die ursprünglichen Erwägungen, die § 28a Abs. 2 BDSG a. F. zugrunde liegen, konterkarieren. Die Freiwilligkeit der Einwilligung des Betroffenen zur Datenübermittlung kann gerade deshalb in Zweifel gezogen werden, weil in der Praxis der Verbraucher einen Bankkredit regelmäßig nicht ohne eine von der Bank angeforderte Bonitätsauskunft einer Auskunftei erhalte. Diese Auskunft wäre aber wiederum mit der Einwilligungserklärung des Betroffenen in die Übermittlung bestimmter personenbezogener Daten an diese Auskunftei verbunden.[31] Eine weitere Möglichkeit wäre das Vorliegen eines berechtigten Interesses auf Seiten der einmeldenden Bank in die Übermittlung von Vertragsdaten durch Kreditinstitute nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO. Dieses Interesse könnte darin liegen, sich selbst und die Wirtschaft allgemein vor schädigenden Zahlungsausfällen zu bewahren. Dazu dürfte allerdings schon die Übermittlung von Negativdaten nach § 31 Abs. 1 BDSG n. F. ausreichend sein. Offensichtlich ist, dass an dieser Stelle Rechtsunsicherheit für Kreditinstitute besteht, die vom Gesetzgeber oder dem Datenschutzausschuss (Art. 68 DSGVO) geklärt werden müsste.[32]

1.2 Erhebung und Speicherung anderer personenbezogener Daten

Neben der Einmeldung forderungsbezogener Daten stellt sich die Frage, unter welchen Voraussetzungen weitere personenbezogene Daten von Auskunfteien und anderen Unternehmen erhoben und gespeichert werden dürfen. In Betracht kommen hier z. B. Anschrift, Geburtsdatum und Wohnort des Betroffenen bis hin zu Daten aus sozialen Netzwerken oder über das Online-Verhalten.

§ 29 Abs. 1 BDSG a. F. stellte einen ausdrücklichen Erlaubnistatbestand für die im Datenschutz grundsätzlich mit einem Verbot versehene Verarbeitung personenbezogener Daten für Auskunfteien dar. Grenze dieser Erlaubnis waren etwaige überwiegende schutzwürdige Interessen des Betroffenen.[33] § 29 BDSG a. F. regelte noch, dass personenbezogene Daten „geschäftsmäßig" zum Zweck der Übermittlung an Dritte erhoben, gespeichert, verändert und benutzt werden dürfen, wenn dem kein schutzwürdiges Interesse des Betroffenen am Ausschluss dieser Datennutzung entgegensteht, oder wenn die Daten allgemein zugänglich sind. Auch in letzterem Fall konnte allerdings eine Interessenabwägung die Zulässigkeit der Datenverarbeitung ausschließen.

Diese Vorschrift findet jedoch weder in der DSGVO noch im BDSG n. F. eine Nachfolgeregelung. Unter welchen Voraussetzungen Auskunfteien personenbezogene Daten zulässigerweise verarbeiten dürfen, ist folglich anhand der allgemeinen Regelungen der DSGVO, insbesondere Art. 6 und Art. 5 Abs. 1 DSGVO zu beurteilen. Es ist bisher offen, ob sich dadurch eine größere Schutzlücke für die Betroffenen ergibt als nach bisheriger Rechtslage.

---

30 Kamp, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 21. Edition, Stand 01.02.2016, C. H. Beck Verlag, Rn. 155 zu § 28a BDSG a. F.

31 BT-Drs. 16/10529, S. 15.

32 Dazu Seiler, „Scoring im neuen EU-Datenschutzrecht", (2017), jurisPR-BKR, 8/2017, Anm. 1.

33 Zu den Grenzen der Interessenabwägung, s. OLG Stuttgart, Urteil vom 12.12.2002, 2 U 130/02.

2. Einwilligung in die Datenverarbeitung für Scoring

Mit der Lockerung der Voraussetzungen für eine rechtmäßige Datenverarbeitung gewinnt die Einwilligung des Betroffenen in die Datenverarbeitung an Bedeutung. Die Frage der Rechtmäßigkeit der Verarbeitung anderer als forderungsbezogener Daten richtet sich nach neuer Rechtslage nunmehr nach Art. 6 Abs. 1 S. 1 lit. a) und b) DSGVO und damit insbesondere nach der Einwilligung des Betroffenen in die konkrete Verarbeitung oder alternativ nach der Erforderlichkeit der Verarbeitung für die Erfüllung eines Vertrags oder die Durchführung vorvertraglicher Maßnahmen. Für die Erfüllung des Vertrags erforderlich sollen solche Daten sein, die die notwendige Entscheidungs- und Kalkulationsgrundlage für das konkrete Rechtsgeschäft bilden. So ist dies beispielweise bei Versicherern, die den Abschluss des Versicherungsvertrags von der Preisgabe von Daten über das Risikoprofil des Kunden abhängig machen dürfen.[34]

Die allgemeinen Voraussetzungen für die Zulässigkeit einer Datenverarbeitung des Art. 6 Abs. 1 DSGVO gelten auch für Unternehmen, die selbst, also ohne Rückgriff auf eine Auskunftei scoren.

Die Einwilligung der betroffenen Person hat gemäß Art. 8 Abs. 2 der Grundrechtecharta der EU primärrechtlichen Status. Sie soll es dem Einzelnen ermöglichen, über seine persönlichen Daten nach eigenem Ermessen zu verfügen und ist damit Ausdruck der Selbstbestimmtheit des Betroffenen. Die Voraussetzungen einer wirksamen Einwilligung ergeben sich aus den Art. 4 Nr. 11 i. V. m. Art. 7 Abs. 2, 4 DSGVO Definiert wird die Einwilligung in Art. 4 Nr. 11 DSGVO als eine **freiwillig**, **in informierter Weise** und unmissverständlich, für den bestimmten Fall abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Sowohl die Informiertheit als auch die Freiwilligkeit der Einwilligung ist in der Praxis jedoch problematisch.

2.1 Information und Transparenz

Das rechtliche Schutzinstrument der Information und Einwilligung beruht auf der Annahme, dass der Verbraucher wirtschaftlich rational handelt und dass sein Handeln seine tatsächlichen Präferenzen widerspiegelt. Dem Betroffenen muss vor seiner Einwilligung klar sein, auf welche personenbezogenen Daten sich seine Einwilligung bezieht und was mit diesen Daten geschehen soll.[35] Welche Informationen dem Betroffenen genau mitgeteilt werden müssen, ist im Fall der Erhebung personenbezogener Daten bei der betroffenen Person in Art. 13 DSGVO geregelt.

Das der Einwilligung zugrunde liegende Problem ist eine strukturelle Informationsasymmetrie zwischen Datenverwender und Betroffenen, die durch die Information der Betroffenen behoben werden soll. Die Information des Betroffenen ist in der Praxis jedoch kaum gewährleistet. Ein Problem liegt in der Verwendung langer Datenschutzbestimmungen, die von den Betroffenen in der Regel nicht mehr gelesen werden.[36] Lange und ausufernde Zweckbestimmungen erschweren es dem Betroffenen, die konkreten Folgen seiner Einwilligung in eine Datenverarbeitung vorauszusehen. Dieses Problem wird umso größer, je mehr sich die Internetnutzung auf mobile Endgeräte verlagert und die Nutzer in diesem Umfeld zunehmend nicht

---

34 Buchner/Kühling, DS-GVO, BDSG, Kühling/Buchner (Hrsg.), 2. Auflage 2018, C. H. Beck Verlag, Rn. 46 zu Art 7 DSGVO.

35 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 31 zu Art. 7 DSGVO.

36 Die australische Verbraucherschutzorganisation Choice beauftragte einen Schauspieler damit, die Nutzungsbedingungen des Amazon E-Readers Kindle vorzulesen, was etwa neun Stunden dauerte.
https://www.theguardian.com/australia-news/2017/mar/15/amazon-kindles-terms-unreasonable-and-would-take-nine-hours-to-read-choice-says (zuletzt abgerufen am 22.08.2017). Einer Studie zufolge bräuchte jeder Internetnutzer etwa 244 Stunden im Jahr, um die Datenschutzerklärungen der Seiten, die er nutzt, einmal zu lesen, McDonald and Cranor,"The Cost of Reading Privacy Policies", (2008), Journal of Law and Policy for the Information Society, Vol. 4 Nr. 3, 543–568, S. 563.

die Zeit oder Möglichkeit haben, sich mit seitenlangen Datenschutzbedingungen auseinanderzusetzen.[37]

Dazu kommt, dass die Datenschutzbestimmungen von Unternehmen, die den Betroffenen sicherlich auch über die Verarbeitung seiner Daten informieren sollen, oft unspezifisch gehalten sind, um einen größtmöglichen Umfang an Daten verarbeiten zu können und auch unvorhergesehene Nutzungen zu ermöglichen. So heißt es beispielsweise in den Datenschutzrichtlinien von Facebook:

„Wir übertragen Informationen an Anbieter, Dienstleister und sonstige Partner, die unser Unternehmen weltweit unterstützen, **beispielsweise** (eigene Hervorh.) indem sie Dienstleistungen für eine technische Infrastruktur zur Verfügung stellen, analysieren, wie unsere Dienste genutzt werden, die Wirksamkeit von Werbeanzeigen und Diensten messen, eine Kundenbetreuung anbieten, **Zahlungen ermöglichen** (eigene Hervorh.) oder wissenschaftliche Studien und Umfragen durchführen."[38]

Es werden hier nur beispielhaft und damit nicht abschließend die möglichen Kontexte und Empfänger der Datenweitergabe angegeben. Auch in der Datenschutzrichtlinie von LinkedIn heißt es u. a.:

„Wenn wir andere persönliche Daten erfassen oder wesentlich ändern, wie wir Ihre Daten verwenden, benachrichtigen wir Sie und modifizieren **vielleicht** (eigene Hervorh.) auch diese Datenschutzrichtlinie".[39]

Diese Datenschutzbestimmungen dürften für die Information des Betroffenen nicht ausreichend sein. Sie sind vage und unklar. Facebook macht nicht deutlich, an wen die Daten genau übertragen werden. In beiden Datenschutzbestimmungen ist nicht aufgelistet, welche Daten konkret gespeichert, verarbeitet und/oder weitergegeben werden.

Dieses Problem wird auch nicht durch die verschiedenen Möglichkeiten der Informationsvermittlung behoben. In Art. 12 Abs. 7 DSGVO wird die Möglichkeit geregelt, die Informationen, die den Betroffenen laut Verordnung bereitzustellen sind, mit standardisierten Bildsymbolen zu kombinieren, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Zu bedenken ist aber, dass die Bildsymbole nur zusätzlich gebraucht werden, schriftliche oder elektronische Kommunikation aber nicht ersetzen können.[40] So können Bildsymbole zwar für mehr Übersicht sorgen, bei übermäßig langen Datenschutzbedingungen jedoch kaum Abhilfe leisten.

Auch Zertifizierungen werden dieses Problem der Information und Transparenz von Datenschutzbestimmungen nicht lösen können. Art. 42 DSGVO stellt einen Rechtsrahmen für die Einführung eines europaweiten Zertifizierungssystems, sowie von speziellen Datenschutzsiegeln und -prüfzeichen auf. Zum Teil wird hier die Einführung gestaffelter Gütesiegel gefordert, die sich an einheitlichen Kriterien, wie dem Umfang der Datenweitergabe an Dritte, der Anonymisierung und Pseudonymisierung der Daten und der Datensicherheit orientieren und einen gewissen Wettbewerb unter den Datenverarbeitern fördern sollen.[41] Ob dies jedoch dazu beiträgt, die Einwilligung der Betroffenen zu stärken, ist fraglich. In Art. 42 Abs. 3 DSGVO ist geregelt, dass die Zertifizierung für die Datenverarbeiter freiwillig bleiben muss. Außerdem dürfte die durch Zertifizierung angestrebte Transparenz nichts mit der Informiertheit der Betroffenen zu tun haben. Im Gegenteil, Betroffene könnten sich blind auf Zertifizierungen verlassen, ohne sich selbst ein Bild von der Datenerhebung zu machen. Dann würde die Transparenz von Datenschutzerklärungen nicht zur Information der Betroffenen beitragen.

---

37 Daher die Forderung des SVRV nach der Einführung eines Datenschutz-One-Pagers, der dem Verbraucher neben der ausführlichen Datenschutzerklärung auf einer Seite zusammengefasst die wichtigsten Informationen über die Datenverarbeitung des potenziellen Vertragspartners darstellt und somit als erste Orientierungshilfe dient, SVRV, Verbraucherrecht 2.0, 2016, S. 46 f.; SVRV, Digitale Souveränität, 2017, S. 20 f.

38 Abrufbar unter: https://de-de.facebook.com/policy.php (zuletzt abgerufen am 11.10.2017), Hervorh. nicht im Original.

39 Abrufbar unter: https://www.linkedin.com/legal/privacy-policy?_l=de_DE (zuletzt abgerufen am 12.10.2017), Hervorh. nicht im Original.

40 Quaas, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 53 zu Art. 12 DSGVO.

41 Krüger, „Datensouveränität und Digitalisierung, Probleme und rechtliche Lösungsansätze", (2016), Zeitschrift für Rechtspolitik, Heft 7, S. 190–192, S. 191.

2.2 Freiwilligkeit und Kopplungsverbot

Auch die Freiwilligkeit, mit der die Einwilligung erteilt werden soll, ist in der praktischen Umsetzung problematisch.

In Art. 7 Abs. 4 DSGVO heißt es, dass bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden muss, ob u. a. die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Mit anderen Worten erscheint die Freiwilligkeit einer Einwilligung zumindest zweifelhaft, wenn diese zur Bedingung für einen Vertragsschluss gemacht wird und zudem Daten verarbeitet werden sollen, die für die Vertragsdurchführung nicht erforderlich sind. Diese Regelung wird auch als Kopplungsverbot bezeichnet.

Anhaltspunkte für die Beurteilung im Rahmen des Art. 7 Abs. 4 DSGVO bieten die Erwägungsgründe 42 und 43 DSGVO. Danach soll nur dann von der Freiwilligkeit einer Einwilligung ausgegangen werden, wenn die betroffene Person eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern ohne Nachteile zu erleiden. Die Einwilligung wird zumindest dann nicht freiwillig abgegeben, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht und es deshalb in Anbetracht aller konkreten Umstände unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde. Die Einwilligung soll darüber hinaus auch dann nicht als freiwillig erteilt gelten, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

Das deutsche Datenschutzrecht enthielt bisher bereits ähnliche Vorschriften. Anders als noch im BDSG a. F. ist eine Kopplung von Vertragsschluss und Datenverarbeitung jetzt wegen Art. 7 Abs. 4 DSGVO nicht mehr zwangsläufig unzulässig, sondern Gegenstand einer Abwägung der Einzelfallumstände. Diese nun in den Rechtsfolgen mildere Regelung soll insbesondere dem angemessenen Interessenausgleich Rechnung tragen, der angesichts des durch das Kopplungsverbot bedingten Eingriffs in die Privatautonomie des Datenverarbeiters erforderlich ist.[42] An dieser Stelle werden folglich die unternehmerischen Interessen des Datenverarbeiters gegenüber den Interessen des Verbrauchers gestärkt. Da es sich nun aber um einen Abwägungsprozess handelt, ist im Einzelnen umstritten, wie weit das Kopplungsverbot reicht. Im Mittelpunkt steht die Erforderlichkeit der Daten zur Vertragserfüllung.[43]

Für Scoring ist das Kopplungsverbot mittelbar von Bedeutung. Zum einen wird das Kopplungsverbot bei Scoring dann relevant, wenn z. B. die Erteilung eines Kredits oder die Erbringung einer Dienstleistung von der Einwilligung des Betroffenen in die Durchführung einer Bonitätsprüfung abhängig gemacht wird. Wenn der Kunde etwa durch Vorkasse in Vorleistung geht, ist eine Bonitätsprüfung nicht erforderlich und daher nach dem Kopplungsverbot unzulässig.[44]

Zum anderen können die von Nutzern dieser entgeltfreien Angebote freigegebenen Daten potenziell auch für eine Verarbeitung durch Scoring-Unternehmen verwendet werden.[45] Viele Apps und internetbasierte Anwendungen basieren auf sogenannten „entgeltfreien" (Nutzungs-) Verträgen. Teilweise wird argumentiert, dass bei solchen Angeboten, deren Gegenleistung gerade in der Datenhingabe besteht, das Kopplungsverbot nicht eingreifen solle, da dies zu einer deutlichen

---

42 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 24 zu Art. 7 DSGVO.

43 Von der Erforderlichkeit zu unterscheiden ist die Erheblichkeit der Daten. Die Datenverarbeiter können beim Scoring festlegen, welche Daten für das von ihnen zu prognostizierende Verhalten nach mathematisch-statistischen Verfahren erheblich sind. Es ist aber fraglich, ob alle Daten, die vom Verarbeiter als (tatsächlich) erheblich identifiziert wurden, auch als (rechtlich) erforderlich i. S. d. Art. 7 Abs. 4 DSGVO gelten sollen (zum Problem der Erheblichkeit der Daten siehe IV.2.1).

44 Achtermann/Lachenmann, Formularhandbuch Datenschutzrecht, Koreng/Lachenmann (Hrsg.), 2. Aufl. 2018, S. 960 ff.

45 Siehe z. B. https://bigdatascoring.com/ (zuletzt abgerufen am 26.04.2018), allerdings nicht auf dem deutschen Markt aktiv; http://www.faz.net/aktuell/feuilleton/silicon-demokratie/kolumne-silicon-demokratie-bonitaet-uebers-handy-12060602.html (zuletzt abgerufen am 26.04.2018).

Abnahme solcher „kostenlosen“ Angebote führen könne, was unter sozialpolitischen Gesichtspunkten nicht wünschenswert sei.[46] Zu bedenken ist aber, dass bei Eingreifen des Kopplungsverbots die Anbieter dieser Dienste kostenpflichtige, aber dafür datenschutzintensivere Alternativen schaffen müssten. In der Abwägung, ob der entgeltfreien Variante eine freiwillige Einwilligung zugrunde liegt, müsste dann berücksichtigt werden, dass dem Nutzer auch die Möglichkeit der kostenpflichtigen, aber datenfreien Nutzung zur Verfügung steht. In diesem Fall läge kein Verstoß gegen das Kopplungsverbot vor. Ein Eingreifen des Kopplungsverbots an dieser Stelle könnte also zu mehr Wahlfreiheit für den Konsumenten führen, der in der Folge tatsächlich frei zwischen entgeltfreien und kostenpflichtigen, aber datenschutzfreundlichen Alternativen wählen kann.

Die Einwilligung als maßgeblicher Regelungsansatz stößt außerdem aufgrund des sog. „Privatsphären-Paradox“ an ihre Grenzen. Darunter wird die Diskrepanz zwischen den Bedenken von Betroffenen hinsichtlich ihrer Privatsphäre auf der einen Seite und dem vermeintlich geringen Wert, den sie ihrer Privatsphäre beimessen, wenn sie beispielsweise persönliche Informationen für preiswerte Produkte online preisgeben, auf der anderen verstanden. In solchen Fällen, kann die Entscheidungsfreiheit des Betroffenen beeinträchtigt sein, weil die gegenteilige Entscheidung mit unverhältnismäßigen Kosten verbunden wäre. Darüber hinaus sind die tatsächlichen Privatsphäre-Bedürfnisse aufgrund ständig wechselnder technischer Anforderungen schwer umsetzbar und die Option, Privatsphäre gefährdende Websites nicht zu nutzen, ist oftmals nicht realistisch.[47] Das Erfordernis der Einwilligung kann dieses Problem nicht lösen.[48]

3. Grundsätze der Datenverarbeitung

§ 31 Abs. 1 Nr.1 BDSG n. F. verlangt, dass Scoring nur als rechtmäßig anzusehen ist, wenn die Vorschriften des Datenschutzrechts und damit auch die Grundsätze der Datenverarbeitung aus Art. 5 DSGVO eingehalten werden. Obschon diese Grundsätze selbst kein Novum im Recht der Datenverarbeitung darstellen, ergeben sich durch die Neuregelung in der DSGVO einige neue Rechtsfolgen. Zum Beispiel gehören Verstöße gegen Art. 5 DSGVO zu den besonders scharf sanktionierten Verletzungen der DSGVO nach Art. 83 Abs. 5 DSGVO. Die in Art. 5 DSGVO festgelegten Grundsätze sollten daher nicht mehr nur als Vorgaben zur Selbstbindung des Datenverarbeiters verstanden werden.[49]

Auch inhaltlich ergeben sich durch die Neuregelung in der DSGVO an einigen Stellen höhere Anforderungen für die Datenverarbeiter. Es wird angenommen, dass die Grundsätze eine höhere Relevanz für den einzelnen Datenverarbeiter bei der Auslegung und Anwendung der besonderen Vorschriften der DSGVO haben werden, als dies bisher der Fall war.[50] Es wird deshalb darauf verwiesen, dass es sich hier vielmehr um Grundpflichten bei der Datenverarbeitung als um bloße Grundsätze handelt.[51]

Inhaltlich betrachtet sind im Zusammenhang mit Scoring insbesondere die Grundsätze der Zweckbindung und der Datenminimierung von Bedeutung. Zu untersuchen gilt, ob diese Grundsätze nicht nur dem Wortlaut nach, sondern auch tatsächlich für einen besseren Persönlichkeitsschutz des Betroffenen sorgen, und wie sie sich auf die für Scoring zulässige Datenbasis auswirken.

---

46 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 27 zu Art. 7 DSGVO.

47 Hull, „Successful Failure: What Foucault can Teach Us about Privacy Self-Management in a World of Facebook and Big Data“, (2015), Ethics and Information Technology, Volume 17, Issue 2, 89–101, S. 93; siehe dazu auch Hoffmann-Riem, der die Einwilligung als praktische Ermächtigung zur Ausweitung der Handlungsmacht der Unternehmen bezeichnet: Hoffmann-Riem, “Verhaltenssteuerung durch Algorithmen”, Archiv des öffentlichen Rechts, Bd. 142, S. 1–42, S. 21.

48 Hull, „Successful Failure: What Foucault can Teach Us about Privacy Self-Management in a World of Facebook and Big Data“, (2015), Ethics and Information Technology, Volume 17, Issue 2, 89–101, S. 93.

49 Pötters, Datenschutz-Grundverordnung, Gola (Hrsg.),2017, C. H. Beck Verlag, Rn. 4 zu Art. 5 DSGVO; Frenzel, in: Datenschutzgrundverordnung, Paal/Pauly (Hrsg.), 1. Aufl. 2017, Rn. 2 zu Art. 5 DSGVO, der allerdings eine Unvereinbarkeit der Sanktionsvorschrift mit dem rechtsstaatlich induzierten Bestimmtheitsgebot sieht.

50 Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Nomos Verlag, Rn.1 zu Teil 2: Grundsätze der DSGVO.

51 Reimer, Europäische Datenschutzgrundverordnung, Sydow (Hrsg.), 1. Auflage 2017, Nomos Verlag, Rn. 2 zu Art. 5 DSGVO.

3.1 Zweckbindungsgrundatz als Begrenzung des Big-Data-Scoring?

Der Zweckbindungsgrundsatz, teilweise als beherrschendes Konstruktionsprinzip,[52] Dreh- und Angelpunkt[53] oder Grundstein[54] des Datenschutzrechts bezeichnet, dient der Legitimation der Verarbeitung personenbezogener Daten. Während dieser Grundsatz im BDSG a. F. nicht explizit geregelt war, sondern sich vielmehr als implizite Voraussetzung in den Erlaubnistatbeständen zur Datenerhebung, -verarbeitung und -nutzung des § 4 Abs. 1 BDSG a. F. wiederfand,[55] hat das Zweckbindungsprinzip durch seine ausdrückliche Regelung in Art. 5 Abs. 1 lit. b) DSGVO nun eine eigenständige rechtliche Verbindlichkeit erlangt.

„Personenbezogene Daten müssen 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 Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken“

Der Zweckbindungsgrundsatz wird im Zusammenhang mit der Erhebung der Daten relevant, die zur Scoreberechnung eingesetzt werden. Da die personenbezogenen Daten selten originär für das Scoring erhoben werden, sondern aus bereits bestehenden Datenquellen (z. B. Datenbanken, Verzeichnissen, Information durch andere Unternehmen) herrühren, sind die datenverarbeitenden Unternehmen hier besonders dazu verpflichtet festzustellen, ob der ursprüngliche Zweck für den die personenbezogenen Daten erhoben wurden, auch mit dem Zweck des Scoring kompatibel ist.

Nach dem Zweckbindungsprinzip ist eine anlasslose Datenerhebung nicht zulässig. Klar ist daher, dass die Zweckbestimmung zumindest präzise formuliert sein muss.[56] Angesichts der Hinweis- und Warnfunktion des Zweckbindungsgrundsatzes muss ausgehend vom objektiven Empfängerhorizont für den Betroffenen erkennbar sein, wofür die Daten genau verwendet werden, ohne dass es zu Zweifeln oder Mehrdeutigkeiten kommt.[57]

Allerdings wird der Zweckbindungsgrundsatz weit ausgelegt, so dass eine weite Zweckdefinition in Datenschutzbestimmungen von der überwiegenden Meinung angesichts fehlender anderweitiger Vorgaben für rechtlich zulässig erachtet.[58] Dabei wird kritisiert, dass im Rahmen dieser Regelung offen bleibt, auf welcher Abstraktionsebene ein Zweck zu bestimmen ist. Insbesondere im Hinblick auf die Frage, ob es im Laufe der Datenverarbeitung zu einer Zweckänderung kommt, müsse festgelegt werden, ob sich der Zweck etwa auf den Geschäftstyp des Verarbeiters (Auskunftei) oder eher auf das jeweilige Vertragsverhältnis (Durchführung einer Bonitätsabfrage) zu beziehen hat.[59] Dies ist wegen der oben beschrieben Probleme bei der Einwilligung im Scoring und Datenerhebungen wichtig.

Neben der Festlegung auf einen bestimmten Zweck legt das Zweckbindungsprinzip fest, dass einmal für bestimmte Zwecke erhobene Daten nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen (Zweckbindung im enge-

---

52 Schantz, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.02.2017, Rn. 13 zu Art. DSGVO Art. 5.

53 Frenzel, Datenschutzgrundverordnung, Paal/Pauly (Hrsg.), 1. Aufl. 2017, Rn. 23 zu Art. 5 DSGVO.

54 Schantz, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.02.2017, Rn. 12 zu Art. 5 DSGVO (als Zitat der Wendung „cornerstone of data protection law“ der Artikel 29-Arbeitsgruppe, WP 203).

55 Ziegenhorn/von Heckel, „Datenverarbeitung durch Private nach der europäischen Datenschutzreform“, (2016), Neue Zeitschrift für Verwaltungsrecht, Heft 22, S. 1585–1591, S. 1589.

56 Ziegenhorn/von Heckel, „Datenverarbeitung durch Private nach der europäischen Datenschutzreform“, (2016), Neue Zeitschrift für Verwaltungsrecht, Heft 22, S. 1585–1591, S. 1589; Culik/Döpke, „Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen“, (2017), Zeitschrift für Datenschutz, Heft 5, S. 226–230, S. 227; Artikel 29-Arbeitsgruppe, WP 203, S. 15 f.

57 Helbing, „Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung“, (2015), Kommunikation & Recht, Heft 3, S.145–150, S. 146.

58 Culik/Döpke, „Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen“, (2017) Zeitschrift für Datenschutz, Heft 5, S. 226–230, S. 227; Härting, „Zweckbindung und Zweckänderung im Datenschutzrecht“, (2015), Neue Juristische Wochenschrift, Heft. 45, S. 3284–3288, S. 3286 f; a. A. Schantz, „Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht“, (2016) Neue Juristische Wochenschrift, Heft 26, S. 1841–1847, S. 1843.

59 Dammann, „Erfolge und Defizite der Datenschutzgrundverordnung“, (2016), Zeitschrift für Datenschutz, Heft 7, S. 307–314, S. 312.

ren Sinne). Im zweiten Halbsatz von Art. 5 Abs. 1 lit. b) DSGVO finden sich allerdings drei Ausnahmen vom engen Zweckbindungsverständnis. Zudem bedeutet Zweckbindung i. e. S. auch nicht, dass die Datenverarbeitung absolut an einen Zweck gebunden ist, solange die neue Art der Datenverarbeitung im Rahmen eines sog. Kompatibilitätstests mit dem ursprünglichen Zweck als vereinbar erscheint.[60]

Der Zweckbindungsgrundsatz verfolgt das Ziel, Transparenz und Nachvollziehbarkeit bei der Verarbeitung personenbezogener Daten zu schaffen.[61] Er hat zwar das Potenzial, einen allzu leichtfertigen Umgang bzw. Handel mit personenbezogenen Daten zu begrenzen. Solange aber die Datenerhebung von einem präzise formulierten, aber inhaltlich potenziell durchaus weiten Verwendungszweck gedeckt ist, ist die nachfolgende Verarbeitung jedenfalls nach dem Zweckbindungsprinzip zulässig. Das zeigt, dass die unterschiedlichen Ausnahmen zum Zweckbindungsgrundsatz Big-Data-Anwendungen nicht grundsätzlich in Frage stellen. [62]Für Scoring bedeutet das, dass auf Big-Data-Analysen basierenden Scoring-Geschäftsmodelle nach dem Zweckbindungsprinzip der DSGVO zulässig sind.

3.2 Vereinbarkeit von Scoring mit dem Grundsatz der Datenminimierung

Der Grundsatz der Datenminimierung ist in Art. 5 Abs. 1 lit. c) DSGVO niedergelegt:

„Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein."

Auch der Grundsatz der Datenminimierung ist in der DSGVO verschärft worden, was sich u. a. aus der Formulierung ergibt, nach der (in der englischen Fassung noch deutlicher) eine Datenverarbeitung nicht mehr nur „not excessive" sein muss, sondern vielmehr „limited to what is necessary".[63] Während § 3a BDSG a. F. unter den Schlagwörtern „Datenvermeidung und Datensparsamkeit" bislang überwiegend formelle Anforderungen an die Datenverarbeitung in Form der Anonymisierung und Pseudonymisierung personenbezogener Daten stellte, hat der Grundsatz der Datenminimierung in der DSGVO zum Ziel, dass im Rahmen der Zweckbindung die Daten nicht nur quantitativ, sondern auch qualitativ begrenzt werden müssen, wobei sich aus dem Begriff der „Minimierung" im Vergleich zu „Sparsamkeit" eine möglichst weitgehende Begrenzung ableiten lässt.[64]

Dabei ist allerdings fraglich, welchen Inhalt die in Art. 5 Abs. 1 lit. c) DSGVO genannten Begriffe der Angemessenheit, Erheblichkeit und der Beschränkung auf das für die Verarbeitung notwendige Maß im Einzelnen an die Datenverarbeitung haben. Teilweise wird der Grundsatz der Datenminimierung als eine Ausprägung des Verhältnismäßigkeitsgrundsatzes verstanden.[65] Die Artikel 29 Datenschutzgruppe stellt hinsichtlich automatisierter Datenverarbeitung nach Art. 22 DSGVO fest, dass die Verantwortlichen zur Einhaltung des Prinzips der Datenminimierung ihr Bedürfnis zur Sammlung personenbezogener Daten rechtfertigen können sollten oder andernfalls erwägen sollten, aggregierte, anonymisierte oder (sofern ausreichend sicher) pseudonymisierte Daten zu verwenden.[66]

Hinsichtlich der Einhaltung des Grundsatzes der Datenminimierung besteht eine Rechenschaftspflicht des Datenverarbeiters nach Art. 5 Abs. 2 DSGVO. Wie

---

60 Albers, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 22. Edition, Stand: 01.11.2017, C. H. Beck Verlag, Rn. 68 ff. zu Art. 6 DSGVO.

61 Frenzel, Datenschutz-Grundverordnung, Paal/Pauly (Hrsg.), 1. Aufl. 2017, Rn. 27 zu Art. 5 DSGVO.

62 Culik/Döpke, „Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen", (2017), Zeitschrift für Datenschutz, Heft 5, S. 226–230, S. 230.

63 Schantz, „Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht", (2016), Neue Juristische Wochenschrift, Heft 26, S. 1841–1847, S. 1843. So auch Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Nomos Verlag, Rn. 6 zu Teil 2: Grundsätze der DSGVO.

64 Frenzel, Datenschutz-Grundverordnung, Paal/Pauly (Hrsg.), 1. Aufl. 2017, Rn. 34 zu Art. 5 DSGVO.

65 So im Detail: Schantz, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.02.2017, Rn. 24 ff. zu Art. DSGVO Art. 5. Andere Auslegung bei: Frenzel, Datenschutz-Grundverordnung, Paal/Pauly (Hrsg.), 1. Aufl. 2017, Rn. 34 ff. zu Art. 5 DSGVO. Pötters weist darauf hin, dass Datensparsamkeit vor allem auch die mehrfache Nutzung von Daten einschränkt: Pötters, Datenschutz-Grundverordnung, Gola (Hrsg.), 2017, C. H. Beck Verlag, Rn. 22 zu Art. 5 DSGVO.

66 Artikel 29-Arbeitsgruppe, WP 251: „Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation", S. 11.

aber kann der scorende Datenverarbeiter ggf. die Verhältnismäßigkeit bzw. begrenzte Datennutzung nachweisen? Reicht allein das Bestehen einer statistischen **Korrelation** zwischen den erhobenen Daten und dem verfolgten Zweck für die Einhaltung des Grundsatzes der Datenminimierung aus? Natürlich schließt sich hier die Frage an, welche Stelle die Einhaltung der Vorschriften in dieser Detailtiefe überhaupt überprüfen kann. Letztendlich kann es sich hier nur um einen Maßstab handeln, der der Bewertung streitiger Einzelfälle dient. Der Grundsatz der Datenminimierung damit weniger geeignet, ein Datenverarbeitungsverfahren insgesamt auf seine Datensparsamkeit hin zu bewerten und systemimmanente Defiziten zu korrigieren.

Im Ergebnis dürfte auch auf großen Datenmengen beruhendes Scoring mit dem Grundsatz der Datenminimierung zu vereinbaren sein, sofern die Datenverarbeiter nachweisen können, dass ihre Berechnungen nicht in gleicher Weise mit weniger oder anderen Daten angestellt werden können und der Nutzen des Scoring nicht außer Verhältnis zur Beeinträchtigung der Interessen des Betroffenen stehen.

4. Zwischenergebnis

Festzuhalten ist zunächst, dass Scoring i. S. d. § 31 BDSG n. F. primär dem Schutz des Wirtschaftsverkehrs dient. Dies ergibt sich schon aus dem Titel des § 31 BDSG n. F. Dieser Schutzzweck mag auch die diversen Schutzlücken erklären, die im Bezug auf den Datenschutz des Betroffenen entstehen. Einige dieser Schutzlücken mögen dem Umstand geschuldet, dass das BDSG n. F. anders als sein Vorgängergesetz als Ergänzung eines anderen Regelungswerkes, der DSGVO, konzipiert ist. Der deutsche Gesetzgeber hatte damit die Möglichkeit, Regelungsspielräume auszuschöpfen und strengere oder mildere Vorschriften zu erlassen. Im Hinblick auf die Datenverarbeitung haben wir gesehen, dass der Gesetzgeber die Anforderungen oftmals gelockert hat.

So ist beispielsweise eine Kopplung von Vertragsschluss und Datenverarbeitung nicht mehr gänzlich ausgeschlossen. Es ist außerdem die Voraussetzung weggefallen, dass personenbezogene Daten „geschäftsmäßig“ nur dann genutzt werden dürfen, wenn dem kein schutzwürdiges Interesse des Betroffenen entgegensteht. Abgesehen von den Problemen, das schutzwürdige Interesse des Betroffenen festzustellen, ist es konzeptionell bedenklich, dass eine solche Schnutznorm nicht weitergeführt wird.

Außerdem stellen beispielsweise Art. 22 Abs. 2 DSGVO, § 37 BDSG n. F. mehrere Ausnahmen auf, die dazu führen, dass die potenziell weitreichenderen Normen nicht auf Scoring anwendbar sind. Dies gilt insbesondere für den Fall, dass der Betroffene in die automatisierte Datenverarbeitung einwilligt oder die automatisierte Entscheidung für den Abschluss oder die Erfüllung eins Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Eine automatisierte Entscheidung ist zudem auch im Rahmen der Leistungserbringung nach einem Versicherungsvertrag zulässig, soweit dem Begehren der betroffenen Person stattgegeben wurde.

Der Zweck des § 31 BDSG n. F., den Wirtschaftsverkehr zu schützen, spiegelt sich auch in der Zentralität der Einwilligung für das Datenschutzrecht wider. Dabei ist die Ineffektivität der Einwilligung als Erlaubnistatbestand für die Datenverarbeitung eines der Hauptprobleme im Datenschutzrecht. Dass die Einwilligung teils zur Umgehung eigentlich Schutz bietender Vorschriften wie etwa Art. 9 DSGVO vergleichsweise einfach herangezogen werden kann, ist aus verbraucherschützender Perspektive bedenklich. Es stellt sich die Frage, ob es nicht Bereiche im Datenschutzrecht geben sollte, in denen die Einwilligung des Betroffenen keine die Datenverarbeitung rechtfertigende Wirkung entfalten sollte. Insbesondere für die Verarbeitung besonderer Kategorien personenbezogener Daten wäre dies zu erwägen.

Etwaige Lösungsvorschläge sind bisher nicht vom Gesetzgeber aufgegriffen worden. Die Forderung, die Einwilligung wegen der unscharfen, aber nach der DSGVO wohl zulässigen Zweckbestimmungen der Datenverarbeitung nicht als Rechtfertigungsgrund bei Big-Data-Analysen gelten zu lassen, wird teilweise als Entmündigung des Betroffenen bezeichnet. Alternativ wird vorgeschlagen, dass die betroffene Person von vornherein bestimmte Verwendungszwecke zulassen bzw. ausschließen kann oder zunächst nur in die Datenverarbeitung und an-

schließend in die Nutzung des Ergebnisses einwilligt.[67] Es wird auch überlegt, Einwilligungen für Big-Data-Analysen grundsätzlich nur zeitlich begrenzt zu ermöglichen.[68] Darüber hinaus bedarf es auch einer Auseinandersetzung mit der Frage, wie die Informiertheit und Freiwilligkeit des Betroffenen über die umfangreichen theoretischen Anforderungen hinaus auch praktisch erreicht werden kann. Art. 42 DSGVO bietet bereits einige Lösungsansätze. Auch der Vorschlag des „One Pagers“[69] sollte diskutiert werden. Bisher haben solche Vorschläge keinen Eingang in die gesetzlichen Regelungen gefunden.

Außerdem zeigt ein Blick auf die Grundsätze der Zweckbindung und Datenminimierung, dass in den Einzelheiten unklar ist, wie die Grundsätze insbesondere im Zeitalter von Big Data bei Scoring operationalisiert und durchgesetzt werden können. Insbesondere der Grundsatz der Datenminimierung stellt zwar den Anspruch, die verarbeitete Datenbasis auch qualitativ zu fördern, in der Praxis dürfte er aber eher als Maßstab für Bewertungen individueller Problemfälle dienen als für die Gewährleistung insgesamt datensparsamer Verarbeitungssysteme. Der Datenminimierungsgrundsatz wird überwiegend eng ausgelegt und angewandt. In Bezug auf den Zweckbindungsgrundsatz ist das Problem dagegen die weite Auslegung, so dass Unternehmen bei der Festlegung des Zwecks ihrer Datenverarbeitung großen Spielraum haben. Der verhältnismäßig stark schutzorientierte Wortlaut der entsprechenden Regelungen läuft in der Praxis damit ins Leere.

67 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 32 zu Art. 7 DSGVO.

68 Martini, „Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht“, (2014), Deutsches Verwaltungsblatt, Heft 23, S. 1481–1489, S. 1486.

69 Siehe z. B. die Forderung des SVRV nach der Einführung eines One-Pagers in SVRV, Digitale Souveränität, 2017, S. 20 f.

IV Problem: Datenbasis

In diesem Abschnitt befassen wir uns mit der Frage der Anforderungen an die für Scoring genutzte Datenbasis. Problematisch ist insbesondere die Richtigkeit und Aussagekraft, sowie die Verwendung besonders sensibler Daten wie Geschlecht oder gesundheitsbezogene Daten. Unternehmen werben z. B. zunehmend damit, dass Daten aus sozialen Netzwerken benutzt werden, um Kreditfähigkeit besser zu bestimmen.[70] Die Nutzung bestimmter Daten für die Herstellung von Wirkungszusammenhängen ist aber gesellschaftspolitisch nicht unumstritten. Hierzulande hat die Schufa beispielsweise einen Pilotversuch zur Einbeziehung von aus Facebook generierten Daten in die Scorewertberechnung aufgrund öffentlicher Kritik einstellen müssen.[71]

Das zugrundliegende Problem liegt in den Versprechen von Big-Data-Analysen zur Entdeckung von Wirkungszusammenhängen und der Erstellung von Persönlichkeitsprofilen und Verhaltensmustern. Dabei werden für Big-Data-Analysen möglichst viele Daten gesammelt und verarbeitet, um noch präzisere Aussagen über Verhaltensmuster treffen zu können. Darüber hinaus basiert Scoring auf der Entdeckung zugrundeliegender Wirkungszusammenhänge zwischen Merkmalen und dem zu bestimmenden Verhalten in Form von statistisch auftretenden Korrelationen. Diese datenbasierten Analysen versprechen bisher unbekannte Zusammenhänge zwischen verschiedenen Phänomenen aufzeigen zu können. Es ist dabei sowohl möglich, dass tatsächlich ein Wirkungszusammenhang zwischen z. B. dem Wohnort einer Person und der Wahrscheinlichkeit mit der sie eine Rechnung bezahlen wird, besteht, als auch, dass diese beiden Merkmale rein zufällig oder aufgrund einer anderen Ursache nebeneinander auftreten. Die Frage nach dem Ursachenzusammenhang oder gar der Kausalität zwischen den verschiedenen Merkmalen wird im Rahmen solcher Analysen nicht gestellt.[72] Damit stellen sich Fragen nach der Präzision der für Scoring genutzten Daten. Außerdem ergeben sich Probleme der Privatsphäre und der Möglichkeit zur Diskriminierung.

1. Richtigkeit und Aussagekraft der Daten

Immer wieder werden Fälle bekannt, in denen es bei Verbrauchern zu schlechten Scorewerten aufgrund von Namensverwechslungen oder veralteten und mittlerweile unrichtigen Daten kommt.[73] Es stellt sich deshalb die Frage, welche Maßnahmen das Datenschutzrecht bietet, um die Richtigkeit der verwendeten Daten bei Scoring sicherzustellen. Im Rahmen des BDSG a. F. war anerkannt, dass die Richtigkeit der Daten im Fall geschäftsmäßiger Datenerhebung und -speicherung zum Zweck der Übermittlung an Auskunfteien (§ 29 BDSG a. F.) eine Rolle spielte. Die hier erforderliche Interessenabwägung fiel bei unrichtigen Daten stets zugunsten des Betroffenen aus, da aus juristischer Sicht die verarbeitende Stelle kein Interesse an der Erhebung und Verarbeitung falscher Daten haben konnte.[74] Dies wurde auch daran deutlich, dass es bei der Berichtigungspflicht der verantwortlichen Stelle gem. § 35 Abs. 1 BDSG a. F. keiner Interessenabwägung mehr bedurfte.[75]

Es war allerdings unklar, ob die datenverarbeitende Stelle (Auskunftei, Unternehmen) eine Pflicht zur Überprüfung der Richtigkeit der Daten hat. Im BDSG a. F. gab es eine solche Prüfpflicht bislang nur, wenn ein entgegenstehendes schutzwürdiges Interesse des Betroffenen angenommen werden musste (§ 29 Abs. 2 Nr. 2 BDSG a. F.). Dies bedeutete, dass die Erhebung und Verarbeitung falscher Daten zugelassen wurde, sofern der Betroffene keine Indizien für deren Unrichtigkeit

---

70 Zum Beispiel die Firma Kreditech: https://www.golem.de/news/kreditech-deutsches-startup-bekommt-40-millionen-us-dollar-1406–107421.html.

71 Siehe dazu: http://www.spiegel.de/netzwelt/web/schufa-will-kreditdaten-bei-facebook-sammeln-a-837454.html (zuletzt abgerufen am (05.04.2018).

72 Dazu: Martini, „Big Data als Herausforderung für den Persönlichkeitsschutz“, (2014), Deutsches Verwaltungsblatt, Heft 23, S. 1481–1489, S. 1485.

73 http://www.sueddeutsche.de/geld/auskunftsdatei-fuer-kreditvergabe-tipps-zum-umgang-mit-der-schufa-1.1768547 (zuletzt abgerufen am 16.05.2018)

74 Dazu Buchner, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.02.2017, C. H. Beck Verlag, Rn. 66 zu § 29 BDSG; Grundlegend zur Schutzwürdigkeit der Betroffeneninteressen bei unvollständigen oder veralteten Daten von Auskunfteien BGH NJW 1984, 1890 f.

75 Ehmann, Bundesdatenschutzgesetz, Simits (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 170 zu § 29 BDSG.

vortragen konnte.[76] Es oblag daher dem Betroffenen, die Richtigkeit seiner Daten festzustellen und sodann Berichtigung zu verlangen. Dies war angesichts der Probleme bei der Durchsetzung von Auskunftsrechten[77] bedenklich. Daher wurde vorgeschlagen, der datenverarbeitende Stelle die Pflicht aufzuerlegen, die dem Betroffenen aus der Erhebung und Verwendung falscher Daten erwachsenden Nachteile und Schäden zu mindern; dies sollte beispielsweise durch ein „risikoorientiert angelegtes Stichprobenkonzept" erreicht werden, mit dessen Hilfe geprüft wird, ob übermittelte Daten zutreffen, oder durch automatisierte Schlüssigkeitsprüfungen oder Vertragsstrafenvereinbarungen für den Fall, dass sich übermittelte Daten, die erhoben wurden, als unrichtig erweisen.[78] Zudem wurde eine lückenlose Rückverfolgbarkeit der Datenherkunft gefordert.[79]

Ob sich an diesem Diskussionsstand mit der DSGVO etwas ändert, ist derzeit nicht abzusehen. Nach Art. 5 Abs. 1 lit. b) DSGVO muss die verantwortliche Stelle alle Maßnahmen treffen, „damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden" können.[80] Außerdem hält Erwägungsgrund[81] 71 Satz 6 DSGVO fest, dass der für das „Profiling" Verantwortliche technische und organisatorische Maßnahmen ergreifen soll,

„mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird".

Allerdings wird Art. 5 Abs. 1 lit. b) DSGVO dahingehend interpretiert, dass die verantwortliche Stelle aktiv die Richtigkeit der erhobenen und genutzten Daten überprüfen muss.[82] Die Einführung dieses nun allgemeingültigen Grundsatzes ist für die systemübergreifende Gewährleistung einer gewissen Datenqualität grundsätzlich positiv zu beurteilen. Andererseits ist die Berichtspflicht aus § 28a Abs. 3 BDSG a. F. weggefallen. Sie verlangte, dass bei Änderung von Daten, die an eine Auskunftei übermittelt wurden, eine Mitteilung der verantwortlichen Stelle an die Auskunftei zu erfolgen hat. Es bleibt abzuwarten, ob dies durch die Pflicht der verantwortlichen Stelle für Datenrichtigkeit zu sorgen, aufgefangen werden kann. Außerdem ist Bezug des Art. 5 Abs. 1 lit. B) DSGVO auf den Zweck der Verarbeitung unklar.

Die tatsächliche Aussagekraft der für die Scorecard genutzten Daten kann nicht nur durch mangelnde Richtigkeit, sondern auch durch die Verwendung von Schätzdaten geschmälert sein. Schätzdaten sind Daten, die beim Berechnen des Scores einer Person nicht vorliegen und deshalb aus anderen, vorliegenden Daten abgeleitet werden. Ein Beispiel ist die Altersschätzung anhand des Vornamens oder die Herleitung des Familienstands einer Person aus öffentlich zugänglichen Verzeichnissen (z. B. Adressbuch).[83] Das Problem dabei ist, dass solche Daten losgelöst von den tatsächlichen Eigenschaften und Verhaltensweisen des Betroffenen sind. § 31 BDSG n. F. stellt allerdings keine Hürden in dieser Hinsicht auf.

Der Bundesrat wollte in seinen Empfehlungen zum Gesetzesentwurf des § 28b BDSG a. F. eine Regelung einführen, wonach Schätzdaten nicht für die Berechnung

76 Ehmann, Bundesdatenschutzgesetz, Simits (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 173 zu § 29 BDSG.

77 Siehe dazu Spindler/Thorun/Wittmann, „Rechtsdurchsetzung im Verbraucherdatenschutz. Bestandsaufnahme und Handlungsempfehlungen", 2017, Studie für die Friedrich-Ebert-Stiftung.

78 Ehmann, Bundesdatenschutzgesetz, Simits (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 174 zu § 29 BDSG.

79 Ehmann, Bundesdatenschutzgesetz, Simits (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 174 zu § 29 BDSG.

80 Unterstützt wird diese Pflicht durch das Berichtigungsrecht des Betroffenen, Art. 16 DSGVO, § 58 BDSG n. F. Allerdings trägt der Betroffene die Beweislast für die Unrichtigkeit der Daten, was vor dem Hintergrund der mangelnden Transparenz der eingesetzten Datenbasis schwierig ist, s. dazu Paal, DS-GVO, BDSG, Paal/Pauly (Hrsg.), 2. Auflage 2018, C. H. Beck Verlag, Rn. 15 zu Art. 16 DSGVO.

81 Die Verbraucherzentrale Bundesverband (vzbv) kritisiert, dass sich Schutzgewährleistungen für Betroffene in der DSGVO oft nur in den Erwägungsgründen finden, was diese schwäche und ihre rechtliche Verbindlichkeit in Zweifel ziehe, s. http://www.vzbv.de/sites/default/files/vzbv_kurzbewertung_ds-gvo.pdf (zuletzt abgerufen am 01.03.2018).

82 Pötters, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 24 zu Art. 5 DS-GVO.

83 ULD Schleswig-Holstein / GP Forschungsgruppe, Scoring nach der Datenschutznovelle 2009 und neue Entwicklungen, (2014), S. 34.

des Score-Wertes verwendet werden dürfen.[84] Als Begründung führte er aus, dass die Aussagekraft von Wahrscheinlichkeitswerten durch die Verwendung von Schätzdaten gemindert wird. Dieser Vorschlag des Bundesrates fand jedoch keinen Eingang in das BDSG a. F.. Der Bundesregierung ging das Verbot von Schätzdaten zu weit, weil diese bereits der Kennzeichnungspflicht nach § 35 Abs. 1 BDSG a. F. unterlagen und weil ohnehin nur „richtige" Daten verwendet werden dürfen; diese „besonders hohen Anforderungen" sah die Bundesregierung als ausreichend an.[85] Dies bedeutet, dass Schätzwerte nicht als unrichtig anzusehen sind, sofern sie gem. § 35 BDSG a. F. gekennzeichnet waren.[86]

Das BDSG n. F. greift dagegen die Kennzeichnungspflicht für Schätzdaten nicht wieder auf. Auch die DSGVO verlangt keine explizite Kennzeichnung. Lediglich Erwägungsgrund 71 DSGVO wird dahingehend interpretiert, dass nicht entsprechend gekennzeichnete Informationen i. d. R. als unrichtig eingestuft werden müssen, da sie suggerieren, eine tatsächliche Eigenschaft des Betroffenen zu betreffen, obschon es sich in Wirklichkeit nur um eine Eigenschaft handelt, die mit einiger Wahrscheinlichkeit auf den Betroffenen zutrifft.[87]

2. Wissenschaftlichkeit des Scoringverfahrens

Um sicherzustellen, dass nur solche Daten zur Scorewert-Berechnung verwendet werden, mit denen das jeweilige Verhalten einer Person tatsächlich bestimmt werden kann, stellt § 31 Abs. 1 BDSG n. F. die Bedingung auf, dass die Erheblichkeit der Daten unter Zugrundlegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahren nachweisbar sein muss. Das Scoring darf somit nicht auf „Bauch-Faktoren" basieren, wenn diese keine statistische Signifikanz haben.[88]

2.1 Erheblichkeit der Daten für den Score

Es verbleibt die Frage, in welcher Beziehung die geforderte Erheblichkeit der Daten beim Scoring aus § 31 Abs. 1 BDSG n. F. (dazu mehr unter IV.2.1) zu den Anforderungen aus dem Grundsatz der Datenminimierung, insbesondere der dort erwähnten Erheblichkeit der Daten, steht.[89]

Wie und von wem die Erheblichkeit der verwendeten Daten für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens festzustellen ist, lässt der Gesetzgeber jedoch offen. Dies lässt Raum für eine weite Auslegung des Merkmals der Erheblichkeit. Aus der Tatsache, dass die Verwendung von Schätzdaten beim Scoring nicht ausgeschlossen ist, wird gefolgert, dem jeweiligen Datenverarbeiter stehe bei der Beurteilung

84 BR-Drs. 548/1/08, S. 13.

85 BT-Drs. 16/10581, S. 3.

86 Ehmann, Bundesdatenschutzgesetz, Simits (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 171 zu § 29 BDSG

87 Reif, Datenschutz-Grundverordnung, Gola (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 16 zu Art. 16 DSGVO.

88 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 31.1 zu § 28b BDSGa. F. Dazu befinden sich weitere Informationen in: Hessischer Landtag, Vorlage der Landesregierung betreffend den Sechzehnten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, S. 20ff, abrufbar unter: http://starweb.hessen.de/cache/DRS/16/0/01680.pdf, und in ULD Schleswig-Holstein, Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, (Gutachten im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft – BMVEL –, 2005), S. 49 ff. (für das Beispiel des Kredit-Scorings).

89 Unter Berücksichtigung der unterschiedlichen Regelungsbereiche des § 31 Abs. 1 BDSG n. F. und Art. 5 DSGVO mussten die Voraussetzungen beider Normen vorliegen. D. h., dass aus der außerdem explizit erwähnten Erheblichkeit der Daten in § 31 Abs. 1 BDSG n. F. eine zusätzliche Anforderung an den Datenverarbeiter abzuleiten ist. Im Gegensatz zu § 31 Abs. 1 BDSG n. F. verlangt der Grundsatz der Datenminimierung nicht den Einsatz eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens zum Nachweis der Erheblichkeit der Daten. Somit kann davon ausgegangen werden, dass im Rahmen der Datenminimierung bereits eine Interessenabwägung, wie es zur Durchführung der Verhältnismäßigkeitsprüfung geboten ist, ausreicht. Demgegenüber stellt § 31 Abs. 1 BDSG n. F. höhere Anforderungen an die Art und Weise, wie der Nachweis der Erheblichkeit der eingesetzten Daten zu erbringen ist.

der Erheblichkeit ein großer Beurteilungsspielraum zu. Mangels anders lautender, einschränkender gesetzlicher Angaben ist davon auszugehen, dass die in § 31 BDSG n. F. geforderte Erheblichkeit der Daten tatsächlich besteht, sofern ein wie auch immer gearteter statistischer Wirkungszusammenhang zwischen dem fraglichen Merkmal und der zu bestimmenden Wahrscheinlichkeit des Verhaltens festgestellt wurde. Damit reicht der Spielraum des Datenverarbeiters bis zur Grenze reiner Spekulation.[90] Aufgrund dieses weiten Auslegungsspielraums ist § 31 Abs. 1 BDSG n. F. Kritik und der Forderung nach Konkretisierung ausgesetzt.[91] Es seien weitere Erwägungen anzustellen, um über eine wissenschaftlich-statistische Signifikanz der Daten hinaus die Relevanz der Daten für den verfolgten Zweck sicherzustellen. Dazu zähle, dass je nach Art des konkreten Vertragsverhältnisses ein unmittelbarer Zusammenhang zwischen dem jeweiligen Sachverhalt und dem zu bewertenden Merkmal, wie z. B. der Kreditwürdigkeit einer Person, bestehen muss. Dieses als Vertragsrelevanz bezeichnete Merkmal erfüllen nur solche Daten, die einen unmittelbaren Einfluss auf für den jeweiligen Vertrag wichtige Vertragspflichten haben.[92] Im Bereich des Kreditscoring werden dafür beispielhaft solche Daten genannt, die mit dem Vermögen und Einkommen des Betroffenen in direktem Zusammenhang stehen. Erhebungen in Bezug auf den Wohnort, das Geschlecht, den Haushalt, die Anzahl der Kinder oder den Kfz-Besitz seien dagegen nicht als relevant anzusehen.

Ein weiteres Problem wird außerdem in der Tatsache gesehen, dass nicht nur irrelevante Daten Einfluss auf die Bewertung der Kreditwürdigkeit einer Person haben könnten, sondern darüber hinaus eigentlich relevante Daten zum Teil keine Berücksichtigung bei der Bewertung fänden.[93] In der Rechtsprechung gibt es zwar einige Fälle zu diesem Problem; einheitliche Maßstäbe können jedoch noch nicht aufgestellt werden. Beispielsweise hat das OLG Frankfurt a. M. festgestellt, dass nicht aussagekräftige Kriterien nicht verwendet und offensichtlich signifikante Faktoren nicht außer Acht gelassen werden dürfen.[94] Das OLG stellte fest, dass die Verwertung nur eines Merkmals als Einzelfaktor in einem Scoringverfahren dem Maßstab der komplexen, auf statistischen und wissenschaftlichen Algorithmen beruhenden Bewertung nicht genügt.[95] In dem Fall hatte eine Ratingagentur einem Unternehmen einen schlechten Bonitätscore erteilt, der lediglich darauf gestützt war, dass es sich um einen Einzelkaufmann handele, den keine Kapitalnachweispflicht treffe. Die Agentur berief sich auf ihre Meinungsfreiheit, für die es keine Rolle spiele, ob Kreditwürdigkeitsprüfungen wahr oder falsch seien. Das Gericht sah dies als „verantwortungslose Oberflächlichkeit“ an. Allerdings stellte das OLG München 2014 fest, dass sich für Betroffene kein Anspruch auf eine „vollständige“ Bewertung aus § 28b BDSG a. F. ableiten lasse. Der Gesetzgeber akzeptiere, dass Scoring-Verfahren nur einen Ausschnitt der über eine Person verfügbaren Informationen berücksichtige, solange für die Berechnung ein mathematisch-statistisches Verfahren angewendet werde.[96] Diese Beurteilung dürfte sich auch durch § 31 Abs. 1 BDSG n. F. nicht geändert haben.

Ob das Recht des Betroffenen auf Vervollständigung unvollständiger personenbezogener Daten aus Art. 16 S. 2 DSGVO die bislang geltenden Rechtslage zu ändern vermag, bleibt abzuwarten. Überwiegend wird davon ausgegangen, dass ein solches Recht bereits implizit aus §§ 20 Abs. 1, 35 Abs. 1 BDSG a. F. hervorging,[97] so dass sich durch die nun explizite Regelung keine Änderungen ergeben dürften. Wenngleich dies aus verbraucherschützender Sicht ein unbefriedigendes Ergebnis sein mag, kann als Argument hinzugefügt werden, dass

90 Wäßle/Heinemann, „Scoring im Spannungsfeld von Datenschutz und Informationsfreiheit“, (2010), Computer und Recht, Heft 6, S. 410–416, S. 412

91 Die Ausführungen beziehen sich hier insbesondere auf das Kreditscoring. ULD Schleswig-Holstein, Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, (Gutachten im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft – BMVEL –, 2005), S. 75 ff.

92 Siehe dazu auch: Petri, „Ist Credit-Scoring rechtswidrig?“, in: Sokol (Hrsg.) Living by numbers. Leben zwischen Statistik und Wirklichkeit“, S. 111–121.

93 ULD Schleswig-Holstein, Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, (Gutachten im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft – BMVEL –, 2005), S. 75.

94 OLG Frankfurt, Urteil vom 07.04.2015 – Az. 24 U 82/14.

95 OLG Frankfurt, Urteil vom 07.04.2015 – Az. 24 U 82/14.

96 OLG München, Urteil vom 12.03.2014 – 15 U 2395/13.

97 Worms, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 23. Edition, Stand 01.08.2017, C. H. Beck Verlag, Rn. 42 zu Art. 16 DSGVO.

der Zweck des Datenschutzrechts gem. Art. 1 Abs. 2 DSGVO in dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten besteht und sich aus diesem Schutzauftrag kein Anspruch auf eine vollständige Darstellung der eigenen Person ableiten lässt. Die Nichtberücksichtigung möglicherweise erheblicher Daten beim Scoring ist demnach nach geltendem Datenschutzrecht zulässig.

2.2 Anforderungen an die Wissenschaftlichkeit

§ 31 Abs. 1 Nr. 2 BDSG n. F. besagt, dass die Erheblichkeit der Daten für das Scoring unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachzuweisen ist. Ähnlich führt Erwägungsgrund 71 der DSGVO aus, dass zur Gewährleistung einer fairen und transparenten Verarbeitung personenbezogener Daten, der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden sollte.[98] Es werden jedoch keine konkreten technischen oder wissenschaftlichen Anforderungen an automatisierte Datenverarbeitungen wie Scoring gestellt. Dies ist problematisch, weil die wissenschaftliche Anerkennung des eingesetzten Verfahrens durch die Aufsichtsbehörden nachvollzogen werden muss.

Welche statistischen Maße anerkannt sind und welche Güte diese erreichen müssen, ist momentan unklar. Einige Auskunfteien verwenden den sogenannten Gini-Koeffizienten als Maßstab zur Abbildung der Güte ihres Berechnungsmodells.[99] Der Gini-Koeffizient ist ein statistisches Maß, das zur Darstellung von Ungleichverteilungen entwickelt wurde. Die Verwendung des Gini-Koeffizienten wird im Bankwesen als Maß dafür verwendet, wie gut ein Ratingsystem gute von schlechten Schuldnern trennen kann, und trifft damit eine Aussage über die sogenannte Trennschärfe des Modells, also des zur Berechnung von Scores eingesetzten Algorithmus. Die Trennschärfe wird beim Scoring auch mit der Exaktheit der getroffenen Aussagen bzw. der Prognosequalität in Beziehung gesetzt.[100] Es gibt aber noch weitere statistische Methoden zur Berechnung der Güte von Scoring-Modellen gibt, Bisher wurde von Aufsichtsbehörden anerkannt, dass logistische Regressionsmodelle den „Wissenschaftlichkeits"-Anforderungen genügen.[101]

Nach zum Teil vertretener Ansicht soll es ausreichen, dass das angewandte Verfahren im Sinne der Wissenschaftlichkeit evident sei,[102] beziehungsweise, dass das Verfahren wissenschaftlichen Ansprüchen genüge.[103] Von anderer Seite wird darauf hingewiesen, das Merkmal des wissenschaftlich anerkannten mathematisch-statistischen Verfahrens habe weniger eine materielle Bedeutung und diene hauptsächlich dem Zweck, den Aufsichtsbehörden die Überprüfung der Einhaltung der Vorschriften zu erleichtern.[104] Diese Auffassung sieht sich dem Einwand ausgesetzt, dass der Maßstab der Kontrolltätigkeit trotzdem unklar bleibt.

Außerdem wird auch ein Vergleich auf ähnlich gelagerte Vorschriften in §§ 107 Abs. 1 Nr. 2, 121a Abs. 2 Nr. 1 SGB V oder § 6 Abs. 2 Beihilfeverordnung (BhVO) herangezogen. Die Rechtsprechung zu den genannten Vorschriften zeige, dass „wissenschaftlich anerkannte Methoden" lediglich die Beurteilung einer dritten, an einer Hochschule oder einer anderen Forschungsein-

---

98 Zum Teil wird aus diesen Anforderungen gefolgert, Art. 22 DSGVO sei auch auf die der letztendlichen Entscheidung vorgelagerten Prozesse beim Scoring anwendbar, insbesondere das externe Scoring unter Beteiligung von Auskunfteien. Näher dazu: Taeger, „Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018", (2017), Recht der Datenverarbeitung, Heft 1, S. 3–9, S. 6.

99 Dies hat sich aus verschiedenen Hintergrundgesprächen des SVRV ergeben und auch offizielle Quellen verweisen darauf. Siehe z. B.: https://www.schufa.de/media/editorial/unternehmenskunden/dateien_1/pibs/branchenscores/score_3_0/90Jahre_1703_PIB_Branchenscores30_Banken_Web.pdf, S. 2 (zuletzt abgerufen am 20.10.2017).

100 Siehe hierzu eine Auskunft der Schufa: https://www.schufa.de/media/editorial/unternehmenskunden/dateien_1/pibs/branchenscores/score_3_0/90Jahre_1703_PIB_Branchenscores30_Banken_Web.pdf (zuletzt abgerufen am 01.03.2018).

101 ULD Schleswig-Holstein, Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, (Gutachten im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft – BMVEL –, 2005), S. 48.

102 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 31 zu § 28b BDSG.

103 Kai von Lewinski/Dirk von Lewinski, „Evidenz-basierter Datenschutz", (2014), Datenschutz und Datensicherheit, Volume 38, Issue 3, S. 175 ff.; krit. zur faktischen Überprüfbarkeit: Weichert, „Scoring in Zeiten von Big Data", (2014), Zeitschrift für Rechtspolitik, Heft 6, S. 168–171, S. 170.

104 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 33 zu § 28b BDSG.

richtung als Wissenschaftler in der jeweiligen Fachrichtung tätigen Person erfordere. § 28b BDSG a. F. (und nun auch § 31 Abs. 1 BDSG n. F.) verlange dagegen keine „allgemein anerkannte" wissenschaftlich Methode und stelle damit auch keine qualifizierte Wissenschaftsklausel dar; dies sei Ausdruck der Entscheidung des Gesetzgebers, den Datenverarbeitern einen weiten Gestaltungsspielraum bei der Umsetzung der Scoringregelungen einzuräumen.[105] Diese Annahme wird offenbar von der Praxis gestützt, in der sich die Datenschutzbehörden die Wissenschaftlichkeit solcher Verfahren durch Vorlage von Gutachten der Verarbeiter bestätigen lassen.[106]

Im Rahmen des Gesetzgebungsverfahrens zu § 28b BDSG a. F. wurden weitergehende Kriterien für die Wissenschaftlichkeit des Verfahrens erwogen: Der Bundesrat forderte, den Wortlaut dahingehend zu ändern, dass „Verfahren verwendet werden, die insbesondere hinsichtlich ihrer Methodik dem Stand der Technik entsprechen, und alle organisatorischen und technischen Vorkehrungen getroffen werden, um unrichtige Bewertungen und fehlerhafte Dateneingaben zu vermeiden".[107] Der Bundestag sah diese Anforderungen in dem Begriff des wissenschaftlich anerkannten, mathematisch-statistischen Verfahrens bereits als gegeben an und wies darauf hin, dass demnach Verfahren, die veraltet seien, nicht mehr zulässigerweise angewandt werden könnten.[108] Daraus wird zum Teil gefolgert, die Wissenschaftlichkeit erfordere, dass die Verfahren stetig fortentwickelt werden.[109] Damit wurde allerdings offen gelassen, ob die vom Bundesrat geforderten organisatorischen und technischen Vorkehrungen zur Vermeidung von unrichtigen Bewertungen ebenfalls durch den Begriff der Wissenschaftlichkeit der Verfahren abgedeckt sind.

Laut Gesetzesbegründung zur Datenschutznovelle 2009 führt die Wissenschaftlichkeit des mathematisch-statistischen Verfahrens jedenfalls zu einer Dokumentationspflicht der verantwortlichen Stelle.[110] Anhand der Dokumentation soll die Wissenschaftlichkeit des Scoringverfahrens von den Datenschutzaufsichtsbehörden nachvollzogen werden können. Allerdings ist die Rolle der Datenschutzbehörden auf diesem Feld jedoch in mehrerer Hinsicht problematisch.

Erstens kann die Aufsichtstätigkeit ein industrieweites mathematisches Standardmodell (im Sinne einer „best practice") nicht ersetzen.[111] Auch logistische Regressionsmodelle stellen nicht zwingend einen industrieweiten Standard dar. Zu Recht wird auch kritisiert, dass den zuständigen Aufsichtsbehörden sowohl normative Kontrollansätze als auch personelle und technische Ressourcen fehlen.[112] Dies stellt nicht nur ein Problem für die Behörden, sondern auch für die Datenverarbeiter dar, die ihre Verfahren rechtssicher gestalten müssen. Der Umstand, dass Datenschutzbehörden oft externe Expertise in Anspruch nehmen, löst das Problem der Nachvollziehbarkeit nicht. Bei der Beauftragung von externen Gutachten kann es zu Interessenkonflikten kommen. Bedenklich erscheint daher die Auffassung, mit der Vorlage eines wissenschaftlichen Gutachtens durch die Auskunftei an die Datenschutzaufsichtsbehörden entfalle jeder Anlass dazu, eine fehlende Überprüfung der wissenschaftlichen Qualität zu bemängeln.[113] Es ist auch anerkannt, dass permanentes Monitoring erforderlich ist, um Scoring-Methoden ständig auf ihre Validität zu überprüfen, damit gesellschaftlichen Entwicklungen Rechnung getragen werden kann. Externe Gutachten können diese Rolle kaum erfüllen.

---

105 Wäßle/Heinemann, „Scoring im Spannungsfeld von Datenschutz und Informationsfreiheit", (2010), Computer und Recht, Heft 6, S. 410–416, S. 413 unter Verweis auf BVerwG, Urteil vom 29.06.1995 – 2 C 15.94, abgedruckt in NJW 1996, S. 801 f.

106 Von Lewinski, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 20. Edition, Stand: 01.05.2017, C. H. Beck Verlag, Rn. 31 zu § 28b BDSG.

107 BR-Drs. 548/08, S. 9.

108 BT-Drs. 16/10581, S. 3.

109 Helfrich, Multimedia-Recht, Hoeren/Sieber/Holznagel (Hrsg.), 44. EL Januar 2017, Rn. 90 zu Teil 16.4.

110 BT-Drs. 16/10529, 10.10.2008, S. 16.

111 Zur Forderung nach einem Standardmodell näher: Geslevich-Packing/Lev-Aretz, „On Social Credit and the right to be unnetworked", (2016), Columbia Business Law Review, S. 340–425, S. 352.

112 Weichert, „Scoring in Zeiten von Big Data", (2014), Zeitschrift für Rechtspolitik, Heft 6, S. 168–171, S. 170.

113 Taeger, Anmerkung zu BGH, Urteil vom 28.01.2014 – VI ZR 156/13, MultiMedia und Recht, Heft 7, S. 489–494, S. 493.

3. Verbot der Nutzung bestimmter Daten?

Neben der Richtigkeit und Aussagekraft der Daten und den Anforderungen an Scoringverfahren, ist für Scoring auch die Frage des Nutzungsverbots für bestimmte Daten relevant. Ein weiteres Problem beim Scoring und der Nutzung von personenbezogenen Daten ist die Frage, welche Daten benutzt werden dürfen. Beispielsweise war zuvor – anders als jetzt in § 31 Abs. 1 BDSG n. F. – die ausschließliche Verwendung von Anschriftendaten, das sogenannte Geo-Scoring, grundsätzlich ausgeschlossen.

Im Datenschutzrecht werden nicht alle Arten personenbezogener Daten gleich behandelt. Da bestimmte persönliche Daten als sensibler betrachtet werden als andere und damit in besonderem Maße schützenswert sind, werden besondere Voraussetzungen für ihre Nutzung aufgestellt. Die Verarbeitung besonderer Kategorien personenbezogener Daten unterliegt in Artikel 9 Abs. 1 DSGVO einem grundsätzlichen Verbot, von dem allerdings viele genannte Ausnahmen, z. B. in Bezug auf soziale Sicherheit, Gesundheitsvorsorge, oder im öffentlichen Interesse gemacht werden können. Exemplarisch befassen wir uns hier mit der Einwilligung in die Nutzung solcher sensibler Daten und der Verarbeitung öffentlich zugänglicher Daten.

3.1 Einwilligung in die Nutzung besonderer personenbezogener Daten

Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten untersagt, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Im Gegensatz zur bisherigen Regelung in § 3 Abs. 9 BDSG a. F. wurde der Umfang der als besonders schützenswert geltenden Daten mit der DSGVO deutlich erweitert. Art. 9 Abs. 1 DSGVO gilt gem. Art. 22 Abs. 3 DSGVO auch für automatisierte Entscheidungen, die unter den Ausnahmetatbestand des Art. 22 Abs. 2 DSGVO fallen.

Art. 9 Abs. 1 DSGVO verlangt für bestimmte Arten sensibler Daten auch, dass schon deren potenzielle Datenquellen einem Verarbeitungsverbot unterliegen sollen. Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit *hervorgehen*, ist damit untersagt. Angesichts der neuen Verarbeitungsmöglichkeiten im Rahmen von Big Data ergeben sich für die Datenverarbeiter allerdings erhebliche praktische Probleme bei der Einschätzung, ob aus einem bestimmten Datenbestand potenziell sensible Daten hervorgehen können.[114]

Die Regelung des Art. 9 DSGVO ist nicht unumstritten. Kritisiert wird die statische Festlegung der in Art. 9 Abs. 1 DSGVO aufgeführten Datenkategorien. Ob ein Datum im Einzelfall tatsächlich sensibel sei, hänge vielmehr vom jeweiligen Verarbeitungskontext ab und könne demnach nicht pauschal beurteilt werden.[115] Es wird auch darauf hingewiesen, die gesetzgeberische Aufteilung in sensible und im Umkehrschluss weniger sensible Daten sei systemwidrig und widerspreche dem in der Rechtsprechung zum Recht auf informationelle Selbstbestimmung verankerten Annahme, es gebe keine für sich gesehen belanglosen Daten.[116] Allerdings verkennt diese Argumentation, dass die Existenz besonderer Kategorien personenbezogener Daten nicht automatisch bedeutet, dass es sich bei den darin nicht erwähnten Daten um „belanglose“ Daten handelt. Letztere müssen nach wie vor nach den Anforderungen des Art. 6 DSGVO verarbeitet werden. Art. 9 DSGVO widerspricht auch nicht dem allgemein in der DSGVO geregelten Verbotsprinzip für die Verarbeitung personenbezogener Daten. Er stellt vielmehr, ebenfalls als Verbotsvorbehalt

114 Schneider, „Schließt Art. 9 DSGVO die Zulässigkeit der Verarbeitung bei Big Data aus? Überlegungen, wie weit die Untersagung bei besonderen Datenkategorien reicht“, (2017), Zeitschrift für Datenschutz, S. 303–308, S. 305.

115 Frenzel, Datenschutz-Grundverordnung, Paal/Pauly (Hrsg.), 1. Auflage 2017, C. H. Beck Verlag, Rn. 6.

116 Schneider, „Schließt Art. 9 DSGVO die Zulässigkeit der Verarbeitung bei Big Data aus? Überlegungen, wie weit die Untersagung bei besonderen Datenkategorien reicht“, (2017), Zeitschrift für Datenschutz, S. 303–308, S. 304; BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83.

mit bestimmten Ausnahmen, eine lex specialis zu dem allgemeinen Art. 6 DSGVO dar.[117]

Während das grundsätzlich bestehende Verarbeitungsverbot in Art. 9 Abs. 1 DSGVO aus persönlichkeitsrechtlicher Perspektive zu begrüßen ist, sind die in Art. 9 Abs. 2 DSGVO folgenden zehn Ausnahmen allerdings problematisch. So gibt es Ausnahmen in Bezug auf soziale Sicherheit oder die Gesundheitsvorsorge. Der Bundesrat hatte in seinen Empfehlungen zum Gesetzesentwurf des § 28b BDSG a. F. noch angeregt, dass die besonders sensiblen Daten des § 3 Abs. 9 BDSG a. F. (rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) nicht für Scoring genutzt werden sollten, konnte sich damit allerdings nicht durchsetzen.[118] Im BDSG n. F. ist die Verarbeitung besonderer Kategorien personenbezogener Daten in § 22 geregelt. Art. 22 DSGVO verlangt, dass angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen werden. Hier werden zwar zahlreiche in Art. 9 Abs. 2 DSGVO enthaltene Öffnungsklauseln in Anspruch genommen, jedoch nicht die aus Art. 9 Abs. 2 lit. a) DSGVO, was bedeutet, dass nach deutschem Recht in die Verwendung aller Arten besonderer Kategorien personenbezogener Daten eingewilligt werden kann (dazu IV.3). Die Zentralität der Einwilligung im Datenschutzrecht und die damit verbundenen Probleme werden an dieser Stelle besonders deutlich.

Außerdem ist in Art. 9 Abs. 2 lit. a) DSGVO die Möglichkeit geregelt, als Betroffener in die Verwendung dieser besonderen Kategorien von Daten einzuwilligen. Im Vergleich zu den entsprechenden Regelungen im BDSG a. F. wird eine *ausdrückliche* Einwilligung des Betroffenen verlangt. Welche besonderen Anforderungen an die Einwilligung zu stellen sind, ist unklar. Nahe liegt, dass dadurch die ansonsten zulässige konkludente oder stillschweigende Einwilligung ausgeschlossen ist. Zudem dürfte davon auszugehen sein, dass sich die Einwilligung explizit auf die Verarbeitung sensitiver Daten beziehen muss.[119] Dass die Einwilligung schriftlich abgegeben werden muss, lässt sich dagegen nicht automatisch aus der verlangten Ausdrücklichkeit ableiten, dürfte aber zu Beweis- und Dokumentationszwecken, gerade in diesem sensiblen Bereich für die Datenverarbeiter geboten sein.[120]

Trotz der offenbar vergleichsweise höheren Anforderungen an die Einwilligung in Art. 9 Abs. 2 lit. a) DSGVO dürften sich auch hier die grundsätzlich bestehenden Probleme mit der Freiwilligkeit der Einwilligung in die Datenverarbeitung fortsetzen (s. III.2).[121]

3.2 Verarbeitung öffentlich zugänglicher sensibler Daten

Als weitere Ausnahme erlaubt Art. 9 Abs. 2 lit. e) DSGVO die Verarbeitung besonders sensibler Daten, die die betroffene Person offensichtlich öffentlich zugänglich gemacht hat. Öffentlich gemacht sind die Daten dann, wenn sie dem Zugriff einer unbestimmten Anzahl von Personen ohne wesentliche Zulassungsschranke offenstehen.[122] Zu denken ist hier insbesondere an eine Veröffentlichung im Internet und in den Printmedien oder TV.

Der Grund für diese Ausnahme vom grundsätzlichen Verbot des Art. 9 Abs. 1 DSGVO ist die angenommene Dispositionsbefugnis der Betroffenen. Gem. Art. 1 Abs. 2 DSGVO haben die Betroffenen u. a. das Recht auf Schutz ihrer personenbezogenen Daten. Wenn also nur das Recht des Einzelnen auf *Schutz* der Daten und nicht die personenbezogenen *Daten selbst* geschützt werden, besteht konsequenterweise für den Einzelnen auch das Recht, auf diesen Schutz zu verzichten. Der Grund für die Regelung, dass öffentlich zugänglich gemachte Daten keinen besonderen Schutz i. S. d. Art. 9 Abs. 1 DSGVO bedürfen,

117 Siehe dazu z. B. Erwägungsgrund 51, der darauf hinweist, dass neben den Anforderungen des Art. 9 die allgemeinen Bestimmungen der Datenverarbeitungen gelten.

118 BR-Drs. 548/1/08, 0909.2008, S. 13.

119 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.),2017, C. H. Beck Verlag, Rn. 14 zu Art. 9 DSGVO.

120 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.),2017, C. H. Beck Verlag, Rn. 15 zu Art. 9 DSGVO.

121 Dazu Domurath/Kosyra, „Verbraucherschutz im Internet der Dinge", (2016), SVRV Working Paper Nr. 3.

122 Schulz, Datenschutz-Grundverordnung, Gola (Hrsg.), 2017, C. H. Beck Verlag, Rn. 24 zu Art. 9 DSGVO.

besteht also in der Annahme, der Betroffene habe durch die Veröffentlichung bewusst auf sein Recht auf Schutz der sensiblen Daten verzichtet.

Die Annahme dieser Dispositionsbefugnis ist in der Praxis jedoch problematisch. Veröffentlicht beispielsweise die Verfasserin eines frei zugänglichen Blogs ihre politische Meinung, nimmt sie damit ihr Recht auf freie Meinungsäußerung wahr. Dass sie sich über nur aufgrund von Big-Data-Analysen eintretende Konsequenzen ihrer Veröffentlichung, etwa die Verwendung dieser Daten bei der Entscheidung über den Abschluss ihres nächsten Mobilfunkvertrages Gedanken macht, liegt fern. Die Relativierung der Schutzbedürftigkeit in dieser Situation versetzt die Betroffenen in die Situation, entweder das Recht auf freie Meinungsäußerung in Anspruch zu nehmen oder den Schutz ihrer Daten in Hinblick auf politische Meinungen zu bewahren.

Dieses Dilemma kann nicht mit Hinweis auf die Parallele aufgelöst werden, dass Kriterien wie die politische Einstellung oder Gewerkschaftszugehörigkeit eines potenziellen Vertragspartners auch in rein menschlichen Entscheidungsprozessen abseits von Algorithmen und automatischer Datenverarbeitung eine implizite Rolle bei Vertragsabschlüssen spielen können. Im Gegensatz zu rein menschlichen Entscheidungsfindungsprozessen handelt es sich bei Scoring um eine Systematisierung von derartigen Entscheidungen. Diese birgt die Gefahr, dass etwaige ungerechtfertigte Ungleichbehandlungen verfestigt werden, indem die auf Algorithmen basierenden Entscheidungsmuster wiederholt werden. Bei den in Art. 9 Abs. 2 DSGVO aufgeführten Ausnahmen handelt es sich um Erlaubnistatbestände, solche sensiblen Daten für eine Vielzahl von Verarbeitungswecken, auch für Scoring, zu verwenden. Der in § 31 Abs. 1 BDSG n. F. angelegten Grundsatzentscheidung, automatisierte Entscheidungssysteme zu erlauben, stehen damit keine ausreichenden Schutzvorschriften hinsichtlich der Verwendung sensibler Daten gegenüber.

3.3 Diskriminierungsverbot

Schließlich stellt sich die Frage, ob bestimmte Daten nicht für die Errechnung eines Scores benutzt werden dürfen, weil ihre Benutzung diskriminierende Entscheidungen ermöglicht. Die Praxisrelevanz dieses Themas wird am Fall der Münchener Anwältin Caroline C. deutlich, die gegen eine Auskunft über ihre Kreditwürdigkeit vorging. Sie behauptete, dass ihr Ehemann trotz vergleichbarer Einkünfte und Vermögensverhältnisse einen besseren Score erhalten hat und verklagte die Schufa auf Unterlassung, Schadensersatz und Auskunft. Sie argumentierte, dass der ausgewiesene Score nicht mit ihrer tatsächlichen Bonität übereinstimme und die Schufa bei der Einschätzung der Kreditwürdigkeit von Verbrauchern Frauen benachteilige. Die Klage blieb erfolglos.

Das OLG München führte zur Begründung aus, dass der Scorewert von der Meinungsäußerungsfreiheit der Auskunftei gedeckt sei. In dem Umstand, dass Männer und Frauen hinsichtlich ihrer Bonität unterschiedlich bewertet werden, liege auch keine Diskriminierung, da nur tatsächlich statistisch-mathematisch belegte Unterschiede berücksichtigt würden.[123] Der BGH hatte in seinem Grundsatzurteil zur Schufa bereits entschieden, dass das genaue Zustandekommen des Scorewertes dem Geschäftsgeheimnis der Auskunfteien unterliegt.[124] Die Überprüfung einer möglichen Diskrimierung fand daher nicht statt.

Die Frage, inwiefern möglicherweise diskriminierende Effekte bei automatisierter Entscheidungsfindung ausgeschlossen oder verhindert werden können, bleibt trotz dieser für Verbraucher enttäuschenden Urteile bestehen. Beispielsweise schließt das Diskriminierungsverbot des § 1 AGG die Benachteiligung aus Gründen der Rasse oder wegen der ethnischen Herkunft, wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität aus. Das AGG regelt allerdings nicht die Verarbeitung sensibler Datenkategorien, sondern die etwaige ungerechtfertigte benachteiligende Behandlung von Personen, und setzt damit erst bei der Anwendung eines Scores auf eine Person an, nicht aber bei der vorhergehenden Datenverarbeitung, die z. B. zur Entwicklung einer Scorecard führt.

123 OLG München, Urteil vom 12.03.2014 – 15 U 2395/13.

124 BGH, Urteil vom 28.01.2014 – VI ZR 156/13. Die Klägerin hat eine Verfassungsbeschwerde eingereicht (Az: 1 BvR 756/2014), über die bislang nicht entschieden wurde.

Zudem ist der Anwendungsbereich des AGG eng gesteckt. Vom Gesetz erfasst sind gem. § 2 AGG insbesondere das Arbeits- und Mietrecht, gem. § 19 Abs. 1 außerdem Massengeschäfte und damit vergleichbare Schuldverhältnisse, bei denen das Ansehen der Person nach Art des Schuldverhältnisses nachrangige Bedeutung hat, sowie privatrechtliche Versicherungen. Zu denken ist bei Massengeschäften, insbesondere an Scoring im Online- und Versandhandel, das darüber entscheidet, ob dem Kunden die Möglichkeit des Kaufs auf Rechnung angeboten wird, oder nicht. Im Fall des externen Scorings, bei dem Unternehmen für die Berechnung von Scores auf andere Unternehmen zurückgreifen, fehlt es allerdings an einem Vertragsverhältnis i. S. d. § 19 Abs. 1 AGG zwischen dem Betroffenen und dem Unternehmen, das den Score berechnet (meist eine Auskunftei).[125]

Anders stellt sich dies zumindest beim internen Scoring dar, das direkt von dem Unternehmen durchgeführt wird, welches über den Vertragsschluss entscheidet. Hier eröffnet ein zumindest vorvertragliches Schuldverhältnis zwischen dem scorenden Unternehmen und dem gescorten, potenziellen Vertragspartner den Anwendungsbereich des § 19 Abs. 1 AGG.[126] Vor dem Hintergrund dieser Unterschiede in der Anwendung des AGG auf Scoring wird die Erweiterung des Anwendungsbereichs des AGG auf Ungleichbehandlungen gefordert, die auf einer algorithmenbasierten Datenauswertung oder auf einem automatisierten Entscheidungsverfahren beruhen.[127]

Fraglich ist, ob selbst die Verwendung eines Scores zur Entscheidungsfindung als eine Benachteiligung i. S. d. § 19 Abs. 1 AGG angesehen werden kann. Dies wird verneint, da es sich bei der Scorebildung um eine Gesamtschau der die Person betreffenden Faktoren handelt, so dass letztendlich nicht davon gesprochen werden könne, eine Person werde spezifisch z. B. aufgrund ihres Alters oder ihres Geschlechts diskriminiert.[128] Darüber hinaus habe ein Unternehmen, das auf einen extern errechneten Score zurückgreift, gar nicht die Möglichkeit nachzuvollziehen, welche Merkmale in die Berechnung eingegangen seien. Deshalb handele es sich hier auch nicht um eine bewusste Entscheidung des Unternehmens in Hinblick auf eine z. B. alters- oder geschlechtsbedingte Benachteiligung.[129]

Die schwierige und im Grunde nach den Umständen des jeweiligen Einzelfalls zu beantwortende Frage nach einer tatsächlichen Ungleichbehandlung i. S. d. § 19 Abs. 1 AGG kann allerdings dahinstehen, wenn ein Grund besteht, der eine Ungleichbehandlung sachlich rechtfertigen kann. Beispielsweise wird darauf verwiesen, die Verfolgung ökonomischer Interessen sei als sachlicher Grund i. S. d. § 20 Abs. 1 AGG für eine Ungleichbehandlung anerkannt, insbesondere im Fall der Vorleistungsbereitschaft von Unternehmen im Onlinehandel. Einschränkend sei aber nur dann eine sachliche Rechtfertigung gegeben, wenn Merkmale wie etwa das Alter oder das Geschlecht tatsächlich Auswirkungen auf die Zahlungswahrscheinlichkeit der Person hätten, also erheblich i. S. d. § 31 Abs. 1 BDSG n. F. seien. Andernfalls sei die Ungleichbehandlung als willkürlich und damit als Verstoß gegen § 19 Abs. 1 AGG zu sehen.[130]

§ 3 Abs. 2 AGG verbietet auch eine ungerechtfertigte mittelbare Benachteiligung. Angenommen, die Verwendung von Anschriftendaten würde für Scoring gänzlich ausgeschlossen, könnte sich die Anschrift einer Person insbesondere durch die Möglichkeiten von Big-Data-Analysen, aber wohl aus der Zusammenschau anderer Daten, wie etwa Bewegungsmustern oder Kreditkartendaten, die Aufschluss darüber geben, an welchen Orten eine Personen sich vorwiegend aufhält, folgern lassen. Gleiches gilt für Alter, Herkunft und ähnliche sensible Daten. Eine mittelbare Benachteiligung liegt nach § 3 Abs. 2 AGG vor, wenn dem Anschein nach neutrale Vorschriften, Kriterien oder Verfahren Personen wegen eines in § 1 AGG genannten Grundes gegenüber anderen Personen in besonderer Weise benachteiligen können. Würden

125 OLG München, Urteil vom 12.03.2014 – 15 U 2395/13.

126 Wendtland, BeckOK BGB, Bamberger/Roth (Hrsg.), 01.02.2017, C. H. Beck Verlag, Rn. 2 zu § 19 AGG.

127 Martini, „Algorithmen als Herausforderung für die Rechtsordnung“, (2017), Juristenzeitung, Heft 21, S. 1017–1025, S. 1021.

128 Moos/Rothkegel, „Nutzung von Scoring-Diensten im Online-Versandhandel“, (2016), Zeitschrift für Datenschutz, Heft 12, S. 561–568, S. 564.

129 Moos/Rothkegel, „Nutzung von Scoring-Diensten im Online-Versandhandel“, (2016), Zeitschrift für Datenschutz, Heft 12, S. 561–568, S. 564.

130 Moos/Rothkegel, „Nutzung von Scoring-Diensten im Online-Versandhandel“, (2016), Zeitschrift für Datenschutz, Heft 12, S. 561–568, S. 564.

z. B. Personen bestimmter Herkunft über die Anknüpfung an den Kauf bestimmter Produkte oder an den Besuch bestimmter Internetseiten die Möglichkeit des Kaufs auf Rechnung im Online-Handel verwehrt, handelt es sich dabei um eine grundsätzlich verbotene mittelbare Benachteiligung. Bei der Entscheidung über eine mögliche Rechtfertigung stellen sich die gleichen Fragen wie bei einer unmittelbaren Benachteiligung. Sofern das Unternehmen im Rahmen von § 31 Abs. 1 BDSG n. F. nachweisen kann, dass das Alter oder die Herkunft erhebliche Merkmale zur Feststellung der Kreditwürdigkeit sind und darüber hinaus ein eigenes wirtschaftliches Interesse an der Ungleichbehandlung darlegen kann, greift das Verbot aus § 19 AGG nicht ein.

Zusammenfassend bietet das AGG zwar Möglichkeiten, eine willkürliche Ungleichbehandlung einzelner Personen im Wirtschaftsverkehr zu verhindern. In Hinblick auf Scoring ist dabei allerdings problematisch, dass die notwendigen Informationen dazu, welche Merkmale wie in die Scoreberechnung eingehen, dem Geschäftsgeheimnis der Unternehmen unterliegen. Die Feststellung, ein diskriminierungsfreier Score müsse die Voraussetzungen des § 31 Abs. 1 BDSG n. F. erfüllen, ist zwar richtig, führt allerdings in einem Zirkelschluss wieder zu dem ungelösten Problem nach der Frage der Erheblichkeit der verwendeten Daten. Außerdem können unternehmerische Interessen an der Nutzung bestimmter Daten eine Diskriminierung sachlich rechtfertigen.

4. Transparenz der Scoreformel und Grenzen

Im Rahmen der Diskussion um die Überprüfbarkeit der Wissenschaftlichkeit der Scoringverfahren und der Art der verwendeten Daten wird außerdem vermehrt gefordert, die Parameter der Algorithmen, die den Berechnungen der Scorecards und Scores zugrunde liegen, transparent zu machen.[131] Dahinter steht die Überlegung, dass Transparenz im Wirtschaftsverkehr unabdingbar ist, um z. B. als Verbraucher informierte Entscheidungen treffen zu können. Deshalb hat der Betroffene beispielsweise einen datenschutzrechtlichen Auskunftsanspruch aus Art. 15 DSGVO. Auf der Basis des Auskunftsanspruchs können weitere Rechte geltend gemacht werden, wie z. B. Ansprüche auf Berichtigung oder Löschung von Daten.

Allerdings ist die bisherige Rechtsprechung unmissverständlich in der Formulierung der Grenzen des Auskunftsanspruchs des Betroffenen gem. § 34 Abs. 1 BDSG a. F. in Bezug auf das Geschäftsgeheimnis und die Meinungsfreiheit der verarbeitenden Stelle. Das OLG München hat in dem bereits erwähnten Fall der Münchener Anwältin Caroline C. entschieden, dass der Scorewert von der Meinungsäußerungsfreiheit der Auskunftei gedeckt sei.[132] In seinem Grundsatz-Urteil zum Schufa Scoring hat der BGH 2014 zudem festgestellt, dass der Auskunftsanspruch nach § 34 Abs. 1 BDSG a. F. dem Betroffenen keine Auskunft über die Scoreformel selbst gewährt.[133] Dem Auskunftsanspruch des § 34 Abs. 4 BDSG a. F. liege die gesetzgeberische Intention zugrunde, trotz der Schaffung einer größeren Transparenz bei Scoringverfahren Geschäftsgeheimnisse der Auskunfteien, namentlich die Scoreformel, zu schützen. Auch die Gewichtung der in den Score einfließenden Elemente sei genauso wenig Gegenstand des Auskunftsanspruchs des Betroffenen wie Informationen über die Vergleichsgruppen, in die er zur Berechnung der Scores eingeordnet wurde. Der BGH begründete dies insbesondere damit, dass eine vom Bundesrat im Gesetzgebungsverfahren verlangte Än-

131 Siehe z. B. Gutachten des Sachverständigenrats für Verbraucherfragen, „Verbraucherrecht 2.0“, (2016), S. 67, das eine stichprobenartige Offenlegung von Algorithmen gegenüber einem Kreis von Experten einer Digitalagentur fordert; SVRV, Digitale Souveränität, 2017, S. 21 f.

132 OLG München, Urteil vom 12.03.2014 – 15 U 2395/13.

133 BGH, Urteil vom 28.01.2014 – VI ZR 156/13. Kritisch zum Schufa-Urteil: Engels, „Kein Anspruch auf Auskunft über Scoreformel“, (2014), Der IT-Rechts-Berater, Heft 5, S. 100 f.; Gärtner, „Scoring und Datenschutz“, (2014), Zeitschrift für Bank- und Kapitalmarktrecht, Heft 5, S. 198.

derung, eine Auskunftspflicht über die Reihenfolge der Gewichtung der Daten des Betroffenen im Rahmen der Berechnung vorzusehen, nicht umgesetzt wurde. Dem Betroffenen müsse durch das Auskunftsrecht vielmehr die Möglichkeit gegeben werden, den in die Bewertung eingeflossenen Lebenssachverhalt zu erkennen und darauf reagieren zu können. Dazu seien die detaillierten Informationen über die Scoreformel und die Gewichtung der Merkmale nicht erforderlich.

Problematisch an dieser Auslegung ist, dass es dem Betroffenen unmöglich gemacht wird, die Sachgerechtigkeit und Diskriminierungsfreiheit seines Scores zu überprüfen.[134] Den unternehmerischen Interessen an der Geheimhaltung der Scoreformel wird der Vorzug gegenüber den Interessen des Betroffenen an seinem Persönlichkeitsschutz gegeben. Darüber hinaus impliziert die Begründung des OLG München im Fall der Münchener Anwältin, dass Fakten als mathematisch-belegbare Unterschiede nicht diskriminierend wirkend können.[135] Dies wird dem Zweck des Datenschutzes, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (Art. 1 Abs. 2 DSGVO), nicht gerecht.[136]

Es ist schwer vorherzusehen, ob Art. 15 DSGVO an dieser Rechtslage etwas ändern wird. In Art. 15 Abs. 1 lit. h) DSGVO ist festgelegt, dass die betroffene Person Auskunft über das Bestehen einer ausschließlich automatisierten Entscheidungsfindung gem. Art. 22 DSGVO und aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für sich erhalten können soll. Gleichzeitig besteht damit keine differenzierte Auskunftspflicht seitens des Verantwortlichen in Fällen, die nicht unter Art. 22 DSGVO fallen.[137] Ob mit der genannten involvierten Logik der automatisierten Verarbeitung auch die Gewichtung der Merkmale oder gar die Scoreformel gemeint ist, ist unklar und wird unterschiedlich beurteilt.[138] Insgesamt bleibt also abzuwarten, ob sich an der Rechtsprechung zum Auskunftsrecht des Betroffenen und damit auch an der Transparenz dem Verbraucher gegenüber mit der DSGVO etwas ändern wird.

5. Zwischenergebnis

Die Rechtsprobleme der bei Scoring verwendeten Datenbasis sind mannigfaltig. Auch hier ergeben sich Schutzlücken, die aus im Wegfall schützender Regelungen in der DSGVO und aus der Annahme des Überwiegens wirtschaftlicher Interessen von Unternehmen herrühren.

Zwar muss nach dem Datenschutzrecht die Datenbasis grundsätzlich richtig sein. Wie und durch wen diese Richtigkeit sicherzustellen ist, ist allerdings unklar. Die im BDSG a. F. bislang explizit geregelten Berichtigungspflichten hinsichtlich falscher Daten sind nunmehr weggefallen und es bleibt abzuwarten, ob dies durch den sehr allgemeinen Grundsatz der Richtigkeit der Daten in der DSGVO aufgefangen werden kann. Außerdem ist die Nichtberücksichtigung möglicherweise erheblicher Daten und die Verwendung von Schätzdaten beim Scoring zulässig, obschon diese die tatsächliche Aussagekraft der eingesetzten Daten in Frage stellen. Die nach dem BDSG a. F. bestehende Pflicht, die Verwendung von Schätzdaten anzuzeigen, fehlt in der DSGVO und wird auch vom BDSG n. F. nicht wieder aufgegriffen. Zwar gibt es Ansichten, die aus den allgemeinen Regelungen und Erwägungsgründen die Pflicht zur Kennzeichnung von Schätzdaten ableiten, ein vergleichbarer Schutzstandard wie bisher ist damit jedoch nicht gewährleistet. Bedenklich ist außerdem, dass auch die Regelung, welche die Verwendung von Informationen über Konditionenabfragen bei der Beurteilung der Bonität des Betroffenen untersagt, weggefallen ist. Aus Verbrauchersicht ist es erforderlich, die

134 Martini, „Big Data als Herausforderung für den Persönlichkeitsschutz“, (2014), Deutsches Verwaltungsblatt, Heft 23, S. 1481–1489, S. 1485.

135 OLG München, Urteil vom 12.03.2014 – 15 U 2395/13.

136 Martini, „Big Data als Herausforderung für den Persönlichkeitsschutz“, (2014), Deutsches Verwaltungsblatt, Heft 23, S. 1481–1489, S. 1485.

137 Schmidt-Wudy, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 23. Edition, Stand 01.02.2018, S. H. Beck Verlag, Rn. 77 zu Art. 15 DSGVO.

138 Zustimmend: Schmidt-Wudy, BeckOK Datenschutzrecht, Wolff/Brink (Hrsg.), 23. Edition, Stand 01.02.2018, Rn. 78.3 zu Art. 15 DSGVO; Ablehnend: Ehmann, Datenschutz-Grundverordnung, Ehmann/Selmayr (Hrsg.), 2017, C. H. Beck Verlag, Rn. 16 zu Art. 15 DSGVO; Paal, DS-GVO BDSG, Paal/Pauly (Hrsg.), 2. Auflage 2018, C. H. Beck Verlag, Rn. 31 zu Art. 15 DSGVO.

Konditionen verschiedener Kreditanbieter miteinander zu vergleichen zu können. Daraus sollte Verbrauchern kein Nachteil erwachsen.

Darüber hinaus bleibt auch unter der neuen Rechtsordnung ungeklärt, wie die Erheblichkeit der zur Scoreberechnung zugrunde gelegten Daten festzustellen ist. Unbefriedigend ist die aktuell bestehende Praxis, nach der die Erheblichkeit der Daten allein durch die Unternehmen selbst eingeschätzt und durch Aufsichtsbehörden kaum verlässlich überprüft werden kann. Es stellt sich die Frage, ob nicht über die rein statistische Erheblichkeit der Daten weitere Qualitätskriterien, wie z. B. eine bestimmte Vertragsrelevanz eine Rolle bei der Beurteilung der Erheblichkeit spielen sollten.

Auch die Anforderungen an das mathematisch-statistische Verfahren, auf dem die Erheblichkeit der Daten beruhen muss, bleiben unklar. Insgesamt ist die Auslegung, die wissenschaftliche Anerkennung des Verfahrens sei bereits durch die Bestätigung einer in der Wissenschaft tätigen Person gegeben, aus Verbrauchersicht unbefriedigend. Diese Auffassung vermeidet die Auseinandersetzung mit der grundsätzlichen Frage, welche technischen oder mathematisch-statistischen Anforderungen an Scoringverfahren gestellt werden können und sollten. Der Einsatz externer Gutachter kann nur ein Behelfslösung sein, die das Problem der fehlenden Ressourcen der zuständigen Aufsichtsbehörden nicht lösen lann. Unter welchen Voraussetzungen ein externer Gutachter das Verfahren anerkennen oder gerade nicht anerkennen kann, wird mit § 31 Abs. 1 BDSG n. F. nicht festgelegt. Zur Lösung des Problems sollten die Anregungen, die der Bundesrat schon bei Entwurf des § 28b BDSG a. F. zur Konkretisierung des wissenschaftlich anerkannten, mathematisch-statistischen Verfahrens einbrachte, zur Ausgestaltung des § 31 Abs. 1 BDSG n. F. herangezogen werden. Die Lösung dieser Probleme ist umso wichtiger und schwieriger, als dass Scoring-Systeme zunehmend „selbstlernend“ sind und Erfahrungen aus aktuellen (evtl. gescorten) Verträgen in die anonymisierten Erfahrungswerte einfließen lassen.[139]

Auch die Regelung der Verarbeitung besonderer Kategorien personenbezogener Daten nach der neuen Rechtslage ist aus normativer Sicht unbefriedigend. Das grundsätzlich zu begrüßende Verbot aus Art. 9 DSGVO wird durch die weitreichenden Ausnahmetatbestände relativiert und quasi ausgehebelt. Ein angemessener Schutz sensibler Daten für die Betroffenen ist dadurch nicht gegeben. Das AGG hat aufgrund seines begrenzten Anwendungsbereichs auf das Diskriminierungspotenzial der verwendeten Datenbasis bei Scoring keine zufriedenstellenden Antworten. Dies und auch die eingeschränkte Transparenz beim Auskunftsrecht des Betroffenen hinsichtlich des Zustandekommens seines Scores trägt dazu bei, dass das Datenschutzrecht im Fall von Scoring einem seiner eigentlichen Zwecke, dem Persönlichkeitsschutz, nur unzureichend gerecht wird.

139 ULD Schleswig-Holstein, Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, (Gutachten im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft – BMVEL –, 2005), S. 49.

V Offene Fragen

Die Auseinandersetzung mit den europäischen und deutschen auf Scoring anwendbaren Datenschutzregeln hat gezeigt, dass es Schutzlücken im Datenschutz und weiteren Regelungsbedarf im Bereich Scoring gibt. Es muss gefragt werden, ob das Datenschutzrecht den Regelungsbedarf, den Scoring mit sich bringt, überhaupt abdecken kann. Ein weiteres Problem ist der angenommene Charakter von Daten als Wirtschaftsgut.

1. Grenzen des Datenschutzrechts

Die Grenzen des Datenschutzrechts in Bezug auf Scoring liegen darin, dass diskriminierungsrechtliche Fragen oft nicht erfasst werden. Darüber hinaus dient das Datenschutzrecht auch nicht primär dazu, verbraucherschützende Interessen durchzusetzen, obschon Scoring genau diese mit seinen Anwendungsfeldern im Kreditbereich, Online-Handel oder bei Versicherungen stark betrifft.

Vergleichbare Defizite weist das Datenschutzrecht hinsichtlich der Gewährleistung mathematisch-statistischer Standards auf. Es ist nicht klar, ob Vorgaben für die mathematisch-statistische Ausgestaltung von Entscheidungssystemen überhaupt dem Regelungsbereich des Datenschutzrechts unterfallen können oder sollen und ob dies überhaupt dem Schutzgut der DSGVO unterfällt. [140] Zudem kann das Datenschutzrecht auch weitere Fragen, wie z. B. die Haftung für aus Fehlentscheidungen entstehende Schäden nicht regeln.

Schließlich hat das Datenschutzrecht keine Wirkung in Bereichen, in denen es um die Verarbeitung nicht personenbezogener Daten geht, wie z. B. die Datenanalysen, die der Entwicklung einer Scorecard dienen. Dass an diesem Punkt aber Grundsatzentscheidungen getroffen werden, die automatisierten Entscheidungssystemen zugrunde liegen, sollte der Gesetzgeber nicht aus den Augen verlieren. Angesichts der wachsenden Bedeutung automatisierter Entscheidungssysteme und damit auch von Scoring sollte für eine zufriedenstellende, d. h. umfassende Regelung von Scoring auch über das Datenschutzrecht hinausgedacht werden.

Eine Orientierung könnte dabei die aktuelle Debatte um die legislative Erfassung von Algorithmen bieten.[141] Auch Scoring beruht heute auf komplexen Computerprogrammen und birgt daher Risiken der Manipulation von Verhalten und Gefahren für den Schutz der Privatheit.[142] Hier den richtigen Ausgleich zwischen Transparenz und Privatsphärenschutz auf der einen und Unternehmensschutz auf der anderen Seite zu finden, stellt eine Herausforderung für die Regulierung von Computerprogrammen zugrundeliegenden Algorithmen dar.

2. Daten als Wirtschaftsgut

Die bisherige Darstellung der Regelungen des Datenschutzrechts der Durchsetzung macht deutlich, dass den unternehmerischen Interessen große Wichtigkeit eingeräumt wird. Nicht umsonst lautet die Überschrift des Scoring-Paragraphen im BDSG n. F. „Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften“. Die Rechtsprechung bestätigt dies: Meinungsfreiheit und Geschäftsgeheimnisse von Unternehmen dienen als Grenzen für Auskunftsansprüche von Betroffenen über die von ihnen verarbeiteten Daten und deren Gewichtung.

---

140 Siehe zum Schutzgut der DSGVO: Veil, „Die Datenschutz-Grundverordnung: des Kaisers neue Kleider“, (2018), Neue Zeitschrift für Verwaltungsrecht, Heft 10, S. 686–696, S. 690 ff.

141 Siehe dazu insbesondere Martini, „Algorithmen als Herausforderung für die Rechtsordnung“, (2017), Juristenzeitung, Heft 21, S. 1017–1025; Der SVRV hat in seinem Gutachten „Verbraucherrecht 2.0“ bereits die Einführung eines Algorithmengesetzes gefordert: SVRV, Verbraucherrecht 2.0 – Lösungsoptionen, (2016), S. 18.

142 Siehe Hoffmann-Riem, „Verhaltenssteuerung durch Algorithmen“, (2017), Archiv des öffentlichen Rechts, Band 142, S.1–42, S.5. Hoffmann-Riem weist zudem darauf hin, dass die unternehmerische Softwareentwicklung bei Algorithmen trotz ihres enormen verhaltenssteuernden Potenzials keiner rechtsstaatlich-demokratischen Kontrolle unterliegt, S. 32.

Dies ist vor dem Hintergrund zu verstehen, dass das Datenschutzrecht auch dazu dient, eine Wirtschaftsordnung für Daten aufzubauen.[143] Die Grenzen zwischen Verbraucher- und Datenschutzrecht verschwimmen zunehmend. Verbraucherschutzrecht und Datenschutzrecht weisen zwar durchaus Parallelen auf, z. B. in Fragen der Informiertheit und der Transparenz,[144] jedoch ergeben sich aus der Verschmelzung der beiden Bereiche Probleme, die nicht vernachlässigt werden sollten.

Problematisch ist insbesondere, dass regulativ-normativ davon ausgegangen wird, dass sich – wie im Verbraucherrecht bereits kritisiert – auch im Datenschutzrecht zwei gleichberechtigte Parteien gegenüberstehen.[145] Die zentrale Rolle der Einwilligung im Datenschutzrecht basiert auf der Annahme, dass Betroffene rational und selbstbestimmt handeln. Die Einwilligung in Datenerhebungen und -verarbeitungen dient dabei der informationellen Selbstbestimmung des Betroffenen. Zwar ist der selbstbestimmte und informierte Umgang mit personenbezogenen Daten die Basis für eine individuelle Entwicklung und Entfaltung des Betroffenen und den Schutz des Persönlichkeitsrechts maßgeblich und Schutzmechanismen, die Information, Transparenz und Selbstbestimmung fördern, sind daher grundlegend. Dies bedeutet jedoch nicht, dass es ausreicht, wenn sich das Regelwerk in der Förderung von Information und Transparenz erschöpft. Selbst wenn vollständige Transparenz und Informiertheit erreicht ist, führt dies nicht automatisch dazu, dass Betroffene tatsächlich auch selbstbestimmt mit Daten umgehen können. Die Probleme der Parameter von Information und Transparenz, wie sie im Verbraucherrecht zutage kommen, setzen sich hier nur fort.

Ein weiteres Problem in der Orientierung an einem „Datenwirtschaftssystem“ liegt darin, dass Daten als Wirtschaftsgut angesehen werden. Viele Onlineservices werden heutzutage nicht im Austausch für Geld, sondern für personenbezogene Daten angeboten.[146] Unternehmen handeln mit Datenaggregaten, insbesondere in der Werbebranche.[147] Vor diesem Hintergrund wird angenommen, dass Betroffene bzw. Verbraucher über Daten wie über eine Währung verfügen können sollen. Der Umstand, dass für viele Unternehmen Daten bereits ein Wirtschaftsgut darstellen, bedeutet allerdings nicht, dass dies auch für Verbraucher der Fall ist oder – normativ – sein sollte. Ein Unterschied zwischen Unternehmens- und Verbraucherinteressen besteht hier schon darin, dass sich für Unternehmen der Wert von Daten erst im Aggregat ergibt, also in der Gesamtheit möglichst umfassender Daten über möglichst viele Individuen, während das Interesse von Betroffenen bzw. Verbrauchern regelmäßig nur ihre eigenen, individuellen Daten und ihre eigene Privatsphäre betrifft. Daraus folgen nicht nur unterschiedliche Wertigkeiten in Bezug auf individuelle Daten, sondern auch unterschiedliche Interessen im Wirtschaftsverkehr. Das Interesse von Unternehmen an einer möglichst umfassenden Erhebung und Auswertung von möglichst vielen Daten im Aggregat kann nicht mit den Interessen der Betroffenen gleichgesetzt werden und sollte den Regelungsgehalt eines Datenschutzgesetzes nicht zwangsläufig beeinflussen. Daten sind in einer hochdigitalisierten Welt weiterhin schützenswert und sollten nicht in einer auf wirtschaftlichen Verbraucherschutz abhebenden Perspektive verloren gehen.[148]

---

143 SVRV, Verbraucherrecht 2.0, 2016, S. 12.

144 Helberger/Borgesius/Reyna, „The Perfect Match? A closer look at the relationship between EU consumer law and data protection law”, (2017), Common Market Law Review, Volume 54, Issue 5, S. 2.

145 Dix, “Daten als Bezahlung – Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht”, (2017), Zeitschrift für Europäisches Privatrecht, Heft 1, S. 1–5, S. 4.

146 Helberger/Borgesius/Reyna, „The Perfect Match? A closer look at the relationship between EU consumer law and data protection law”, (2017), Common Market Law Review, Volume 54, Issue 5, S. 2.

147 Vgl. Goldhammer/Wiegand, Ökonomischer Wert von Verbraucherdaten für Adress- und Datenhändler, (Studie im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz, 2017), S. 13 ff.

148 Vgl. auch Roßnagel, “Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht”, (2013), Zeitschrift für Datenschutz, Heft 11, S.562–567, S. 563.

VI Schlussbetrachtungen

Mit diesem Papier sollten die datenschutzrechtlichen Regelungen, die auf Scoring anwendbar sind, möglichst umfassend abgebildet und diskutiert werden. Im Ergebnis sind die Anforderungen, die die DSGVO und das BDSG n. F. an die Rechtmäßigkeit von Datenverarbeitungen im Rahmen von Scoring stellen, gering. So muss beispielsweise die Anwendung der datenschutzrechtlichen Grundsätze der Zweckbindung und der Datenminimierung überdacht werden, um die Diskrepanz zwischen ihrem Wortlaut in DSGVO und BDSG n. F. und ihrer Anwendung in der Praxis zu überwinden. Momentan unterliegen sie einem großen Spielraum für die verantwortliche Stelle bzw. stoßen im Zeitalter von Big Data an ihre Grenzen. Scoringspezifische Probleme ergeben sich auch hinsichtlich der Aussagekraft der Daten und dem etwaigen Verbot, bestimmte Daten überhaupt zu verwenden.

Besonders grundlegend muss die Zentralität der Einwilligung im Datenschutzrecht überdacht werden. Im Moment stellt die Einholung von Einwilligungen in Datenerhebungs- und Verarbeitungsprozesse eher eine Art „Haftungsbefreiung“ für Unternehmen dar: ihr liegt die Annahme zugrunde, dass solange Betroffene bewusst und freiwillig bestimmte Beziehungen zu Unternehmen eingehen, kein weiterer Schutz nötig ist. Im Zeitalter von Big Data, in welchem kaum mehr überschaubar ist, wofür Daten überhaupt genau erhoben werden und von wem, muss daher diskutiert werden, ob die (angenommene) freiwillige Einwilligung als Erlaubnistatbestand für Datenverarbeitung nicht funktional überlastet wird. Es stellt sich die Frage, wieviel einzelnen Verbrauchern bei der Bewältigung der Aufgabe des Schutzes ihrer personenbezogenen Daten tatsächlich zugemutet werden kann. Bisweilen liefert die Einwilligung ihnen ein Instrument, mit dem sie nur theoretisch selbstbestimmt den Schutz ihrer Daten gestalten können. Praktisch scheitern viele an dieser Aufgabe regelmäßig. Hier muss genauer geprüft werden, welche Grundsatzentscheidungen hinsichtlich des Scoring konsensfähig sind und damit in die Regulierung einfließen können. Zu denken wäre hier beispielsweise an den bereits 2009 vom Bundesrat angeregten Ausschluss der Verwendung von Geo- oder Schätzdaten beim Scoring und die Begrenzung von Scoring auf solche Verträge, die tatsächlich mit einem kreditorischen Ausfallrisiko belastet sind.

Ein umfassender Persönlichkeitsrechtsschutz der Betroffenen ist momentan nicht gewährleistet. Auf der einen Seite bleibt Verbrauchern aufgrund mangelnder Transparenz verborgen, warum beispielsweise schlechtere Kreditkonditionen eines Mobilfunkvertrages angeboten werden als anderen. Auf der anderen Seite könnte vollkommene Transparenz bei der Scoreberechnung eine verhaltenssteuernde Wirkung auf den Verbraucher entfalten. Ob dies gesellschaftspolitisch wünschenswert ist, muss offen diskutiert werden. Eine gesellschaftliche Debatte um Selbstbestimmung und neue Konturen eines Persönlichkeitsrechts im Zeitalter von Big Data muss daher angestoßen werden.[149]

Diese Probleme überschneiden sich mit der Diskussion darüber, ob die Anwendung algorithmenbasierter Systeme transparenter gestaltet sein sollte und wie ein angemessener Interessenausgleich zwischen Unternehmen und Privatpersonen gewährleistet werden kann. Für eine umfassendere Regelung spricht, dass Scoring nur einer von vielen Bereichen ist, die durch die stetig wachsende Zahl verfügbarer Daten und die neuen Möglichkeiten der Datenverarbeitung einen von Euphorie getragenen Aufschwung erlebt haben. Scoring hat längst den Bereich der Kreditwirtschaft verlassen und entwickelt das Potenzial zu einem gesamtgesellschaftlichen, branchenübergreifenden Phänomen. Wirtschaftliche Effizienzsteigerung und technische Fortentwicklung können grundsätzlich einer gesellschaftlichen Weiterentwicklung zuträglich sein, bedürfen aber einer Begleitung durch eine Wertediskussion, die dafür sorgt, dass insbesondere die Interessen von Verbrauchern und Bürgern nicht unberücksichtigt bleiben. Ob Transparenz allein zu einem Ausgleich dieser gesellschaftlich relevanten Interessen zwischen Unternehmen und Privatpersonen führen kann, muss hinterfragt und diskutiert werden.

Scoring stellt damit nicht nur das Datenschutzrecht vor Herausforderungen, sondern wirft Fragen auf, mit denen sich die Gesellschaft insgesamt auseinandersetzen muss. Dabei muss das enorme Veränderungspotenzial, das Scoring für die moderne Gesellschaft mitbringt, beachtet werden. Immer neue technische Entwicklungen ermöglichen umfangreichere und genauere Prognoseverfahren. Das Bewerten von Per-

149 Dazu bereits Friedewald/Lamla/Roßnagel(Hrsg.) (2017) Informationelle Selbstbestimmung im digitalen Wandel, Verlag Springer Vieweg.

sonen anhand von Daten und Zahlen greift auf immer mehr alltägliche Lebensbereiche über. Klar ist, dass es langfristig eines weiten Lösungsansatzes bedarf, in dem Datenschutz nur *ein* Baustein eines umfassenderen Regelwerks ist.

Alles in allem sollte der Fokus auf das Gerüst von Rechtsvorschriften für Scoring und algorithmenbasierte Systeme den Blick auf die größeren gesellschaftlichen Fragen nicht verbergen: welchen gesellschaftlichen Nutzen bringen bestimmte technische Neuerungen? Sollten nicht nur die Verwendung bestimmter Daten, sondern auch Scoring in bestimmten, besonders sensiblen Lebensbereichen wie Gesundheit eingeschränkt werden? Welche normativen Steuerungseffekte von Scoring sind gesellschaftspolitische wünschenswert oder akzeptabel und welche nicht? Bei diesen und weitergehenden Diskussionen muss die normative Kraft von Scoringergebnissen im Vordergrund stehen und damit nicht nur ihr Einfluss auf das verfassungsrechtlich garantierte Recht auf informationelle Selbstbestimmung des Einzelnen, sondern vielmehr auch ihr Potenzial zur (Neu-)Ordnung von gesellschaftlichen Strukturen und Beziehungen im Ganzen.

VII Literatur und Quellen

Albrecht, J. & Jotzo, F. (2017). Das neue Datenschutzrecht der EU. Baden-Baden: Nomos Verlag.

Alvarez, P. & Soares, S. (2013). Schufa für die Welt?. Zeit Online vom 07.11.2013. Verfügbar unter: http://www.zeit.de/2013/46/kreditech-scoring-kreditwuerdigkeit-schufa [17.04.2018].

Auer-Reinsdorff, A. & Conrad, I. (Hrsg.) (2016). Handbuch IT- und Datenschutzrecht. 2. Auflage, München: C.H. Beck Verlag.

Bamberger, H., Roth, H., Hau, W., Poseck & R. (Hrsg.) (2017). Beck'scher Online-Kommentar BGB. 43. Edition, München: C.H.Beck Verlag.

Bigalke, S. (2013). Tipps zum Umgang mit der Schufa. Verfügbar unter: https://www.sueddeutsche.de/geld/auskunftsdatei-fuer-kreditvergabe-tipps-zum-umgang-mit-der-schufa-1.1768547 [16.05.2018].

Culik, N. & Döpke, C. Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen. Zeitschrift für Datenschutz, 5, 226-230.

Dammann, U. (2016). Erfolge und Defizite der Datenschutzgrundverordnung. Zeitschrift für Datenschutz, 7, 307-314.

Dix, A. (2017). Daten als Bezahlung – Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht. Zeitschrift für Europäisches Privatrecht, 1, 1-5.

Engels, T. (2014). Kein Anspruch auf Auskunft über Scoreformel, Der IT-Rechts-Berater, 5, 100-101.

Forgó, N., Helfrich, M. & Schneider, J. (2017). Betrieblicher Datenschutz, 2. Auflage, München: C.H. Beck Verlag.

Friedewald, M., Lamla, J. & Roßnagel, A. (2017). Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden: Springer Vieweg.

Gärtner, S. (2014). Scoring und Datenschutz. Zeitschrift für Bank- und Kapitalmarktrecht, 5, 197-199.

Geslevich-Packing, N. & Lev-Aretz, Y. (2016). On Social Credit and the right to be unnetworked. Columbia Business Law Review, 2, 339-425.

Gola, P. (Hrsg.). (2017). Datenschutz-Grundverordnung. 1. Auflage, München: C.H. Beck Verlag.

Gola, P., Klug, C., Körffer, B. & Schomerus, R. (2015). Bundesdatenschutzgesetz, 12. Auflage, München: C.H. Beck Verlag.

Goldmedia. (2017). Ökonomischer Wert von Verbraucherdaten für Adress- und Datenhändler. Studie im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz.

Herzog, R., Scholz, R., Herdegen & M., Klein, H. (2016). Grundgesetz, 79. Ergänzungslieferung, München: C.H.Beck Verlag.

Hoeren, T., Sieber, U. & Holznagel, B. (2017). Handbuch Multimedia-Recht, 44. Ergänzungslieferung, München: C.H. Beck Verlag.

Helbing, T. (2015). Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung. Kommunikation & Recht, 3, 145-150.

Helfrich, M. (2017). DSAnpUG-EU: Ist der sperrige Name hier schon Programm?. Zeitschrift für Datenschutz, 3, 97-98.

Härting, N. (2015). Zweckbindung und Zweckänderung im Datenschutzrecht. Neue Juristische Wochenschrift, 45, 3284-3288.

Helberger N., Borgesius F. & Reyna A. (2017). The Perfect Match? A closer look at the relationship between EU consumer law and data protection law. Common Market Law Review, 54, (5).

Hiller, A. (2017). Social-Media Analyse und Profilierung bei Versicherungen beeinflussen nicht nur Mitgliedsbeiträge. Verfügbar unter: https://netzpolitik.org/2017/social-media-analyse-und-profilierung-bei-versicherungen-beeinflussen-nicht-nur-mitgliedsbeitraege/ [09.02.2018].

Hoeren, T. (2009). Datenschutz und Scoring: Grundelemente der BDSG-Novelle I. Verbraucher und Recht, 10, 363-369.

Hoffmann-Riem, W. (2017), Verhaltensstuerung durch Algorithmen – Eine Herausforderung für das Recht. Archiv des öffentlichen Rechts, 142, 1-42.

Hull, G. (2015). Successful Failure: What Foucault can Teach Us about Privacy Self-Management in a World of Facebook and Big Data. Ethics and Information Technology, 17 (2) 89-101.

Hunt, E. (2017). Amazon Kindle's Terms 'unreasonable' and would take nine hours to read, Choice says. Verfügbar unter: https://www.theguardian.com/australia-news/2017/mar/15/amazon-kindles-terms-unreasonable-and-would-take-nine-hours-to-read-choice-says [24.05.2018].

Kamlah, W. (1999). Das Schufa-Verfahren und seine datenschutzrechtliche Zulässigkeit. Multi Media und Recht, 7, 395-404.

Kamp, M. & Weichert, T. (2005). Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher. Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft.

Koreng, A. & Lachenmann, M. (Hrsg.). (2018). Formularhandbuch Datenschutzrecht. 2. Auflage 2018, München: C.H. Beck Verlag.

Kühling, J., Martini, M., Heberlein, J., Kühl, B., Nink, D., Weinzierl, Q. & Wenzel, M. (2016). Die Datenschutz-Grundverordnung und das nationale Recht. Münster: Verlagshaus Monsenstein und Vannerdat OHG.

Kühling, J. & Buchner, B. (Hrsg.). (2018). DS-GVO, BDSG, 2. Auflage 2018, München: C.H. Beck Verlag.

Krüger, P. (2016). Datensouveränität und Digitalisierung, Probleme und rechtliche Lösungsansätze. Zeitschrift für Rechtspolitik, 7, 190–192.

Von Lewinski, K., von Lewinski, D. (2014). Evidenz-basierter Datenschutz. Datenschutz und Datensicherheit, 38 (3), 175-180.

Martini, M. (2014). Big Data als Herausforderung für den Persönlichkeitsschutz, Deutsches Verwaltungsblatt, 23, 1481-1489.

Martini, M. (2017). Algorithmen als Herausforderung für die Rechtsordnung. Juristenzeitung, 21, 1017-1025.

McDonald, A. & Cranor, L. (2008). The Cost of Reading Privacy Policies. Journal of Law and Policy for the Information Society, 4 (3), 543-568.

Moos, F. & Rothkegel, T. (2016). Nutzung von Scoring-Diensten im Online-Versandhandel. Zeitschrift für Datenschutz, 12, 561-568.

Morozov, E. (2013). Bonität übers Handy. Verfügbar unter: http://www.faz.net/aktuell/feuilleton/silicon-demokratie/kolumne-silicon-demokratie-bonitaet-uebers-handy-12060602.html [24.05.2018].

Paal, B. & Pauly, D. (Hrsg.). (2017). Datenschutz-Grundverordnung. München: C.H. Beck Verlag.

Säcker, J., Rixecker, R., Oetker, H. & Limpberg, B. (Hrsg.). (2016). Münchener Kommentar zum Bürgerlichen Gesetzbuch. München: C.H. Beck Verlag.

Schmidt, K. (Hrsg.). (2013). Münchener Kommentar zum Handelsgesetzbuch. 3. Auflage, München: C.H. Beck Verlag.

Simits, S. (Hrsg.). (2014). Bundesdatenschutzgesetz. 8. Auflage, Baden-Baden: Nomos Verlag.

Sydow, G. (Hrsg.). (2017). Europäische Datenschutzgrundverordnung, Baden-Baden: Nomos Verlag.

Wolff, H. & Brink, S. (Hrsg.). (2017). Beck'scher Online-Kommentar. 22. Edition, München: C.H. Beck Verlag.

Roßnagel, A. (2013). Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. Zeitschrift für Datenschutz, 11, 562-567.

Roßnagel, A. (2017). Gesetzgebung im Rahmen der Datenschutz-Grundverordnung. Datenschutz und Datensicherheit, 41, (5), 277-281.

Schantz, P. (2016). Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. Neue Juristische Wochenschrift, 26, 1841-1847.

Schneider, J. (2017). Schließt Art. 9 DSGVO die Zulässigkeit der Verarbeitung bei Big Data aus? Überlegungen, wie weit die Untersagung bei besonderen Datenkategorien reicht. Zeitschrift für Datenschutz, 7, 303-308.

Seiderer, S. (2012). Was Social Media bereits über Ihre Bonität verrät. Verfügbar unter: https://www.welt.de/regionales/hamburg/article108401373/Was-Social-Media-bereits-ueber-Ihre-Bonitaet-verraet.html [28.05.2018].

Seiler, D. (2017). Scoring im neuen EU-Datenschutzrecht. JurisPR Bank und Kapitalmarktrecht, 8, Anm. 1.

Sokol, B. (Hrsg.). (2005). Living by numbers. Düsseldorf: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

SVRV (2016). Verbraucherrecht 2.0. Verbraucher in der digitalen Welt. Gutachten des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen.

SVRV (2017). Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen.

Taeger, J. (2016). Scoring in Deutschland nach der EU-Datenschutzgrundverordnung. Zeitschrift für Rechtspolitik, 3, 72-75.

Taeger, J. (2017). Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018. Recht der Datenverarbeitung, 1, 3-9.

Taeger, J. (2014). Anmerkung zu BGH, Urteil vom 28.01.2014, VI ZR 156/13. MultiMedia und Recht, 7, 489-494.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) & GP Forschungsgruppe (2014). Scoring nach der Datenschutz-Novelle 2009 und neue Entwickungen. Studie im Auftrag der Bundesanstalt für Ernährung, des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz und des Bundesministeriums der Justiz und für Verbraucherschutz.

Veil, W. (2018). Die Datenschutz-Grundverordnung: des Kaisers neue Kleider. Neue Zeitschrift für Verwaltungsrecht, 10, 686-696.

Weichert, T. (2014). Scoring in Zeiten von Big Data. Zeitschrift für Rechtspolitik, 6, 168-171.

Wuermeling, U. (2002). Scoring von Kreditrisiken. Neue Juristische Wochenschrift, 48, 3508-3510.

Ziegenhorn, G. & von Heckel, K. (2016). Datenverarbeitung durch Private nach der europäischen Datenschutzreform. Neue Zeitschrift für Verwaltungsrecht, 22, 1585-1591.

Sachverständigenrat für Verbraucherfragen

Der Sachverständigenrat für Verbraucherfragen ist ein Beratungsgremium des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV). Er wurde im November 2014 vom Bundesminister der Justiz und für Verbraucherschutz, Heiko Maas, eingerichtet. Der Sachverständigenrat für Verbraucherfragen soll auf der Basis wissenschaftlicher Erkenntnisse und unter Berücksichtigung der Erfahrungen aus der Praxis das Bundesministerium der Justiz und für Verbraucherschutz bei der Gestaltung der Verbraucherpolitik unterstützen.

Der Sachverständigenrat ist unabhängig und hat seinen Sitz in Berlin.

Vorsitzende des Sachverständigenrats ist Prof. Dr. Lucia Reisch.