Gerald Spindler, Christian Thorun, Jörn Wittmann

# Rechtsdurchsetzung im Verbraucherdatenschutz

## Bestandsaufnahme und Handlungsempfehlungen

gute gesellschaft –
soziale demokratie
#2017 plus

FRIEDRICH EBERT STIFTUNG

gute gesellschaft –
soziale demokratie
#2017 plus

EIN PROJEKT DER FRIEDRICH-EBERT-STIFTUNG
IN DEN JAHREN 2015 BIS 2017

Was macht eine Gute Gesellschaft aus? Wir verstehen darunter soziale Gerechtigkeit, ökologische Nachhaltigkeit, eine innovative und erfolgreiche Wirtschaft und eine Demokratie, an der die Bürger_innen aktiv mitwirken. Diese Gesellschaft wird getragen von den Grundwerten der Freiheit, Gerechtigkeit und Solidarität.

Wir brauchen neue Ideen und Konzepte, um die Gute Gesellschaft nicht zur Utopie werden zu lassen. Deswegen entwickelt die Friedrich-Ebert-Stiftung konkrete Handlungsempfehlungen für die Politik der kommenden Jahre. Folgende Themenbereiche stehen dabei im Mittelpunkt:

- Debatte um Grundwerte: Freiheit, Gerechtigkeit und Solidarität;
- Demokratie und demokratische Teilhabe;
- neues Wachstum und gestaltende Wirtschafts- und Finanzpolitik;
- Gute Arbeit und sozialer Fortschritt.

Eine Gute Gesellschaft entsteht nicht von selbst, sie muss kontinuierlich unter Mitwirkung von uns allen gestaltet werden. Für dieses Projekt nutzt die Friedrich-Ebert-Stiftung ihr weltweites Netzwerk, um die deutsche, europäische und internationale Perspektive miteinander zu verbinden. In zahlreichen Veröffentlichungen und Veranstaltungen in den Jahren 2015 bis 2017 wird sich die Stiftung dem Thema kontinuierlich widmen, um die Gute Gesellschaft zukunftsfähig zu machen.

Weitere Informationen zum Projekt erhalten Sie hier:
**www.fes-2017plus.de**

## Die Friedrich-Ebert-Stiftung

Die Friedrich-Ebert-Stiftung (FES) wurde 1925 gegründet und ist die traditionsreichste politische Stiftung Deutschlands. Dem Vermächtnis ihres Namensgebers ist sie bis heute verpflichtet und setzt sich für die Grundwerte der Sozialen Demokratie ein: Freiheit, Gerechtigkeit und Solidarität. Ideell ist sie der Sozialdemokratie und den freien Gewerkschaften verbunden.

Die FES fördert die Soziale Demokratie vor allem durch:

- politische Bildungsarbeit zur Stärkung der Zivilgesellschaft;
- Politikberatung;
- internationale Zusammenarbeit mit Auslandsbüros in über 100 Ländern;
- Begabtenförderung;
- das kollektive Gedächtnis der Sozialen Demokratie mit u. a. Archiv und Bibliothek.

## Über die Autor dieser Ausgabe

**Prof. Dr. Gerald Spindler** ist Direktor des Instituts für Wirtschaftsrecht an der Juristischen Fakultät der Georg-August-Universität Göttingen, Mitglied der Akademie der Wissenschaften zu Göttingen, Herausgeber mehrerer Zeitschriften im Bereich des IT-Rechts und berät sowohl die Bundesregierung als auch die EU-Kommission in Fragen des Internetrechts.
**Prof. Dr. Christian Thorun** ist Geschäftsführer des Instituts für Verbraucherpolitik (ConPolicy GmbH), Professor für Politikwissenschaft, Internationale Politik und Public Affairs an der Quadriga Hochschule Berlin, Beiratsmitglied beim Verein für Selbstregulierung der Informationswirtschaft (SRIW) und assoziiertes Mitglied des Think Tank 30.
**Jörn Wittmann** ist Jurist und zertifizierter Datenschutzbeauftragter, Doktorand an der Universität Göttingen und beim Verein für Selbstregulierung der Informationswirtschaft (SRIW) beschäftigt.

## Für diese Publikation ist in der FES verantwortlich

**Dr. Robert Philipps**, Abteilung Wirtschafts- und Sozialpolitik, Leiter des Arbeitskreises Mittelstand und des Gesprächskreises Verbraucherpolitik.

Gerald Spindler, Christian Thorun, Jörn Wittmann

# Rechtsdurchsetzung im Verbraucherdatenschutz

## Bestandsaufnahme und Handlungsempfehlungen



>

>

# ZUSAMMENFASSUNG

Die Digitalisierung prägt unseren Alltag. Allerdings sind ihre Effekte für Verbraucher_innen als ambivalent einzustufen. Auf der einen Seite profitieren diese von neuen Angeboten, auf der anderen Seite geht Digitalisierung einher mit einer „flüchtigen Überwachung", Profilbildung und Segmentierung.

Meinungsumfragen zeigen, dass Verbraucher_innen vor dem Hintergrund dieser Ambivalenz durchaus verunsichert sind. Sie geben an, nur unzureichend über eine Kontrolle ihrer Daten zu verfügen, bemängeln, dass sie oft mehr persönliche Daten preisgeben müssen als notwendig, und befürchten, etwa Opfer eines Weiterverkaufs ihrer Daten zu werden.

Diese Sorgen werfen nicht nur die Frage auf, ob die Verbraucherrechte im Bereich des Datenschutzes ausreichen, sondern auch, ob die bestehenden Rechte in einer effektiven Weise durchgesetzt werden. Denn genau an dieser Effektivität kommen immer wieder Zweifel auf. So zeigen unterschiedliche Marktuntersuchungen, dass bspw. App-Anbieter die Nutzer_innen nicht oder nur unzureichend über die Datenverarbeitung informieren. Auch sind diese Erklärungen oft in einer Sprache verfasst, die für die Nutzer_innen nicht verständlich ist.

Diese Studie zielt darauf ab, das deutsche System der Rechtsdurchsetzung im Verbraucherdatenschutz einer kritischen Bestandsanalyse zu unterziehen. Hierbei werden fünf Rechtsdurchsetzungsinstrumente betrachtet: Betroffenenrechte, die staatliche Aufsicht, die kollektive Rechtsdurchsetzung durch anerkannte Verbraucherverbände, die betrieblichen Datenschutzbeauftragten und die Ko-Regulierung. Zudem wird für jedes dieser Instrumente analysiert, mit welchen Auswirkungen durch die Regelungen der Datenschutz-Grundverordnung (DS-GVO), auf die sich die EU-Institutionen im Rahmen des Trilogs am 15.12.2015 geeinigt haben, zu rechnen ist.

Ein wichtiges Ergebnis der Studie ist: Bei den Betroffenenrechten, der staatlichen Aufsicht sowie der Ko-Regulierung ist der Handlungsbedarf am größten. Da die Bundesregierung die gesetzliche Grundlage zur kollektiven Rechtsdurchsetzung durch Verbraucherverbände jüngst verändert hat, ist zugleich davon auszugehen, dass sich die Lage in diesem Bereich spürbar verbessern wird. Am System der Datenschutzbeauftragten sollte zudem weiter festgehalten werden.

Die vorliegende Studie zeigt außerdem zahlreiche Maßnahmen auf, mit deren Hilfe die Rechtsdurchsetzung verbessert werden könnte. Diese Vorschläge reichen von einer Vereinfachung der Datenschutzerklärungen, über die Förderung der Prinzipien Privacy by Design und Privacy by Default bis hin zu Maßnahmen, um die staatliche Aufsicht zu stärken und die Anreize für die Ko-Regulierung zu erhöhen.

**DR. ROBERT PHILIPPS**
**PROF. DR. GERALD SPINDLER**
**PROF. DR. CHRISTIAN THORUN**
**JÖRN WITTMANN**

# 1

# EINLEITUNG

## 1.1 HINTERGRUND

Die Digitalisierung des Alltags und der Wirtschaft ist ein prägendes Charakteristikum unserer Zeit. Informations- und Kommunikationstechnologien (IKT) stellen jedoch keinen eigenständigen Sektor mehr dar, sondern transformieren die unterschiedlichsten Lebens- und Wirtschaftsbereiche (European Commission 2015: 3). Beispiele hierfür sind die für viele Verbraucher_innen zur Normalität gewordene Kommunikation über Soziale Netzwerke, die Informationsbeschaffung über das Internet, Foren und Bewertungsportale, aber auch die Abwicklung ihrer Finanzen über das Onlinebanking, die Steuerung des Smart Home von der Couch aus oder der Einkauf rund um die Uhr, an jedem Tag in der Woche über das Internet oder die Smartphone-App.

Neben den vielfältigen positiven Effekten dieser Digitalisierung für die Verbraucher_innen führt diese Entwicklung allerdings auch dazu, dass Unternehmen exponentiell zunehmend mehr personenbezogene Daten über Verbraucher_innen erheben und auswerten. Diese Daten umfassen sehr weitgehende Informationen etwa über Vorlieben (wie die Interessen beim Lesen, den Musikgeschmack und die sozialen Kontakte) und konkretes Verhalten (Wie oft betätig sich jemand sportlich? Wann wird ferngesehen?). Mittlerweile können solche Daten ohne signifikante Kosten erhoben und im Rahmen von Big Data und Cloud Computing analysiert werden. Es ist davon auszugehen, dass sich diese Entwicklung in den kommenden Jahren fortsetzen und beschleunigen wird. Big Data-Anwendungen, das Internet der Dinge, eHealth, eMobility, Smart Home oder die Entwicklung von Wearables sind Beispiele hierfür.

Aus Verbrauchersicht sind die Effekte dieser Entwicklung insgesamt als ambivalent zu bewerten. Während Verbraucher_innen auf der einen Seite von neuen digitalen Diensten und Anwendungen profitieren, geht deren Entwicklung auf der anderen Seite mit einer Zunahme „flüchtiger Überwachung" einher (Baumann/Lyon 2013). Denn Verbraucherdaten werden häufig nicht nur für die Vertragsabwicklung, sondern auch für andere kommerzielle Zwecke verwendet: Beispielsweise werden sie für die sogenannte Profilbildung genutzt, um Verbraucher_innen zu segmentieren und ihnen zielgerichtete Werbung und Angebote unterbreiten zu können. Sie werden aber auch verwendet, um einigen Verbraucher_innen den Zugang zu bestimmten Produkten zu verwehren, oder genutzt, um Produkte und Dienstleistungen individuell zu bepreisen. Grundsätzlich können die neuen Datenerhebungs- und Verarbeitungsmöglichkeiten, wenn sie entgegen der Verbraucherinteressen genutzt werden, zu erheblichen Verletzungen der Persönlichkeitsrechte und anderer Rechtsgüter der Betroffenen führen.

Meinungsbefragungen zeigen, dass Verbraucher_innen durchaus verunsichert sind:

- So gaben 87 Prozent der Bundesbürger_innen in einer Befragung an, über keine komplette Kontrolle ihrer Daten zu verfügen (European Commission 2015: 10).
- Knapp 40 Prozent sind der Meinung, dass sie oft mehr persönliche Informationen beim Zugang zu Onlinediensten preisgeben müssen, als notwendig wäre (European Commission 2011: 49).
- In einer Befragung gaben 63 Prozent der Bundesbürger_innen an, sie würden befürchten, Opfer eines Weiterverkaufs ihrer Daten werden zu können, 44 Prozent sorgten sich, sie könnten abgehört werden, und knapp 40 Prozent sahen ein Risiko darin, Opfer von Phishing zu werden (Initiative D21 2014: 41).

Dieses Zahlen werfen nicht nur die Frage auf, ob das materielle Datenschutzrecht einen ausreichenden Rechtsschutz gewährleistet, sondern auch, ob die Rechtsdurchsetzung adäquat ist und demnach Rechtsverstöße durch Unternehmen konsequent geahndet werden – sei es durch die Verbraucher_innen selbst oder auch durch die Datenschutzaufsicht und andere Instrumente. Untersuchungen zeigen, dass durchaus Anlass zum Zweifel besteht. So stellte das Bayerische Landesamt für Datenschutzaufsicht jüngst im Rahmen eines Tests von Apps, die sich an Kinder richten, fest, dass bei lediglich 50 Prozent der untersuchten Apps Datenschutzerklärungen auf Deutsch angeboten wurden – ein klarer Rechtsverstoß bei der Hälfte der untersuchten Apps (Bayerisches Landesamt für Datenschutzaufsicht 2015). Auch verweisen Untersuchungen der Stiftung Warentest darauf, dass Apps häufig

mehr Daten auslesen, als es für die konkrete Dienstleistungserbringung notwendig wäre, dass Daten oft nicht anonymisiert und immer wieder unverschlüsselt übertragen werden (dies selbst bei essenziellen Informationen wie Benutzernamen und Passwörtern).[1]

## 1.2 ZIELSETZUNG UND FRAGESTELLUNGEN DER STUDIE

Vor diesem Hintergrund zielt die vorliegende Studie darauf ab, das System der Rechtsdurchsetzung im Verbraucherdatenschutz in Deutschland zusammenfassend darzustellen, Stärken und Schwächen herauszuarbeiten und Handlungsempfehlungen abzuleiten. Diese Handlungsempfehlungen werden eingebettet in die neuen Regelungen der Datenschutz-Grundverordnung (DS-GVO), auf die sich die europäischen Institutionen im Rahmen der Trilog-Verhandlungen am 15.12.2015 geeinigt haben. Hierfür werden die folgenden Leitfragen behandelt:

- Welche Akteure und Institutionen sind heute für die Rechtsdurchsetzung im Verbraucherdatenschutz in Deutschland zuständig?
- Welchen Stellenwert nehmen sie jeweils in der Rechtsdurchsetzung ein?
- Welche voraussichtlichen Auswirkungen hat die DS-GVO auf das System der Rechtsdurchsetzung in Deutschland?
- Über welche Stärken und Schwächen verfügen die unterschiedlichen Rechtsdurchsetzungsinstrumente?
- Welche politischen Handlungsbedarfe leiten sich insgesamt aus der Stärken- und Schwächenanalyse ab? Welche Handlungsempfehlungen können ausgesprochen werden?

## 1.3 VORGEHEN UND METHODISCHE EINSCHRÄNKUNGEN

Gemäß der Aufgabenstellung handelt es sich bei dieser Publikation um eine überblicksartige Studie der Rechtsdurchsetzung im Bereich des Verbraucherdatenschutzes in Deutschland. Sie basiert auf einer Auswertung der für das Thema relevanten Literatur sowie den Anregungen und Ergebnissen eines Expertengespräches der Friedrich-Ebert-Stiftung.

Durch den Überblickscharakter muss eine Reihe von Einschränkungen berücksichtigt werden:

- Der Fokus der Arbeit liegt auf dem Verbraucherdatenschutz. Die Rechtsdurchsetzung bzw. die Betroffenenrechte im öffentlichen Bereich werden daher nicht weiter thematisiert. Auch wird für eine bessere Lesbarkeit – wenn möglich – darauf verzichtet, die rechtlich präzisen Begriffe „Betroffene" und „verantwortliche Stelle" zu verwenden. Stattdessen werden die Begriffe „Verbraucher_in" und „Unternehmen" verwendet.
- In der Analyse der DS-GVO kann naheliegender Weise keine umfassende Bewertung aller voraussichtlichen datenschutzrechtlichen Auswirkungen auf Deutschland vorgenommen werden. Wir gehen daher selektiv vor und beschränken uns auf die Bereiche mit einem direkten Bezug zur Rechtsdurchsetzung. In den Ausnahmefällen, in denen wir auch auf weitere Datenschutzrechte mit mittelbarem Bezug zur Rechtsdurchsetzung eingehen (siehe hierzu etwa den Exkurs in Abschnitt 2.1.1.5), beschränken wir uns auf die Zweckbindung, Datenvermeidung und Datensparsamkeit, die Einwilligung sowie das Kopplungsverbot. Weitere relevante Fragen etwa nach der Definition des Personenbezugs oder der Begrenzung der Profilbildung werden hier ausgeklammert, um den Rahmen der Arbeit nicht zu sprengen. Für die Analyse der DS-GVO werden die öffentlich zugänglichen Dokumente der EU-Kommission vom 25.1.2012 sowie die Beschlüsse des Europäischen Parlaments vom 12.3.2014, des Rats der Europäischen Union vom 15.6.2015 sowie der Text, auf den sich die EU-Institutionen im Rahmen des Trilogs am 15.12.2015 geeinigt haben, herangezogen.[2]
- Das sogenannte Forum Shopping stellte bislang im Datenschutzrecht eine große Herausforderung dar. Zwar verfolgt die vollharmonisierende Datenschutzrichtlinie 96/46/EG (EuGH 2004: 95 m. Anm. Roßnagel; Vulin 2012: 415 ff.; Brühann 2011) den Zweck, ein gleichwertiges Schutzniveau innerhalb der Europäischen Union zu schaffen,[3] dennoch wich die konkrete Umsetzung und Auslegung der Datenschutzgesetze in der Vergangenheit innerhalb der EU teilweise voneinander ab. Das hat Unternehmen Anreize geliefert, den Sitz ihrer Niederlassung dort zu wählen, wo das Schutzniveau am geringsten ist (siehe dazu ausführlich Lejeune 2013: 823). Da die DS-GVO durch die direkte Bindungswirkung einer Verordnung unmittelbar ein einheitliches Datenschutzrecht im gesamten Gebiet der EU schaffen wird, entfällt die Herausforderung des Forum Shoppings weitgehend. Diese Thematik wird deshalb im Folgenden nicht weiter problematisiert.
- Überdies hat die Frage des anwendbaren Rechts in der Vergangenheit immer wieder große Probleme bereitet. Die weit überwiegende Zahl der großen Internetdienstanbieter stammt weder aus dem europäischen Rechtsraum noch erbringt sie ihre Dienste von dort. Das europäische Datenschutzrecht verfolgte bislang den Ansatz, dass innerhalb der EU/des EWR das Datenschutzrecht dort Anwendung findet, wo die für die Datenverarbeitung verantwortliche Stelle ihren Sitz hat (Sitzlandprinzip – § 1 Abs. 5 BDSG; Art. 4 Buchst. a) RL 95/46/EG). Außerhalb der EU/des EWR kommt das Recht zur Anwendung, indem die

1 Stiftung Warentest, Ausgespäht: Datenschutz bei Apps, test (6/2012), S. 38–43. Stiftung Warentest, Shopping-Apps: Nur zwei sind sicher und gut (11/2012), S. 38–42. Stiftung Warentest, Heiter bis wolkig: Wetter-Apps (6/2013), S. 83–85. und Stiftung Warentest, Spritpreis-Apps im Datenschutz-Test: Vier sind kritisch, Meldung vom 7.2.2014.

2 Hierbei werden zum einen die vom Bayerischen Landesamt für Datenschutzaufsicht zur Verfügung gestellte Synopse der DS-GVO als Grundlage verwendet (https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/BayLDA_Synopse_DS-GVO_KOMM-EU-Parlament-Rat_160623TK.pdf) als auch der Text, auf den sich die EU-Institutionen im Rahmen des Trilogs geeinigt haben (http://statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf).

3 RL 96/46/EG, ABl. L 281, S. 31, Erwägungsgründe 7 und 8.

relevanten Daten erhoben oder verarbeitet werden (Territorialprinzip – § 1 Abs. S. 2 BDSG; Art. 4 Buchst. c) RL 95/46/EG). Diese Regelungen haben in der Vergangenheit immer wieder zu Unklarheiten darüber geführt, welches Recht von welchem Staat im Einzelfall Anwendung finden muss.

Diese Unklarheiten werden mit der Einführung des Marktortprinzips im Rahmen der DS-GVO der Vergangenheit angehören (Art. 3 Abs. 2 DS-GVO-Entwurf). Mit Wirksamwerden der DS-GVO kommt immer dann das EU-Datenschutzrecht zur Anwendung, wenn ein Unternehmen sein Angebot auch auf die Verbraucher_innen mindestens eines EU-Mitgliedstaates ausrichtet. Die Unklarheiten, wann deutsches bzw. europäisches Datenschutzrecht zur Anwendung kommt, dürften damit weitestgehend der Vergangenheit angehören. Vor allem werden damit außereuropäische Betreiber weitverbreiteter Dienste – wie etwa von Suchmaschinen oder von Sozialen Netzwerken – unzweifelhaft mit ihren Angeboten den Anwendungsbereich des europäischen Datenschutzrechts betreten und dieses entsprechend zu befolgen haben. Da die Herausforderung des anwendbaren Rechts demnach mit dem Inkrafttreten der DS-GVO weitgehend gelöst ist, wird auch dieser Aspekt im Folgenden nicht thematisiert.

– In der Rechtsdurchsetzung könnten theoretisch auch die Mitbewerber eine Rolle spielen. Da dieses Instrument der Rechtsdurchsetzung im Bereich des Datenschutzrechts in Deutschland bislang jedoch sehr unausgeprägt ist und auch nicht abzusehen ist, ob und wann sich dass ändern könnte, wird dieser Aspekt hier nicht weiter diskutiert.

Die Studie ist in zwei wesentliche Kapitel untergliedert. Im zweiten Kapitel wird das System der Rechtsdurchsetzung in Deutschland beschrieben, werden die voraussichtlichen Implikationen, die sich aus der DS-GVO ergeben, erörtert und die Stärken und Schwächen der jeweiligen Instrumente herausgearbeitet. Im dritten Kapitel werden Handlungsempfehlungen abgeleitet.

# 2

# SYSTEM DER RECHTSDURCHSETZUNG IM VERBRAUCHERDATENSCHUTZ

Das System der Rechtsdurchsetzung im Verbraucherdatenschutz besteht in Deutschland im Wesentlichen aus fünf Säulen:[4]

1. Rechtsdurchsetzung durch die Betroffenen selbst;
2. staatliche Aufsicht durch die Datenschutzaufsicht;
3. Rechtsdurchsetzung durch anerkannte Verbraucherverbände;
4. Rechtsdurchsetzung durch die betrieblichen Datenschutzbeauftragten;
5. Rechtsdurchsetzung im Wege der Ko-Regulierung.

Diese fünf Säulen werden im Folgenden dargestellt und analysiert. Hierbei geht es sowohl darum, jeweils die rechtlichen Grundlagen aufzuzeigen und die voraussichtlichen Auswirkungen der DS-GVO abzuschätzen als auch die Stärken und Schwächen der Instrumente zu bewerten.

## 2.1 RECHTSDURCHSETZUNG DURCH DIE BETROFFENEN

Eine wesentliche Säule für die Rechtsdurchsetzung in einer freiheitlich-rechtstaatlichen Demokratie stellen die betroffenen Verbraucher_innen selbst dar. Diese sollten über Möglichkeiten verfügen, ihre Rechte effektiv durchzusetzen und Unternehmen ggf. im Rahmen haftungsrechtlicher Regelungen auch auf Schadensersatz zu verklagen.

Im Folgenden werden daher die Rechtsdurchsetzungsmöglichkeiten der Verbraucher_innen dargestellt. Zunächst wird erläutert, welchen Stellenwert das Bundesdatenschutzgesetz (BDSG) den betroffenen Verbraucher_innen selbst beimisst. Dargestellt werden in diesem Zusammenhang deren wesentliche Rechte auf 1) Auskunft, 2) Benachrichtigung, 3) Berichtigung, Löschung und Sperrung sowie 4) auf Widerspruch. Auch wird hier analysiert, welche Auswirkungen die DS-GVO auf die Betroffenenrechte haben könnte. In einem zweiten Schritt wird der haftungsrechtliche Schutz problematisiert, ehe im abschließenden dritten Schritt diese Rechtsdurchsetzungsmöglichkeiten einer Stärken- und Schwächenanalyse unterworfen werden.

### 2.1.1 DIE BETROFFENENRECHTE NACH DEM BDSG

Im Bundesdatenschutzgesetz (BDSG) finden sich auf der einen Seite Rechte, die Verbraucher_innen in die Lage versetzen sollen, Kenntnis über die Datenverarbeitungsprozesse bei Unternehmen zu erlangen. Hierbei handelt es sich um die Auskunfts- und Benachrichtigungsrechte (§§ 33 und 34 BDSG). Diese Rechte stellen sogenannte Transparenzregelungen[5] dar. Auf der anderen Seite sieht das BDSG Korrekturrechte für die betroffenen Verbraucher_innen vor. Hierbei handelt es sich um die Rechte zur Berichtigung, Löschung und Sperrung personenbezogener Daten (§§ 35 BDSG). Zudem besteht für den Einzelnen die Möglichkeit, unter gewissen Umständen einer rechtmäßigen Verarbeitung seiner personenbezogenen Daten zu widersprechen (§ 35 Abs. 5 BDSG).

Die Transparenzregelungen können als notwendige Voraussetzung für die Korrekturrechte der Betroffenen angesehen werden. Denn erst die Kenntnis, welche personenbezogenen Daten zu welchem Zweck verarbeitet werden, versetzt Verbraucher_innen in die Lage, ihre Rechte auf Berichtigung, Löschung und Sperrung sowie Widerspruch tatsächlich ausüben zu können (Gola et al. 2015: § 33 BDSG, Rn. 1; Plath/Kamlah 2013: § 35 BDSG, Rn. 1). Transparenz gegenüber den Betroffenen sowie deren korrigierende Einflussnahme auf Verarbeitungsprozesse bilden damit die wesentlichen Elemente der Rechtsdurchsetzung durch die Betroffenen im deutschen Datenschutzrecht (Simitis/Dix 2014: § 35 BDSG, Rn. 2 m. w. Nachw).

Der Kenntnis über die Verarbeitung personenbezogener Daten kommt jedoch nicht nur zentrale Bedeutung für die Ausübung der Korrekturrechte, sondern vielmehr auch für das

4 Die Rechtsdurchsetzung durch die Mitbewerber wird im Folgenden – wie in Abschnitt 1.3 erläutert – nicht berücksichtigt.

5 Weitere Transparenzregelungen sind z. B. § 13 Abs. 1 TMG bei Telemediendiensten oder § 93 Abs. 1 TKG bei Telekommunikationsdiensten sowie das Führen und Zurverfügungstellen eines Verfahrensverzeichnisses nach § 4g Abs. 2 S. 2 i. V. m § 4e S. 1 Nr. 1-8 BDSG. Zur Abgrenzung, wann es sich um einen Telemediendienst, einen Telekommunikationsdienst oder Rundfunk handelt, siehe ausführlich Spindler/Schuster (2015: § 1 TMG, Rn.1 ff.).

freiheitlich demokratische Gemeinwesen insgesamt zu. So stellte das Bundesverfassungsgericht (BVerfG) in seinem wegweisenden Volkszählungsurteil fest (BVerfG 1984, 419, 422):

*„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."*

Das hier manifestierte Transparenzgebot macht es daher auch verfassungsrechtlich zwingend erforderlich, dass der Einzelne stets wissen können muss, wer welche seine Person betreffenden Daten gespeichert hat und wie diese zu welchem Zweck verarbeitet werden. Vor diesem Hintergrund werden die vier oben genannten Betroffenenrechte im Folgenden dargestellt.

#### 2.1.1.1 Das Recht auf Auskunft

Das in § 34 BDSG geregelte Recht auf Auskunft berechtigt jeden/jede Verbraucher_in – unabhängig von seiner/ihrer Geschäftsfähigkeit und frei von Formvorschriften –, ein Auskunftsersuchen bei einer datenschutzrechtlich verantwortlichen Stelle einzureichen. Die Unternehmen haben daraufhin umfassend gegenüber den Verbraucher_innen offenzulegen, welche personenbezogenen Daten zur Person gespeichert sind, aus welcher Quelle diese Daten stammen, an welche Dritten Daten ggf. übermittelt werden bzw. wurden und welchen Zwecken die Speicherung dient (siehe ausführlich Gola et al. 2015: § 34 BDSG, Rn. 9 ff.).

Ein Unternehmen darf den Verbraucher_innen für die Auskunftserteilung grundsätzlich keine Kosten in Rechnung stellen (§ 34 Abs. 8 BDSG). Ausnahmen davon gelten jedoch, wenn die Geltendmachung des Auskunftsrechts rechtsmissbräuchlich erfolgt oder die Auskunft personenbezogene Daten betrifft, die geschäftsmäßig zum Zweck der Übermittlung gespeichert werden. Bei Letzterem kann nur einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangt werden. Die Erhebung eines Entgeltes für jede weitere Auskunft je Kalenderjahr ist zulässig, sofern die Betroffenen die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen können. Erfasst sind hiervon z. B. Sachverhalte, die Daten bei Auskunfteien und Kreditinformationseinrichtungen betreffen. Allerdings ist für die Erhebung eines Entgeltes stets erforderlich, dass der/die Auskunftsersuchende im konkreten Einzelfall tatsächlich erkennbar ihm/ihr anderenfalls entstehende Kosten einspart (siehe dazu Walz 1991: 368; Gola et al. 2015: § 34 BDSG, Rn. 21).

Das Auskunftsrecht ist gem. § 6 Abs. 1 BDSG unabdingbar, kann also nicht auf Basis einer Vereinbarung zwischen der verantwortlichen Stelle und den jeweils Betroffenen ausgeschlossen werden. Es wird flankiert durch weitere – nicht zwingend datenschutzrechtliche – gesetzliche oder ggf. vertragliche Ansprüche, z. B. auf Einsicht oder Vorlage von Unterlagen (siehe ausführlich Gola et al. 2015: § 34 BDSG Rn. 3; Simitis/Dix 2014: § 33 BDSG, Rn. 90 ff.).

#### 2.1.1.2 Das Recht auf Benachrichtigung

§ 33 BDSG legt fest, dass in dem Fall, dass personenbezogene Daten ohne Kenntnis der Betroffenen gespeichert werden, diese jedoch umfassend über die konkrete Verarbeitung zu informieren sind. Die Vorschrift ergänzt § 4 Abs. 3 BDSG, demzufolge Betroffene sowohl dann zu benachrichtigen sind, wenn die Daten ohne ihre Kenntnis bei ihnen selbst[6] oder bei einem Dritten erhoben werden. Dieses Recht auf Benachrichtigung erklärt sich vor dem Hintergrund, dass eine Datenerhebung und -verarbeitung nicht nur durch Einwilligung der Betroffenen selbst legitimiert werden, sondern auch auf Grundlage der vielfältig vorhandenen und über zahlreiche Gesetze verteilten datenschutzrechtlichen Erlaubnistatbestände erfolgen kann. Würde man es in den letztgenannten Fällen bei einem bloßen Auskunftsrecht der Betroffenen belassen, würde dem Transparenzgebot nicht hinreichend Rechnung getragen. Denn ohne erstmalige Information darüber, dass eine verantwortliche Stelle Daten über eine Person verarbeitet, würde mangels Kenntnis über den Datenverarbeitungsvorgang und korrekten Adressaten auch ein Auskunftsersuchen der Betroffenen leerlaufen.

#### 2.1.1.3 Das Recht auf Berichtigung, Löschung und Sperrung

Die in § 35 BDSG verankerten, ebenfalls unabdingbaren (§ 6 Abs. 1 BDSG) Regelungen hinsichtlich der Berichtigung, Löschung und Sperrung verhelfen Verbraucher_innen dazu, korrigierend in Datenverarbeitungsprozesse einzugreifen. Basis für diese korrigierenden Eingriffe ist das zuvor durch die datenschutzrechtlichen Transparenzregelungen erlangte Wissen. Die Rechte stehen nicht in Abhängigkeit von der Geltendmachung eines Anspruchs durch Betroffene, weswegen an dieser Stelle nicht nur Korrekturrechte der Betroffenen normiert werden, sondern ebenfalls entsprechende Pflichten der verantwortlichen Stelle, bei Vorliegen der Voraussetzungen der jeweili-

---

6 Gem. § 4 Abs. 2 S. 1 BDSG sind personenbezogene Daten grundsätzlich bei den Betroffenen selbst zu erheben. Ausnahmen davon regelt § 4 Abs. 2 S. 2 BDSG.

gen Regelung tätig zu werden.[7] Die Kosten für die Vornahme der Korrekturen hat die verantwortliche Stelle zu tragen.[8]

Das Recht auf Berichtigung verpflichtet datenschutzrechtlich verantwortliche Stellen dazu, personenbezogene Tatsachenangaben, die Auskunft über persönliche oder sachliche Verhältnisse eines/einer Betroffenen vermitteln, stets in Einklang mit der Wirklichkeit zu halten.[9] Dadurch soll unter anderem verhindert werden, dass aufgrund falscher, unvollständiger oder aus dem Kontext gerissener Informationen ein falscher Eindruck über die Betroffenen entsteht.[10] Daher müssen etwa auch Daten berichtigt werden, die zwar korrekt wiedergeben, dass eine Person eine bestehende Schuld nicht oder nicht vollständig gezahlt hat, aber keine Informationen dazu liefern, ob ggf. zulässige Gründe für ein solches Verhalten des/der Schuldner_in vorgelegen haben.[11]

Das Recht auf Löschung[12] ist Ausfluss der datenschutzrechtlichen Grundprinzipien der Datenvermeidung und der Datensparsamkeit (Taeger et al. 2013: § 35, Rn. 25). Es unterscheidet zwischen Sachverhalten, bei denen eine Löschung erfolgen kann (Abs. 2. S. 1), und solchen, bei denen die Löschung verpflichtend ist (Abs. 2. S. 2).[13] Weil es sich bei der Löschung personenbezogener Daten ebenfalls um einen Verarbeitungsvorgang i. S. d. BDSG handelt, muss entsprechend dem datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt nach § 4 Abs. 1 BDSG auch hierfür entweder eine Einwilligung des/der Betroffenen oder aber ein gesetzlicher Erlaubnistatbestand vorliegen (siehe dazu auch Taeger et al. 2013: § 35, Rn. 16):

– Die Kann-Vorschrift nach § 35 Abs. 2 S. 1 BDSG erlaubt das Löschen personenbezogener Daten, sofern keine gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungspflichten (Abs. 3 Nr. 1) oder schutzwürdigen Interessen des/der Betroffenen (Abs. 3 Nr. 2) dem entgegenstehen.
– Die verpflichtende Löschung nach Abs. 2 S. 2 erfolgt im Unterschied dazu, wenn die Speicherung unzulässig ist, also ohne Einwilligung oder nicht auf Basis eines Erlaubnistatbestandes erfolgte (Abs. 2 S. 2 Nr. 1), es sich um sensible Daten handelt, die das Persönlichkeitsrecht Betroffener besonders stark beeinträchtigen und deren Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden können (Abs. 2 S. 2 Nr. 2),[14] oder die Speicherung der Daten nicht mehr erforderlich ist (Abs. 2 S. 2 Nr. 3 und Nr. 4). Die Löschpflicht bei Wegfall der Erforderlichkeit ist Ausdruck des datenschutzrechtlichen Zweckbindungsgrundsatzes. Danach muss grundsätzlich ein unmittelbarer Zusammenhang zwischen konkreter Datenverarbeitung und dem ursprünglichen Zweck der Datenerhebung bestehen (Taeger et al. 2013: § 35, Rn. 25). Sind also die personenbezogenen Daten für die Zweckerfüllung nicht mehr erforderlich, greift die Löschverpflichtung.

Die Voraussetzungen für die Sperrung personenbezogener Daten regeln § 35 Abs. 3, 4, 4a, 6 und 8 BDSG. Sperrung meint hierbei gemäß der Legaldefinition des § 3 Abs. 4 Nr. 4 BDSG das Kennzeichnen gespeicherter personenbezogener Daten, um deren weitere Verarbeitung oder Nutzung einzuschränken. Sinn der Regelungen ist also eine Verarbeitungsbeschränkung der betroffenen personenbezogenen Daten auf einige wenige Ausnahmetatbestände (Abs. 8), mithin die Normierung eines relativen Nutzungsverbotes und eine Verschärfung des Zweckbindungsgrundsatzes (Simitis/Dix 2014: § 35, Rn. 47). Die Sperrung tritt immer dann an die Stelle der Löschung, wenn Letzteres aufgrund eines Hindernisses ausgeschlossen ist (Taeger et al. 2013: § 35, Rn. 31; siehe ausführlich zur Sperrung Simitis/Dix 2014: § 35, Rn. 46 ff.). Das können bspw. die bereits genannten gesetzlichen, satzungsgemäßen oder vertraglichen Aufbewahrungsfristen sein (Abs. 3 Nr. 1). Wird die Richtigkeit der Daten von einem Betroffenen bestritten und ist weder die Richtigkeit noch die Unrichtigkeit feststellbar (sogenannte Non-liquet-Situation), verpflichtet Abs. 4 ebenfalls zur Sperrung (Simitis/Dix 2014: § 35, Rn. 51).

#### 2.1.1.4 Das Recht auf Widerspruch

Nach § 35 Abs. 5 S. 1 steht Betroffenen das Recht zu, der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu widersprechen. Dieses Widerspruchsrecht gilt jedoch nicht uneingeschränkt. Denn einerseits ist das Recht nach S. 2 ausgeschlossen, wenn eine Rechtsvorschrift zu den entsprechenden Datenumgängen verpflichtet oder andererseits aber das schutzwürdige Interesse des Betroffenen im Einzelfall das der verantwortlichen Stelle nicht überwiegt. Die Vorschrift bleibt damit auf besondere Einzelfälle, die vom „Normalfall" abweichen, beschränkt (Simitis/Dix 2014: § 35, Rn. 56; Gola et al. 2015: § 35 BDSG, Rn. 28) und kann daher in aller Regeln nicht pauschal für gewisse Fallgruppen ohne eingehende Prüfung beantwortet werden. In jedem Fall liegen jedoch die Voraussetzungen für einen Widerspruch durch einen Betroffenen vor, wenn sein Leib und Leben aufgrund der Verarbeitung gefährdet ist (siehe ausführlich Simitis/Dix 2014: § 35, Rn. 58 f. m. w. Bsp.).

---

7 Vgl. Taeger et al. (2013: § 35, Rn. 8); Gola et al. (2015: § 35, Rn. 3 f.); Simitis/Dix (2014: § 35, Rn. 9); Plath/Kamlah (2013: § 35, Rn. 5); Erbs et al. (2015: § 20, Rn. 1 f., § 35, Rn. 2).

8 Vgl. Simitis/Dix (2014: § 35, Rn. 5); Taeger et al. (2015: § 35, Rn. 9); Plath/Kamlah (2013: § 35, Rn. 7).

9 Siehe ausführlich Simitis/Dix (2014: § 35, Rn. 9, insbesondere Rn. 13); zur Unterscheidung von Tatsachenangaben und Werturteilen siehe Simitis/Dix (2014: § 20, Rn. 9 ff.); siehe ferner Plath/Kamlah (2013: § 35, Rn. 10).

10 Siehe ausführlich Simitis/Dix (2014: § 35, Rn. 9, insbesondere Rn. 13); zur Unterscheidung von Tatsachenangaben und Werturteilen siehe Simitis/Dix (2014: § 20, Rn. 9 ff.); siehe ferner Plath/Kamlah (2013: § 35, Rn. 10).

11 Vgl. Simitis/Dix (2014: § 35, Rn. 9, 15); Taeger et al. (2013: § 35, Rn. 9); Gola et al. (2015: § 35, Rn. 5).

11 Simitis/Dix (2014: § 35, Rn. 15, siehe für weitere Beispiele in den Rn. 14 ff.) sowie bei Taeger et al. (2013: § 35, Rn. 10 ff.).

13 Nach § 3 Abs. 4 Nr. 5 BDSG bedeutet Löschen i. S. d. BDSG die Unkenntlichmachung gespeicherter personenbezogener Daten.

14 Abs. 2. S. 2 Nr. 2: „(…) Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten (…)"

### 2.1.1.5 Exkurs: Elementare weitere Datenschutzrechte mit mittelbarem Bezug zur Rechtsdurchsetzung

Neben den oben beschriebenen unmittelbaren Datenschutzrechten, die für die Rechtsdurchsetzung durch die Betroffenen selbst von zentraler Bedeutung sind, existiert eine Reihe weiterer Rechte, die zwar nur einen mittelbaren Bezug zur Rechtsdurchsetzung aufweisen, aber dennoch für das Funktionieren der Rechtsdurchsetzung durch die Betroffenen selbst von zentraler Bedeutung sind. Hierzu zählen: die Zweckbindung, Datenvermeidung und Datensparsamkeit, das Verbot mit Erlaubnisvorbehalt und die Einwilligung sowie das Kopplungsverbot. Diese Rechte werden im Folgenden überblicksartig dargestellt.

#### Zweckbindung, Datenvermeidung und Datensparsamkeit

Der bereits kurz angesprochene Zweckbindungsgrundsatz ist grundlegend für das derzeitige deutsche Datenschutzrecht (siehe etwa §§ 28 ff. BDSG) und fordert, dass personenbezogene Daten grundsätzlich nur für den Zweck verarbeitet werden dürfen, für den sie erhoben worden sind (Hoeren et al. 2015: Teil 16.1, Rn. 78 f.). Nur unter besonderen Voraussetzungen darf von diesem Grundsatz eine Ausnahme gemacht werden (Hoeren et al. 2015: Teil 16.1 Rn. 84 ff.).

Hinzu treten die Grundprinzipien der Datenvermeidung und der Datensparsamkeit (§ 3a BDSG), wonach personenbezogene Daten nur soweit erhoben, verarbeitet und genutzt werden dürfen, wie es der jeweilige legitime Zweck erfordert. Die Maxime hierbei ist: Es sollten so wenig Daten wie möglich erhoben und genutzt werden.

Die Zweckbindung, Datenvermeidung und Datensparsamkeit hängen demnach eng mit den oben beschriebenen Transparenzanforderungen zusammen. Denn je enger die Zweckbindung ausfällt und je weniger Daten überhaupt erhoben, gespeichert und verarbeitet werden, desto besser können Verbraucher_innen einen Überblick darüber be- und erhalten, welches Unternehmen mit welchem Ziel die eigenen Daten verarbeitet.

#### Verbot mit Erlaubnisvorbehalt und freiwillige, informierte und explizite Einwilligung

Das deutsche Datenschutzrecht wird vom Grundsatz des Verbots mit Erlaubnisvorbehalt geprägt. Gemäß § 4 Abs. 1 BDSG ist eine Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, es liegt eine Einwilligung des/der Betroffenen oder ein gesetzlicher Erlaubnistatbestand vor. Hierdurch soll sichergestellt werden, dass der/die Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner/ihrer personenbezogenen Daten entscheiden und somit das Recht auf informationelle Selbstbestimmung ausüben kann.

Demnach spielt die Einwilligung eine zentrale Rolle in der Dogmatik des Datenschutzrechts. Damit eine Einwilligung wirksam ist, muss sie freiwillig, informiert und explizit erfolgen: Verbraucher_innen dürfen nicht zur Einwilligung gedrängt werden; sie müssen nachvollziehen können, worin sie einwilligen; sie müssen klar erkennen können, dass sie einwilligen; sie müssen ihre Einwilligung für die Zukunft auch widerrufen können (Gola et al. 2015: § 4a, Rn. 25 ff.; Hansen 2015: 1). Dadurch sind sogenannte Blanko-Einwilligungen ausgeschlossen, in denen sich ein Betroffener mit jedweder Art von Datenverarbeitung einverstanden erklärt (Gola et al. 2015: § 4a, Rn. 26).

#### Kopplungsverbot

Das Bundesdatenschutzgesetz untersagt grundsätzlich, den Abschluss eines Vertrags von der Einwilligung zur Datennutzung abhängig zu machen. Eine Einwilligung muss de lege lata – wie oben beschrieben – freiwillig sein. Allerdings sind bei der bisherigen Regelung zwei gravierende Einschränkungen zu berücksichtigen. Zum einen beschränkt sich die derzeitige Regelung auf Fälle der Einwilligung im Bereich Werbung und Adresshandel. Zum anderen –noch wesentlich gravierender – ist das Kopplungsverbot nur dann wirksam, wenn dem/der Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist (§28 Abs. 3b S. 1 BDSG).

Mit anderen Worten ist das derzeitige Kopplungsverbot in der Praxis auf sogenannte Monopolverträge beschränkt.[15] Daher hat sich das Kopplungsverbot in den vergangenen Jahren auch weitgehend als ein stumpfes Schwert erwiesen. Denn gerade bei Angeboten global agierender Internetdienstleister, deren Geschäftsmodelle darauf beruhen, eine Einwilligung in die Verarbeitung personenbezogener Dienste als Gegenleistung für die entgeltfreie Nutzung der Dienste zu erlangen, stehen Nutzer_innen prinzipiell Alternativen zur Verfügung. Formal liegt daher kein Monopol vor (siehe ausführlich Gola et al. 2015: § 28, Rn. 46 m. w. Nachw.; Spindler et al. 2015: § 28 BDSG, Rn. 21). Für die Nutzer_innen stellen diese Alternativen jedoch häufig keine gleichwertige Leistung dar, wenn etwa ein Großteil der Freund_innen nicht in dem alternativen Sozialen Netzwerk vertreten ist (Bräutigam 2012: 636; Spindler et al. 2015: § 28 BDSG, Rn. 21). Durch die Beschränkung auf Monopolverträge ist die Wirksamkeit des Kopplungsverbots in der Praxis daher als sehr beschränkt einzustufen.

### 2.1.1.6 Absehbare Auswirkungen der DS-GVO auf die Betroffenenrechte

Die Bewertung der absehbaren Auswirkungen der DS-GVO auf die Betroffenenrechte fällt gemischt aus. Was die Auskunftsrechte der Verbraucher_innen betrifft, sahen Vorschläge des EU-Parlaments ein Betroffenenrecht auf Herausgabe einer Kopie der verarbeiteten persönlichen Daten in einem interoperablen elektronischen Format vor (Art. 15 Abs. 2a DS-GVO Parlamentsvorschlag) (siehe ausführlich m. w. Nachw. Bräutigam/Schmidt-Wudy 2015: 57 f.). Dieser Vorschlag unterscheidet sich von dem bislang in Deutschland geltenden Recht auf Auskunft, insofern Unternehmen bei Geltendmachung nicht nur darüber zu informieren haben, welche Daten zu welchem Zweck gespeichert und verarbeitet werden, sondern weitergehend auch die konkret gespeicherten Daten an den Betroffenen übermitteln müssen. Gemäß Art. 15 Abs. 1b DS-GVO findet sich dieses Recht auf Herausgabe nun in der Verordnung. Der Vorschlag des Parlaments, dass hierfür ein interoperables elektronisches Format einzusetzen ist, wurde allerdings nicht in der endgültigen Fassung übernommen; vielmehr verweist Art. 15 Abs. 1b DS-GVO jetzt auf eine „electronic form which is commonly used". Im Gegensatz zum bisher nur auf Auskunft be-

---

**15** Gola et al. (2015: § 28, Rn. 46); weitergehend Spindler et al. (2015: § 28, Rn. 19), sofern zwar keine Monopolstellung vorliegt, aber sämtliche Anbieter der Dienstleistung auf dem Markt die Erbringung von der Abgabe der Einwilligung abhängig machen; siehe auch Peifer (2010: 525).

schränkten Recht erhalten damit die Nutzer_innen den kompletten Datensatz und können ihn unter Umständen anderweitig verwenden. Befürchtungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, das Recht auf die Unentgeltlichkeit einer Auskunft könne durch die neue Regelung in Gefahr sein, haben sich im Verlauf der Verhandlungen indes nicht bewahrheitet. Art. 15 Abs. 1b der DS-GVO hält nun fest, dass die erste Kopie unentgeltlich erfolgen muss. Daraus kann der Umkehrschluss gezogen werden, dass die anderen Auskunftsarten auch unentgeltlich erfolgen müssen.

Die Bilanz hinsichtlich der Rechte mit einem mittelbaren Bezug zu den Rechtsdurchsetzungsmöglichkeiten der Betroffenen (vgl. Exkurs im Abschnitt 2.1.1.5) fällt wie folgt aus:

- Im Verhandlungsverlauf wurde befürchtet, der Zweckbindungsgrundsatz und das Ziel der Datensparsamkeit könnten aufgeweicht werden (siehe hierzu Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2015: 5). Allerdings ist gerade die Formulierung in Art. 6 Abs. 4 des Ratsvorschlages[16], die auf eine solche Aufweichung zugunsten von Big Data hindeuten könnte, nicht mehr in der finalen Fassung enthalten. Andererseits erlaubt Art. 6 Abs. 3a der finalen Fassung ein Abweichen von den ursprünglichen Zwecken der Datenerhebung und -verarbeitung – zwar mit restriktiveren Vorzeichen als in der Ratsfassung, erlaubt sie aber dennoch.
- Hinsichtlich des Prinzips einer freiwilligen, informierten und expliziten Einwilligung ist zu konstatieren, dass die finale Fassung nunmehr in Art. 6 Abs. 1 und Art. 7 eine partielle Rückkehr zum Vorschlag der Kommission enthält. Die Erwägungsgründe Nr. 32, 34 verweisen jetzt deutlich auf die erforderliche Freiwilligkeit und führen Beispiele für fehlende Freiwilligkeit an, insbesondere wenn eine „imbalance" zwischen dem/der Nutzer_in und dem Datenverarbeiter vorliegt).
- Anders als noch im Kommissionsentwurf findet sich in Art. 7 Abs. 4 nur ein auf Interessenabwägung gerichtetes Kopplungsverbot wieder.[17] Im Unterschied zu § 28 Abs. 3b BDSG gilt damit jedoch das Kopplungsverbot für alle Datenverarbeitungszwecke und nicht nur – wie im BDSG – im Bereich der Werbung und des Adresshandels.
- Eine gesonderte Einwilligung in jede Datenverarbeitung, die etwa generelle Einwilligungen in Allgemeinen Geschäftsbedingungen (AGB) ausschlösse, enthält die DS-GVO ebenfalls nur ansatzweise. Nur in Art. 7 Abs. 2 sieht sie vor, dass bei einer Einwilligung, die sich auf mehrere Sachverhalte bezieht, eine klare und verständliche Sprache sowie Transparenz erforderlich sind, sodass für den/die Nutzer_in klar wird, dass sich die Einwilligung auf mehrere Vorgänge erstreckt. Allerdings beschränkt Art. 7 Abs. 2 dieses besondere Transparenzgebot auf „schriftliche" Erklärungen. Die DS-GVO kann aber auch so verstanden werden, dass bei einer Einwilligung für mehrere Sachverhalte tendenziell getrennte Einwilligungen erforderlich sind. Wortlaut und Begründund der DS-GVO sind hier nicht völlig eindeutig.

Insgesamt ist festzuhalten, dass die DS-GVO an einigen Stellen Verbesserungen für die Betroffenenrechte verspricht (etwa hinsichtlich der Herausgabe einer Kopie der gespeicherten Daten oder der Ausweitung des Anwendungsbereichs des Kopplungsverbots). Auf der anderen Seite gibt es jedoch an vielen Stellen Interessenabwägungsklauseln. Hierzu zählen etwa die Regelungen des Art. 6 Abs. 3a zur Zweckbindung sowie Art. 6 Abs. 1 und Art. 7 zur Einwilligung. Überdies sieht die Verordnung Möglichkeiten für abweichende Bestimmungen in den Mitgliedstaaten vor.[18] Hierdurch wird zwar die Flexibilität in der Anwendung erhöht. Allerdings leiden Rechtssicherheit sowie einheitliche EU-weite Regelungen, die ein wesentliches Ziel der DS-GVO darstellen. Insgesamt fällt das Zwischenfazit hinsichtlich der Betroffenenrechte daher ambivalent aus.

### 2.1.2 HAFTUNGSRECHTLICHER SCHUTZ

Neben den Transparenz- und Korrekturregelungen sieht das BDSG auch Schadensersatzansprüche für Verbraucher_innen vor. So verpflichtet § 7 BDSG Unternehmen zum Schadensersatz, wenn einem/einer Betroffenen ein materieller Schaden auf Basis eines sorgfaltswidrigen, unzulässigen Umgangs mit personenbezogenen Daten nach den geltenden Datenschutzgesetzen entstanden ist.

Bei den Schadensersatzvorschriften des BDSG handelt es sich nicht um abschließende Regelungen. Betroffene können daher auch auf Basis der allgemeinen deliktischen und vertraglichen Haftungsregelungen beispielsweise den Ersatz materieller und immaterieller Schäden begehren oder vorbeugend gegen verantwortliche Stellen im Wege des Unterlassungsanspruchs nach § 1004 BGB vorgehen (siehe ausführlich Gola et al. 2015: § 7, Rn. 16 ff., § 35, Rn. 26).

### 2.1.3 STÄRKEN- UND SCHWÄCHENANALYSE

Betrachtet man die derzeitige Rechtslage und die darin zahlreich vorhandenen Transparenz- und Korrekturregelungen, vermittelt sich der Eindruck, die betroffenen Verbraucher_innen würden sowohl in hinreichender Weise über die Verarbeitung ihrer personenbezogenen Daten informiert als auch über umfassende Möglichkeiten verfügen, ihre informationelle Selbstbestimmung eigenständig durch Berichtigungen, Löschungen und Sperrungen durchzusetzen.

Tatsächlich existieren in der Praxis der Rechtsdurchsetzung durch die Betroffenen jedoch zahlreiche Defizite. So ist hin-

16 „Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject."

17 „When assessing whether consent is freely given, utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract." Der Kommissionsvorschlag ging noch von einem unbedingten Koppelungsverbot aus.

18 Z. B. Art. 6 Abs. 2a DS-GVO, der den Mitgliedstaaten spezifische Datenschutzbestimmungen im Rahmen des Art. 6 Abs. 1 c, e DS-GVO erlaubt (Erfüllung gesetzlicher Pflichten oder im öffentlichen Interesse), ebenfalls Art. 9 Abs. 5 DS-GVO für besondere Vorschriften der Mitgliedstaaten für hochsensible Daten, z. B. genetische Daten.

sichtlich der Betroffenenrechte auf Transparenz und Korrektur aus verbraucherpolitischer Sicht festzustellen, dass:

- sich Verbraucher_innen oft nicht ausreichend über den Umgang von Unternehmen mit ihren Daten informiert fühlen. So geben etwa nur 16 Prozent der deutschen Teilnehmer_innen an einer EU-weit durchgeführten Befragung an, sich immer ausreichend über die Bedingungen der Datenerfassung und die weitere Verwendung ihrer Daten informiert zu fühlen, wenn sie im Internet gebeten werden, ihre persönlichen Informationen preiszugeben. Insgesamt 41 Prozent sagen hingegen, dass sie sich selten oder nie informiert fühlen, während 38 Prozent diese Frage mit der Aussage „manchmal" (European Commission 2015: 82) beantworten. Dieses Ergebnis sollte nicht überraschen, wenn man bedenkt, dass beispielsweise die Datenschutzbestimmungen von Facebook allein 70.000 Zeichen und damit ungefähr 25 engbedruckte Seiten umfassen (Hansen 2015: 3);
- die Datenschutzerklärungen von Unternehmen, die der Intention des Datenschutzrechts nach dazu beitragen sollten, Verbraucher_innen zu informieren, häufig eher der juristischen Absicherung der Unternehmen dienen und daher in einer Sprache verfasst sind, die für juristische Laien unverständlich ist. So überrascht es wenig, dass 26 Prozent der Verbraucher_innen in einer Befragung angaben, Datenschutzerklärungen nie zu lesen, und 55 Prozent sagten, dass sie diese nur teilweise lesen würden. Als Gründe für die geringe Beachtung der Datenschutzerklärungen gaben 70 Prozent an, dass diese zu lang seien, und 43 Prozent sagten, dass diese unklar formuliert und schwer zu verstehen seien (European Commission 2015: 85 und 89). Ähnliche Werte finden sich auch bei der Frage, ob Verbraucher_innen die AGB lesen. Eine Untersuchung im Auftrag des Verbraucherzentrale Bundesverbands (vzbv) kommt zu dem Ergebnis, dass die Mehrheit der Internetnutzer_innen (53 Prozent) den AGB beim Einkauf im Internet oder beim Installieren einer App immer oder meistens zustimmen, ohne sie wirklich gelesen zu haben. Als der mit Abstand häufigste Grund (72 Prozent) hierfür wird die Länge und Komplexität der AGB genannt (Verbraucherzentrale Bundesverband 2014: 6);
- das Auskunftsrecht zwar grundsätzlich ein wichtiges Recht darstellt. Die Durchsetzung dieses Rechts Verbraucher_innen jedoch vor eine Reihe von Herausforderungen stellt. Denn oft wissen Verbraucher_innen nicht:
  - welche Unternehmen ihre Daten überhaupt verarbeiten;
  - an wen sie sich bei einem Unternehmen konkret wenden sollen, um die Auskunft zu erlangen;
  - wie ein Auskunftsersuchen formuliert sein sollte;
  - wie sie bei Unternehmen nachhaken sollten, wenn eine Antwort ausbleibt.
- die datenschutzrechtlichen Transparenzvorschriften gerade hinsichtlich der Aspekte Vollständigkeit und Wahrheitsgehalt weitgehend abhängig von der Zuverlässigkeit der datenverarbeitenden Stelle sind. Für eine wirksame Umsetzung der Rechte der Betroffenen auf Berichtigung, Löschung und Sperrung von Daten ist jedoch stets eine zuverlässige Informationsgrundlage erforderlich, die gerade bei den „schwarzen Schafen" unter den Datenverarbeitern die Ausnahme sein wird.

Von Unternehmensseite wird hingegen das Festhalten am Verbot mit Erlaubnisvorbehalt kritisiert. Viele Unternehmensvertreter_innen sehen es wegen der Vielzahl von Kommunikationsvorgängen als überholt an. Gefordert wird daher eine Abschwächung, die es zumindest erlaubt, zwischen sensiblen und nichtsensiblen personenbezogenen Daten und Datenverarbeitungsprozessen zu unterscheiden (siehe zusammenfassend Spindler 2014: 104). Hierbei handelt es sich um einen risikobasierten Ansatz, nach dem die Verarbeitung personenbezogener Daten grundsätzlich gestattet wäre und lediglich bei Datenverarbeitungen mit besonders hohem Risiko Verbote und beschränkende Regulierung greifen sollten (BfDI 2015: 28). Das würde nach Ansicht der Befürworter_innen dazu führen, dass sich innovationsfeindliche Nachteile gegenüber anderen Wirtschaftsstandorten außerhalb Europas reduzieren ließen. Auch würden die Markteinstiegsbarrieren für kleinere und mittlere Unternehmen, die nicht über ein umfassendes Compliance-Management verfügen, verringert (ähnlich BfDI 2015: 27 f.). Allerdings ist eine solche Abstufung der Qualität personenbezogener Daten und Datenverarbeitungsprozesse höchst umstritten, und zwei diametral unterschiedliche Lager treffen hier aufeinander (dagegen bspw.: BfDI 2015: 28; dafür bspw: Schneider/Härting 2011: 64 f. m. w. Nachw.).

Der haftungsrechtliche Schutz stellt im Bereich des Verbraucherdatenschutzes ein stumpfes Schwert dar. Grundsätzlich ist beim Schadensersatz zu differenzieren, ob der Ersatz materieller oder immaterieller Schäden begehrt wird. Materielle Schäden sind im deutschen Recht konkrete Vermögenseinbußen, die durch die Rechtsverletzungen erlitten wurden (Gola et al. 2015: § 7 BDSG, Rn. 12). Immaterielle Schäden umfassen hingegen auch solche Schäden, die sich nicht im Vermögen auswirken. Dazu zählen bspw. Schmerzen aufgrund physischer, aber auch psychischer Verletzungen (daher auch als Schmerzensgeld bezeichnet) (siehe ausführlich Oetker MünchKommBGB 2012: § 253, Rn. 9). Bei Verletzungen des Rechts auf informationelle Selbstbestimmung kommt es selten zu konkreten Vermögenseinbußen, bzw. sind sie schwer nachweisbar, sodass dem/der Verletzten häufig nur eine Berufung auf immaterielle Schäden verbleibt. Ein Ersatz immaterieller Schäden ist aber nach der deutschen Rechtsdogmatik ausschließlich in Fällen möglich, bei denen eine schwerwiegende Verletzung des Persönlichkeitsrechts vorliegt und eine Genugtuung auf andere Weise nicht angemessen gewährt werden kann (Gola et al. 2015: § 7, Rn. 19 m. w. Nachw. zur ständigen Rechtsprechung). Bei „normalen" oder geringfügigen Persönlichkeitsrechtsverletzungen scheiden derartige Ansprüche damit grundsätzlich aus. Diese Einschränkungen führen insgesamt dazu, dass zahlreiche Fallgestaltungen aus den Anwendungsbereichen der deutschen Schadensersatzregelungen im Bereich des Verbraucherdatenschutzes herausfallen. Finden die Regelungen hingegen Anwendung, sind die in Deutschland für immaterielle Schäden zugesprochenen Ersatzleistungen in Geld schwer zu beziffern. Im internationalen Vergleich fallen sie zudem gering aus (Spindler 2014: 106 m. w. Nachw.).

In der Konsequenz bedeutet das für den haftungsrechtlichen Schutz, dass der Aufwand und die Kosten, um Kompensation für eine unzulässige Verarbeitung personenbezogener Daten zu erlangen, oft in keinem Verhältnis zu einem

möglichen Ertrag stehen. Daher stellen die Schadensersatzansprüche für die Betroffenen keinen ausreichenden Anreiz dar, gegen Schädiger vorzugehen – und somit stellen sie auch keinen ausreichenden Negativanreiz für Unternehmen dar, Rechtsverstöße proaktiv zu unterbinden.

Aus dem Dargestellten lässt sich demnach zusammenfassend sagen, dass Verbraucher_innen zwar gemäß des derzeitigen Datenschutzrechts theoretisch über weitgehende Transparenz- und Kontrollrechte verfügen. Allerdings führt dies in der Praxis nicht dazu, dass sie ihre Rechte auch wirklich ausüben:

- Die Verbraucher_innen fühlen sich in der Praxis häufig nicht ausreichend über Datenverarbeitungsvorgänge informiert.
- Datenschutzerklärungen werden häufig nicht gelesen, da sie in der Regel zu lang, sprachlich für Laien unverständlich und komplex formuliert sind.
- Das Auskunftsrecht ist in der Praxis zu aufwändig.
- Die Tatsache, dass nach dem deutschen Haftungsrecht im Wesentlichen immaterielle und damit schwer quantifizierbare Schäden geltend gemacht werden können, führt dazu, dass die abschreckende und Unternehmen disziplinierende Wirkung des Haftungsrechts ausbleibt.

Die Analyse wirft zudem grundlegende Fragen etwa über die Weiterentwicklung von Einwilligungen auf. Auf der einen Seite stehen Befürworter_innen einer Abschwächung des Einwilligungserfordernisses, die einen risikobasierten Ansatz einfordern. Auf der anderen Seite stehen die Verfechter_innen dieses Prinzips, die sich überdies für eine Weiterentwicklung stark machen.

In der Konsequenz bedeutet das: Während die Durchsetzung des Datenschutzes durch die Betroffenen zwar eine wesentliche Säule für den Verbraucherdatenschutz darstellen sollte, zeigt sich in der Praxis, dass sie derzeit nur begrenzt trägt. Daher muss auf der einen Seite über neue Möglichkeiten nachgedacht werden, den Selbstdatenschutz zu verbessern. Auf der anderen Seite muss die Rechtsdurchsetzung auch durch andere Instrumente als durch die Betroffenen selbst gewährleistet werden.

Die voraussichtlichen Auswirkungen der DS-GVO auf die Rechtsdurchsetzungsmöglichkeiten der Verbraucher_innen lassen sowohl Verbesserungen als auch Verschlechterungen der gegenwärtigen Rechtslage erwarten. Die finale Fassung der DS-GVO enthält zum einen leichte Verbesserungen bei den Auskunftsrechten – etwa hinsichtlich der Herausgabe einer Kopie der Daten oder beim Kopplungsverbots. Andererseits gibt es jedoch eine Vielzahl von Interessenabwägungsklauseln (etwa bei der Zweckbindung und der Einwilligung), die zulasten der Rechtssicherheit gehen. Auch sehen die Regelungen Möglichkeiten einer Öffnung für abweichende Bestimmungen in Mitgliedstaaten vor. Diese führen – entgegen dem ursprünglichen Ziel der Verordnung – dazu, dass die Verbraucher_innen keine einheitlichen Maßstäbe in der EU vorfinden werden. Insgesamt betrachtet wird die DS-GVO die Rechtsdurchsetzungsmöglichkeiten der Verbraucher_innen im Vergleich zum Status quo daher nicht wesentlich verbessern. Letztlich wird die Gesamtbewertung von der konkreten Auslegungspraxis abhängen.

Tabelle 1
**Ergebnisse der Stärken- und Schwächenanalyse zu den Betroffenenrechten**

| | Zusammenfassung | Gesamtbewertung |
|---|---|---|
| **Stärken- und Schwächenanalyse** | Auf der einen Seite existiert ein umfassendes System von Betroffenenrechten. Auf der anderen Seite führt dieses System in der Praxis nicht dazu, dass Verbraucher_innen ausreichend informiert sind und ihre Rechte selbst durchsetzen können. Es existiert demnach eine gravierende Diskrepanz zwischen den Rechten und der gelebten Praxis.<br>Überdies greift der haftungsrechtliche Schutz nicht, da der Aufwand und die Kosten, eine Kompensation zu erhalten, in keinem Verhältnis zu einem möglichen Ertrag stehen. |  |
| **Voraussichtliche Auswirkungen der DS-GVO** | Die DS-GVO wird die Betroffenenrechte nicht spürbar verbessern. Es wird wegen der zahlreichen Interessenabwägungs- und Öffnungsklauseln stark auf die konkrete Auslegung und nationale Ausgestaltung ankommen. |  |

Quelle: eigene Darstellung.

## 2.2 RECHTSDURCHSETZUNG DURCH DIE STAATLICHE AUFSICHT

Die staatliche Aufsicht stellt die zweite wesentliche Säule der Rechtsdurchsetzung im Verbraucherdatenschutz in Deutschland dar. Sie wird im Folgenden dargestellt. Daran anschließend werden dann die voraussichtlichen Implikationen der DS-GVO auf diese Säule untersucht, ehe die Stärken und Schwächen diskutiert werden.

### 2.2.1 AUFGABEN UND BEFUGNISSE DER STAATLICHEN AUFSICHT IM VERBRAUCHER-DATENSCHUTZ

In der staatlichen Aufsicht ist insbesondere die Rolle der unabhängigen Datenschutzaufsichtsbehörden hervorzuheben. Nach § 38 BDSG ist jeweils eine der 16 Landesdatenschutzbehörden zuständig, die Einhaltung der Datenschutzgesetze bei Unternehmen zu kontrollieren. Welche der Landesdatenschutzbehörden konkret für ein Unternehmen zuständig ist, richtet sich grundsätzlich nach dem Sitz des Unternehmens.[19] Für öffentliche Stellen ist der/die jeweilige Landesdatenschutzbeauftragte zuständig. Die Bundesverwaltung (z. B. Ministerien und Bundesämter), bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, öffentlich-rechtliche Wettbewerbsunternehmen des Bundes, in Verwaltungsangelegenheiten tätige Gerichte des Bundes, Telekommunikations- und Postunternehmen sowie private Unternehmen, die in den Anwendungsbereich des Sicherheitsüberprüfungsgesetzes (SÜG) fallen, unterliegen der Zuständigkeit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).[20]

Um die zugewiesenen Aufgaben ausüben zu können, stellt das Gesetz den Behörden vielfältige Instrumente zur Verfügung. Das sind insbesondere:[21]

- Auskunfts-, Zutritts- und Einsichtsrechte gegenüber verantwortlichen Stellen (§ 38 Abs. 3 und Abs. 4 BDSG);
- Verhängung von Bußgeldern (§ 43 BDSG);
- Anordnung der Beseitigung festgestellter Datenschutzverstöße und bei schwerwiegenden Verstößen die Untersagung einzelner Verfahren (§ 38 Abs. 5 S. 1 und S. 2 BDSG);
- Abberufung des Datenschutzbeauftragten (§ 38 Abs. 5 S. 3);
- Unterrichtung von Betroffenen über Verstöße (§ 38 Abs. 1 S. 5 BDSG);
- Anzeige von Verstößen bei anderen für die Ahndung und Verfolgung zuständigen Stellen (§ 38 Abs. 1 S. 5 BDSG);
- Unterrichtung der Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen bei schwerwiegenden Verstößen (§ 38 Abs. 1 S. 5 BDSG).

In der Ausübung dieser Instrumente ist wichtig, dass ein konkreter Anlass für die Überprüfung eines Unternehmens durch die Aufsichtsbehörde nicht erforderlich ist (Hauschka/Neundorf 2010: § 30, Rn. 10). Überdies sind nach § 4d Abs. 1 BDSG automatisierte Verarbeitungen personenbezogener Daten durch Unternehmen vor ihrer Inbetriebnahme der jeweils zuständigen Aufsichtsbehörde zu melden. Diese Pflicht entfällt allerdings, wenn das Unternehmen einen betrieblichen Datenschutzbeauftragten bestellt hat (§ 4d Abs. 2 BDSG).[22]

### 2.2.2 ABSEHBARE AUSWIRKUNGEN DER DS-GVO AUF DIE ROLLE DER STAATLICHEN AUFSICHT

In der DS-GVO finden sich Änderungen, die konkrete Auswirkungen auf die Sanktionsmittel der datenschutzrechtlichen Aufsichtsbehörden haben. So sieht die DS-GVO vor, dass die zuständigen Aufsichtsbehörden in Abhängigkeit der verletzten Pflichten Geldstrafen bis zu 20 Mio. Euro oder im Fall eines Unternehmens bis zu vier Prozent des weltweiten Jahresumsatzes verhängen können (Art. 79 Abs. 3 DS-GVO). Gegenüber der aktuellen Rechtslage würde dies eine deutliche Erweiterung der sanktionsrechtlichen Mittel der Aufsichtsbehörden bedeuten. Denn diese können derzeit zwar Bußgelder in einer Höhe verhängen, die den wirtschaftlichen Vorteil aus einer Rechtsverletzung überschreitet. Die im geltenden Recht genannten Regelhöchstsätze von 300.000 Euro – in vielen Fällen sogar nur 50.000 Euro – sind jedoch gerade für global operierende Unternehmen vernachlässigbar und daher mit nur einer geringen abschreckenden Wirkung verbunden.

Zudem sehen die Vorschläge vor, die staatliche Rechtsdurchsetzung gerade bei grenzüberschreitend tätigen Unternehmen zu verbessern. Erstens stellt hierbei die Einführung des Marktortprinzips (siehe Abschnitt 1.3) eine fundamentale Verbesserung dar, da hierdurch überhaupt erst die Anwendbarkeit des europäischen Datenschutzrechts für zahlreiche global tätige Unternehmen sichergestellt wird. Zweitens sollen auch die Zuständigkeiten der und die Zusammenarbeit zwischen den nationalen Behörden insgesamt neu geregelt und damit verbessert werden. So sieht die DS-GVO eine „lead supervisory authority" vor, die unter festgelegten Bedingungen mit den anderen Aufsichtsbehörden zusammenarbeiten muss (Art. 51a, 54a DS-GVO). Die DS-GVO enthält vor allem in Art. 54a die Pflicht zur gegenseitigen Kooperation der „lead supervisory authority" mit anderen betroffenen Aufsichtsbehörden, um einen Konsens bei Aufsichtsmaßnahmen zu erzielen. Kann ein solcher Konsens aufgrund einer innerhalb von vier Wochen erfolgenden Einwendung einer Aufsichtsbehörde nicht erreicht werden, sieht Art. 54a Nr. 3 DS-GVO das Eingreifen des sogenannten Kohärenzmechanismus nach Art. 57 DS-GVO vor. In diesen Fällen eines Dissenses kann der Europäische Datenschutzausschuss nach Art. 58a Nr. 1 DS-GVO eine bindende Entscheidung fällen. Das gilt auch, wenn Zuständigkeitskonflikte auftreten sollten. In dringenden Fällen sieht Art. 61 DS-GVO überdies eine Eilkompetenz der Aufsichtsbehörde, aber auch Eilentscheidungen des Europäischen Datenschutzausschusses vor. Der Kommissionsentwurf beinhaltete an dieser Stelle noch einen „One-Stop-Shop". Zwar finden sich Grundzüge dieses Ansatzes weiterhin in den

19 § 38 Abs. 6 BDSG; siehe auch den Überblick über die Aufsichtsbehörden bei Erbs et al. (2015: § 38 BDSG, Rn. 1); Ausnahme: für Post- und Telekommunikationsunternehmen.

20 Siehe BfDI, https://www.bfdi.bund.de/SharedDocs/Publikationen/ZustaendigkeitBfDFuerEingaben.html (12.7.2015).

21 Siehe auch den Überblick bei Hauschka/Neundorf (2010: § 30, Rn. 10).

22 Ausführlich zum Datenschutzbeauftragen s. u. 2.4

Regelungen – allerdings ist das Verfahren nun wesentlich komplizierter ausgestaltet, als es ursprünglich vorgesehen war.

Drittens sieht die finale Fassung des Art. 66 Abs. 1 DS-GVO nunmehr Verbesserungen vor, insofern dem Europäischen Datenschutzausschuss recht detailliert die Aufgabe überantwortet wird, Richtlinien und Best Practices herauszugeben. Allerdings enthält die Verordnung nichts über deren Verbindlichkeit. Insoweit ähnelt die Aufgabenverteilung nunmehr der früheren Art.-29-Gruppe, allerdings mit dem Unterschied, dass der Datenschutzausschuss in Konfliktfällen eine Entscheidungsbefugnis erhält.

### 2.2.3 STÄRKEN- UND SCHWÄCHENANALYSE

Die Datenschutzaufsichtsbehörden nehmen grundsätzlich eine zentrale Funktion in der Durchsetzung des Datenschutzrechts wahr. Allerdings werden eine Reihe von Schwächen bemängelt und Kritikpunkte an der Aufsichtspraxis geäußert:

- So wird eine unzureichende personelle und finanzielle Ausstattung kritisiert.[23] Während etwa das Personal des Bundesamts für Sicherheit in der Informationstechnologie (BSI) um ein Drittel auf 765 Stellen aufgestockt werden soll, ist eine Erhöhung der aktuell 85 Stellen bei der Bundesdatenschutzbeauftragten nicht vorgesehen. Die personelle Unterversorgung wird auch auf Landesebene deutlich. So stehen der Hamburger Aufsichtsbehörde, die letztlich über große Auskunfteien wie Bürgel und global operierende Unternehmen wie Google zu wachen hat, lediglich 6,25 Personen zur Verfügung (Schulzki-Haddouti 2015: 77).
- Diese personelle Unterausstattung bei den Behörden führe u. a. dazu, dass diese kaum mehr in der Lage seien, neben den anlassbedingten Kontrollen, die auf konkrete Beschwerden zurückgehen, essenzielle anlasslose Kontrollen durchzuführen (Schulzki-Haddouti 2015: 77).
- Auch die derzeitigen Sanktionsmittel und hierbei insbesondere die geringe Höhe der Bußgelder werden von einigen als unzureichend angesehen (Friedrich-Ebert-Stiftung 2015: 3).
- Zudem wird von einigen argumentiert, die staatliche Aufsicht erfolge heute eher „zufällig" und gehorche der Logik einer „Aufmerksamkeitsökonomie". Von einem strategischen, risikobasierten Vorgehen könne nicht gesprochen werden (Friedrich-Ebert-Stiftung 2015: 3).
- Zu guter Letzt wird bemängelt, dass die Aufsichtsbehörden im deutschen föderalen System das Recht, trotz des Koordinierungsmechanismus über den Düsseldorfer Kreis, uneinheitlich auslegen. Hierdurch würden Rechtsunsicherheit und ungleiche Maßstäbe entstehen (Friedrich-Ebert-Stiftung 2015: 3). Da die Behörden überdies klare, rechtsverbindliche Entscheidungen scheuen würden, die vor Gericht angefochten werden könnten, mangele es an Rechtsprechung (Schulzki-Haddouti 2015: 77).

Aus dem Dargestellten folgt daher, dass die staatliche Aufsicht zwar grundsätzlich eine wesentliche Säule für die Rechtsdurchsetzung im Verbraucherdatenschutz darstellt. Allerdings leidet die Effektivität dieses Instruments darunter, dass:

- die staatliche Aufsicht personell und finanziell nicht ausreichend ausgestattet ist;
- von den Bußgelder, die sie verhängen kann, keine ausreichende abschreckende Wirkung ausgeht, da diese zu gering sind;
- die Aufsicht – wie von einigen kritisiert – nicht systematisch genug erfolgt und das Recht in Deutschland uneinheitlich auslegt.

Insgesamt lässt sich festhalten, dass durch die Erhöhung des Bußgeldrahmens und die Einführung des Marktortprinzips die DS-GVO wesentliche Verbesserungen mit sich bringt. Hinsichtlich einer verbesserten Zusammenarbeit zwischen den mitgliedstaatlichen Behörden sind die Instrumente „lead supervisory authority" und „Europäischer Datenschutzaus-

23 Siehe etwa BfDI (2015: 18.); Friedrich-Ebert-Stiftung (2015: ); siehe ferner Schulzki-Haddouti (2015: 76 ff.).

Tabelle 2
**Ergebnisse der Stärken- und Schwächenanalyse zur staatlichen Aufsicht**

| | Zusammenfassung | Gesamtbewertung |
|---|---|---|
| **Stärken- und Schwächenanalyse** | Die staatliche Aufsicht stellt in Deutschland eine wesentliche Säule in der Rechtsdurchsetzung dar. Allerdings leidet sie an einer personellen und finanziellen Unterausstattung, und die Bußgeldrahmen sind nicht ausreichend hoch. Auch wird angemahnt, dass das föderale System der Rechtsauslegung zu unterschiedlichen Aufsichtsniveaus führt. |  |
| **Voraussichtliche Auswirkungen der DS-GVO** | Die DS-GVO wird die Wirksamkeit der staatlichen Aufsicht insbesondere durch die Erhöhung der Bußgeldrahmen sowie die Einführung des Marktortprinzips verbessern. Hinsichtlich der Verbesserung der grenzüberschreitenden Rechtsdurchsetzung wird es jedoch auf die konkrete Anwendung der Koordinierungsmechanismen ankommen. |  |

Quelle: eigene Darstellung.

schuss" zwar grundsätzlich sinnvoll und begrüßenswert. Die Zukunft muss aber zeigen, ob die vorgesehenen Verfahrensregeln ein effektives Arbeiten ermöglichen, insbesondere in Konfliktfällen. Auch ist zu kritisieren, dass der Datenschutzausschuss im Wesentlichen nur eine beratende und überprüfende Funktion hat, wenn er etwa Richtlinien herausgibt. Die Verordnung sagt hierbei nichts über deren Verbindlichkeit.

## 2.3 RECHTSDURCHSETZUNG DURCH ANERKANNTE VERBRAUCHERVERBÄNDE

Die Durchsetzung von Verbraucherrechten durch anerkannte Verbraucherverbände stellt eine dritte Säule in der Datenschutzrechtsdurchsetzung dar. Diese wird im Folgenden erläutert und problematisiert.

### 2.3.1 DIE ROLLE ANERKANNTER VERBRAUCHERVERBÄNDE FÜR DIE RECHTSDURCHSETZUNG

Da Verbraucher_innen häufig aufgrund fehlender Rechtskenntnisse, zu hoher Transaktionskosten, einem schlechten Kosten-/Nutzenverhältnis oder nicht ausreichender finanzieller Mittel von einer individuellen Rechtsdurchsetzung absehen, hat der Gesetzgeber mit dem Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (UKlaG) Klagemöglichkeiten für anerkannte Verbraucherverbände geschaffen. Das Gesetz ermöglicht den Verbänden, zur Wahrnehmung der Verbraucherinteressen Unterlassungsansprüche bei unzulässigen Allgemeinen Geschäftsbedingungen (§ 1 UKlaG) sowie bei Verstößen gegen Verbraucherschutzgesetze (§ 2 UKlaG) oder gegen Vorschriften des Gesetzes gegen Unlauteren Wettbewerb (UWG) geltend zu machen.

Was die Anwendbarkeit des Unterlassungsanspruchs von Verbänden bei unzulässiger Verwendung Allgemeiner Geschäftsbedingungen gem. § 1 UklaG betrifft, war für den Bereich des Datenschutzes insbesondere die Frage umstritten, wann bei einer Datenschutzerklärung eines Anbieters von Allgemeinen Geschäftsbedingungen ausgegangen werden kann und damit der Anwendungsbereich der Regelung eröffnet ist. Hierbei wurde für gewöhnlich argumentiert, dass dies grundsätzlich nur dann zutrifft, wenn die in den Datenschutzbestimmungen enthaltenen Formulierungen einen solchen regelnden Charakter aufweisen, der ein konkretes Vertragsverhältnis nahelegt.[24] Es wurde daher zumeist argumentiert, dass Datenschutzbestimmungen lediglich einen informativen bzw. deklaratorischen Charakter aufweisen, weswegen aus dogmatischer Sicht ein Unterlassungsanspruch der Verbände in diesen Fällen ausscheidet (zutreffend Nietsch 2014: 275 f.). Gleichwohl liegen entgegen dieser Auffassung gerichtliche Urteile gegen Unternehmen wie Facebook, Apple und Google vor, die nach Klage des Verbraucherzentrale Bundesverbands (Verbraucherzentrale Bundesverband 2013) die Verwendung gewisser Klauseln in Datenschutzbestimmungen der Anbieter untersagt haben.[25] Mangels höchstgerichtlicher Entscheidung verbleiben allerdings die dargestellten Unsicherheiten hinsichtlich der Anwendbarkeit des § 1 UKlaG grundsätzlich bestehen.

Auch § 2 UKlaG in der Fassung vom 27.8.2002 weist noch erhebliche Probleme hinsichtlich der Anwendbarkeit bei Datenschutzverstößen auf. Dies resultiert aus dem Umstand, dass Datenschutzregelungen nicht vorrangig – wie von dem Gesetz gefordert – dem Schutz von Verbraucher_innen, sondern vielmehr allgemein dem natürlicher Personen dienen (Elbrecht/Schröder 2015: 363; Nietsch 2014: 277). Dementsprechend haben die mit dieser Frage befassten Gerichte in der Vergangenheit überwiegend eine Anwendbarkeit von § 2 UKlaG in Bezug auf die Datenschutzgesetze abgelehnt.[26]

Ähnlich stellt sich die Situation in Bezug auf die wettbewerbsrechtlichen Regelungen nach § 8 Abs. 3 Nr. 3 UWG dar. Diese Vorschrift ermöglicht ein Vorgehen der Verbände auf Basis der Öffnungsklausel des § 4 Nr. 11 UWG. Die verlangt jedoch, dass ein Verstoß gegen eine gesetzliche Vorschrift vorliegt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer_innen das Marktverhalten zu regeln. Ob dieses Erfordernis bei datenschutzrechtlichen Regelungen erfüllt ist, ist in der Rechtsprechung und Literatur stark umstritten (siehe ausführlich dazu Elbrecht/Schröder 2015: 363 f.). Auch hier fehlt es bislang an höchstrichterlicher Rechtsprechung. Insofern ist auch diese Anspruchsgrundlage bedingt durch die Rechtsunsicherheiten nur von geringem Nutzen für die Geltendmachung von Unterlassungsansprüchen durch die Verbände.

Vor diesem Hintergrund und den dargestellten Defiziten bei der flächendeckenden Kontrolle durch die Datenschutzaufsichtsbehörden[27] ist die jüngst verabschiedete Änderung des UKlaG zu sehen.[28] Nach § 2 Abs. 2 Nr. 11 UKlaG sind demnach datenschutzrechtliche Vorschriften, die die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines/einer Verbraucher_in durch Unternehmen zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens von Auskunfteien, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken regeln, nunmehr als Verbraucherschutzgesetze im Sinne des § 2 Absatz 1 UKlaG[29] anzusehen. Ausgenommen sind allerdings Datenerhebungen und -verarbeitungen, die zur Anbahnung und Verarbeitung von Verträgen sowie Erfüllung gesetzlicher Pflichten dienen (§ 2 Abs. 2 Nr. 11 S. 3 UKlaG). Somit könnten nach Inkrafttreten des Gesetzes anerkannte Verbraucherverbände gegen datenschutzrechtliche Verstöße seitens Unternehmen vorgehen, sofern die Kollektivinteressen von Verbraucher_innen betroffen sind, also der Verstoß in seinem Gewicht und seiner Bedeutung über den Einzelfall hinausgeht und eine generelle Klärung geboten scheint.[30]

---

**24** BGH NJW 2005, 1645; NJW 1987, 1634; NJW 1996, 2574; siehe ausführlich dazu Nietsch (2014: 273 ff. m. w. Nachw.).

**25** LG Berlin, K&R 2014, 56; CR 2013, 402; CR 2012, 270; Elbrecht/Schröder (2015: 363); kritisch Nietsch (2014: 272).

**26** Siehe ausführlich dazu die Zusammenfassung bei Elbrecht/Schröder (2015: 363).

**27** Siehe oben Abschnitt 2.2.3

**28** BT-Drucks. 18/4631.

**29** So BT-Drucks. 18/463, S. 2.

**30** Micklitz MünchKommZPO 2013: § 2 UKlaG, Rn. 15 ff., insb. Rn. 16 unter vergleichendem Verweis auf BT-Drucks. 14/2658, S. 53.

### 2.3.2 ABSEHBARE AUSWIRKUNGEN DER DS-GVO AUF DIE RECHTSDURCHSETZUNG DURCH ANERKANNTE VERBRAUCHERVERBÄNDE

Eine Klagebefugnis für Verbände ist auch in der DS-GVO zu finden (Art. 76 DS-GVO). Flankierend hierzu ist vorgesehen, dass Verbände, die im öffentlichen Interesse handeln, das Recht erhalten sollen, im Namen einer oder mehrerer betroffener Personen Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde zu erheben (Art. 73 Abs. 2 DS-GVO). Darüber hinaus sollen solche Verbände auch ganz unabhängig von der Beschwerde einer betroffenen Person in eigenem Namen Beschwerde einlegen und Klage erheben können, wenn sie der Ansicht sind, dass ein Verstoß gegen die DS-GVO[31] vorliegt (Art. 76 Abs. 2 iVm Art. 75 DS-GVO), und sofern der Mitgliedstaat dies vorsieht (Art. 76 Abs. 2 DS-GVO, Erwägungsgrund 116 DS-GVO). Beschränkungen wie das deutsche UKlaG kennt die DS-GVO indes für die Verbandsklage nicht. An dieser ausdrücklichen Regelung zur Beschwerde- und Klagebefugnis ist der Willen des europäischen Gesetzgebers erkennbar, die Position von Interessenvertretungen Betroffener zu stärken.[32]

Allerdings gibt Erwägungsgrund 116 DS-GVO den Mitgliedstaaten auch vor, dass sich das Verbandsklagerecht nicht – unabhängig von der Beauftragung durch eine Person – auf Schadensersatz erstrecken darf.

### 2.3.3 STÄRKEN- UND SCHWÄCHENANALYSE

Mit der Änderung des UKLaG unternimmt die Bundesregierung einen Versuch, die Rechtsdurchsetzung im Verbraucherdatenschutz durch anerkannte Verbraucherverbände spürbar zu verbessern. Allerdings werden die oben genannten Ausnahmen die Verbraucherverbände vor praktische Probleme stellen. So existieren insbesondere die folgenden Schwachstellen:

- Für Fälle, bei denen das Kollektivinteresse nicht vorliegt, es aber zu schwerwiegenden Rechtsverletzungen kommt, bleiben die dargestellten Rechtsdurchsetzungsprobleme bestehen (Weidlich-Flatten 2014: 197).
- Verbände könnten hinsichtlich der Beweislast Schwierigkeiten bekommen. Das gilt gerade in Bezug auf das Tatbestandsmerkmal der „kommerziellen Zwecke". Denn häufig werden die Daten der Verbraucher_innen vorrangig im Zusammenhang mit der Erfüllung eines Vertrags erhoben und verarbeitet. Der Nachweis der darüber hinausgehenden Verarbeitung zu kommerziellen Zwecken könnte in der Praxis Probleme bereiten (Elbrecht/Schröder 2015: 365).

Kritisch angemerkt wird außerdem, dass die Verbraucherverbände über ausreichend personelle und finanzielle Ressourcen verfügen müssen, um diese neuen Rechte auch anwenden zu können (Friedrich-Ebert-Stiftung 2015: 3). In diesem Zusammenhang wird immer wieder die Schaffung einer Rechtsgrundlage für die Abschöpfung von Unrechtsgewinnen bei Datenschutzverstößen gefordert. Eine solche Möglichkeit besteht laut geltendem Recht grundsätzlich nach § 10 UWG. Allerdings fließen die Unrechtsgewinne in den Bundeshaushalt, sodass die Verbraucherverbände über keine ausreichenden Anreize verfügen, zu klagen. Deshalb ist etwa daran zu denken, dass die Abschöpfung von Gewinnen künftig in eine Stiftung

---

**31** Der Vorschlag der Kommission spricht von „Verbänden, die sich den Schutz der Rechte und Interessen von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten zum Ziel gesetzt haben".

**32** Demensprechend wird dies auch vom vzbv begrüßt, siehe Änderungsvorschläge des Verbraucherzentrale Bundesverband (2013: 24 f.); die Kritik an der Formulierung des Art. 73 DS-GVO, wodurch Verbraucherverbände nicht klar erfasst seien, dürfte sich mit den Vorschlägen des Parlaments und des Rates erübrigt haben.

Tabelle 3
**Ergebnisse der Stärken- und Schwächenanalyse zu den anerkannten Verbraucherverbänden**

| | Zusammenfassung | Gesamtbewertung |
|---|---|---|
| **Stärken- und Schwächenanalyse** | Bislang spielen anerkannte Verbraucherverbände lediglich eine marginale Rolle in der kollektiven Rechtsdurchsetzung im Verbraucherdatenschutz, da die rechtlichen Grundlagen umstritten sind bzw. nicht vorliegen. Der Gesetzgeber hat hierauf mit Änderungen im UKlaG reagiert. Diese sollten zu einer spürbaren Verbesserung führen. Allerdings ist hierfür eine ausreichende Finanzierung der Rechtsdurchsetzungsaktivitäten bei den Verbraucherorganisationen notwendig. |  |
| **Voraussichtliche Auswirkungen der DS-GVO** | Von der DS-GVO gehen keine Gefahren für dieses Instrument aus. Im Gegenteil, der Entwurf sieht sogar eine Aufwertung vor (Beschwerde- und Klagebefugnisse). |  |

Quelle: eigene Darstellung.

einfließt, die dem Verbraucherschutz dient und mittelbar auch Verbraucherverbände finanziell unterstützen könnte.

Aus dem Dargestellten folgt, dass durch die Änderung im UKlaG die kollektive Rechtsdurchsetzung verbessert und überdies die bislang sehr geringe Zahl von gerichtlichen Verfahren und Urteilen erhöht werden könnte. Eine solche Erhöhung wäre nicht nur für die unmittelbare Rechtsdurchsetzung wichtig, sondern würde auch zu einer Verbesserung der Rechtssicherheit führen und letztlich auch die Rechtsfortentwicklung fördern. Für den Erfolg wird es aber darauf ankommen, dass den Verbraucherverbänden für die Geltendmachung der Ansprüche nach dem UKlaG auch ausreichend personelle und finanzielle Mittel zur Verfügung stehen.

Von der DS-GVO gehen keine absehbaren Gefahren für dieses Rechtsdurchsetzungsinstrument aus. Im Gegenteil sieht der Entwurf sogar eine Aufwertung der Rolle von Verbraucherorganisationen vor, insofern diese sowohl Beschwerde- wie auch Klagebefugnisse erhalten sollen.

## 2.4 RECHTSDURCHSETZUNG DURCH DIE BETRIEBLICHEN DATENSCHUTZBEAUFTRAGTEN

Neben der Fremdkontrolle durch die Datenschutzaufsichtsbehörden spielt im deutschen Datenschutzsystem bei der Rechtsdurchsetzung die Selbstkontrolle der Unternehmen eine wichtige Rolle. Hierfür ist der betriebliche Datenschutzbeauftrage von zentraler Bedeutung (§ 4f BDSG).

### 2.4.1 AUFGABEN UND BEFUGNISSE DER BETRIEBLICHEN DATENSCHUTZBEAUFTRAGTEN

Das Datenschutzrecht sieht vor, dass Unternehmen, die personenbezogene Daten automatisiert verarbeiten und mehr als neun Personen mit der Verarbeitung dieser Daten beschäftigen, einen betrieblichen Datenschutzbeauftragten bestellen müssen (§ 4f Abs. 1 S. 1, 4 BDSG). Der Beauftragte muss über die erforderliche Sachkunde verfügen (§ 4f Abs. 2 BDSG) und hat ab dem Zeitpunkt der Bestellung auf die Einhaltung der Datenschutzgesetze in der jeweiligen Institution hinzuwirken (§ 4g Abs. 1 BDSG). Bei besonderen Risiken für die Rechte von Betroffenen führt er vor Beginn der entsprechenden Datenverarbeitung eine Vorabkontrolle der Datenverarbeitungsprozesse durch (§ 4d Abs. 5, 6 BDSG). Er ist in der Ausübung seiner Tätigkeit weisungsfrei, und ihm kommen innerhalb der verantwortlichen Stelle Überwachungskompetenzen zu (§ 4g Abs. 1 Nr. 1 BDSG). Damit er seine Tätigkeit tatsächlich ausüben kann, ist er von der Geschäftsführung mit den dafür erforderlichen Informationen (§ 4g Abs. 1 Nr. 1, Abs. 2 BDSG) sowie finanziellen und sachlichen Mitteln auszustatten (§ 4f Abs. 5 BDSG). Der Beauftragte genießt einen besonderen Kündigungsschutz. Seitens der verantwortlichen Stelle kann ihm ausschließlich aus wichtigem Grund gekündigt werden.

Auch wenn diese Regelungen eine recht starke Position in der jeweiligen Institution garantieren, bleiben die Kompetenzen des betrieblichen Datenschutzbeauftragten doch darauf beschränkt, auf die Einhaltung des Datenschutzes hinzuwirken. Dementsprechend kann er keine Maßnahmen gegen den Willen der Geschäftsführung durchsetzen, und die Geschäftsführung ist auch nicht an das Urteil des Datenschutzbeauftragten gebunden (Gola et al. 2015: § 4g, Rn. 2). Dennoch kann er in seiner Rolle dazu beitragen, die abstrakten Datenschutzgesetze hinsichtlich der konkreten Anforderungen des jeweiligen Unternehmens zu präzisieren. Er kann in diesem Rahmen der Geschäftsführung bspw. Ratschläge geben, welche technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten erforderlich sind. Er ist außerdem in der Praxis häufig zentraler Ansprechpartner für die Auskunftsersuche der Betroffenen.

Tabelle 4
**Ergebnisse der Stärken- und Schwächenanalyse zu den betrieblichen Datenschutzbeauftragten**

| | Zusammenfassung | Gesamtbewertung |
|---|---|---|
| **Stärken- und Schwächenanalyse** | Grundsätzlich nehmen die betrieblichen Datenschutzbeauftragten eine wichtige Funktion in der Durchsetzung des Datenschutzes ein. Allerdings wird von einigen kritisiert, dass ihre Rolle noch stärker sein und ihr Beitrag zur Datensparsamkeit größer ausfallen könnte. |  |
| **Voraussichtliche Auswirkungen der DS-GVO** | Von der DS-GVO geht keine Gefahr für das System der Datenschutzbeauftragten aus. Allerdings können nationale Sonderregelungen dem Ziel entgegenstehen, ein EU-weit einheitliches Durchsetzungsregime zu etablieren. |  |

Quelle: eigene Darstellung.

### 2.4.2 ABSEHBARE AUSWIRKUNGEN DER DS-GVO AUF DIE ROLLE DER BETRIEBLICHEN DATENSCHUTZBEAUFTRAGTEN

Hinsichtlich der DS-GVO ist festzuhalten, dass die finale Fassung entgegen der Vorschläge des Parlaments und erst recht des Rates zu einer zwingenden Bestellung eines Datenschutzbeauftragten zurückgekehrt ist (Art. 35 Abs. 1); eine Abhängigkeit von einer genau definierten Unternehmensgröße oder Anzahl Betroffener ist gerade nicht mehr vorgesehen. Demgegenüber greift die Pflicht zur Bestellung eines Datenschutzbeauftragten jetzt immer dann ein, wenn:

*„(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and data relating to criminal convictions and offences referred to in Article 9a“*

Damit bleibt es im Prinzip dabei, dass bei einer großen Zahl Betroffener oder bei einer regelmäßigen und systematischen Überwachung die Bestellung von Datenschutzbeauftragen erforderlich ist. Wann dies allerdings konkret der Fall ist, lässt sich der Verordnung nicht mehr entnehmen.
Darüber hinaus bleibt es den Mitgliedstaaten nach Art. 35 Abs. 4 möglich, Pflichten zur Bestellung von Datenschutzbeauftragten auch unterhalb dieser Schwellen einzuführen bzw. beizubehalten. Für die Rechtslage in Deutschland ergeben sich folglich keine zwingenden Veränderungen. Durch die Möglichkeit abweichender Regelungen auf nationaler Ebene kommt es jedoch zu Einschnitten beim eigentlich mit der DS-GVO beabsichtigten Level-Playing-Fields hinsichtlich des Schutzniveaus innerhalb der EU.

### 2.4.3 STÄRKEN- UND SCHWÄCHENANALYSE

Die betrieblichen Datenschutzbeauftragen stellen grundsätzlich eine wichtige Säule im deutschen System der Rechtsdurchsetzung im Bereich des Datenschutzes dar. Über dieses Instrument wird sichergestellt, dass die Geschäftsleitung für den Datenschutz sensibilisiert wird und die Empfehlungen bei ihren Entscheidungen berücksichtigen kann. Allerdings wird von einigen bemängelt, die Rolle der Datenschutzbeauftragten könnte noch größer sein, sodass diese ihre jeweiligen Geschäftsführungen noch stärker als bislang zu einem datensparsamen Verhalten anregen könnten (siehe hierzu auch die Ausführungen zur Rolle der Ko-Regulierung im nächsten Abschnitt).

Die DS-GVO wird die Stellung der Datenschutzbeauftragten – entgegen der Befürchtungen im Verlauf der Verhandlungen – nicht abschwächen. Allerdings können nationale Sonderregelungen dem Ziel entgegenstehen, ein EU-weit einheitliches Durchsetzungsregime zu etablieren.

## 2.5 RECHTSDURCHSETZUNG IM WEGE DER KO-REGULIERUNG[33]

Die Informationsgesellschaft stellt klassische Regulierungsansätze vor ganz spezifische Herausforderungen. Das hat vor allem damit zu tun, dass die Informationsgesellschaft Charakteristika aufweist, die sich mit „herkömmlichen Mitteln“ nationaler staatlicher Regulierung nur schwer fassen lassen. Die hohe Innovationsgeschwindigkeit ist dabei ein wichtiger Faktor. Mit Rechtssetzungszyklen von drei bis vier Jahren auf nationaler und vier bis sechs Jahren auf EU-Ebene läuft die Rechtsetzung Gefahr, den Entwicklungen permanent hinterherzulaufen. Zum anderen sind hier grenzüberschreitend angebotene und genutzte Produkte und Dienstleistungen zu nennen. Diese machen eine europäische und ggf. internationale Rechtsetzung und -durchsetzung notwendig. In der Vergangenheit hat der Gesetzgeber auf diese Besonderheiten oftmals damit reagiert, dass er in Gesetzen relativ abstrakte und technikneutrale Regelungen erlassen hat. Diese haben jedoch den Nachteil, dass sie zumeist mit rechtlichen Grauzonen und Rechtsunsicherheit einhergehen. Das gilt gerade auch für die Datenschutzgesetzgebung.

Die Ko-Regulierung, z. B. in Form von Verhaltenskodizes, kann hier eine sinnvolle Ergänzung darstellen, um in ausgewählten und insbesondere untergesetzlichen Bereichen einerseits die Rechtsetzung durch Konkretisierungen zu entlasten und so für mehr Rechtssicherheit zu sorgen und andererseits durch private Selbstkontrolleinrichtungen eine bessere Rechtsdurchsetzung zu ermöglichen

### 2.5.1 ROLLE UND FUNKTIONEN DER KO-REGULIERUNG

Im geltenden Datenschutzrecht besteht mit § 38a BDSG vom Prinzip her eine Grundlage für die Anerkennung privat gesetzter Standards, die ihrerseits auf Art. 27 der Datenschutz-Richtlinie beruht. Allerdings normiert § 38a BDSG keinerlei spezielle Rechtswirkung dieser privat gesetzten Standards mit Blick auf Gerichte oder Behörden. Vielmehr findet sich im einschlägigen Schrifttum lediglich der Hinweis, dass diese Kodizes als „amtlich bestätigte Interpretationshilfe“ herangezogen werden könnten (so etwa Gola et al. 2015: § 38a, Rn. 2). In der Praxis bedeutet das, dass Unternehmen zwar einen Kodex erarbeiten und sich einem Selbstregulierungsmechanismus unterwerfen und diesen auch durch die Behörden anerkennen lassen können, dieser Aufwand jedoch mit keinem Anreiz einhergeht – sei es in der Form, dass solche Unternehmen hinsichtlich der Aufsicht entlastet wären oder die Teilnahme am Kodex eine rechtliche Vermutungswirkung hätte. Im Gegenteil: Unternehmen verweisen darauf, dass das föderale System der Rechtsdurchsetzung dazu führt, dass die Datenschutzgesetze durch die unterschiedlichen Behörden auch unterschiedlich ausgelegt werden. So kommt es immer wieder vor, dass Datenschutzpraktiken, die durch eine Behörde als zulässig eingestuft wurden, durch eine andere als unzulässig eingestuft werden.

---

**33** Siehe ausführlich zu dem Thema Spindler/Thorun (2015).

Tabelle 5
**Ergebnisse der Stärken- und Schwächenanalyse zur Ko-Regulierung**

| | Zusammenfassung | Gesamtbewertung |
|---|---|---|
| **Stärken- und Schwächenanalyse** | Es existiert in Deutschland noch eine Reihe von Hürden und es mangelt an Anreizen, damit dieses Instrument von Unternehmen in angemessener Weise angenommen wird. |  |
| **Voraussichtliche Auswirkungen der DS-GVO** | Die DSG-VO verbessert den Rahmen für die Anerkennung von Verhaltenskodizes und die Akkreditierung von Kontrolleinrichtungen. Allerdings wäre es überdies sinnvoll, eine rechtliche Vermutungswirkung für anerkannte Verhaltenskodizes einzuführen. |  |

Quelle: eigene Darstellung.

Dieser unterentwickelte Rechtsrahmen ist eine Erklärung dafür, warum die Ko-Regulierungsaktivitäten bislang hinter den Erwartungen zurückbleiben und Verhaltenskodizes, Datenschutzzertifizierungen und -siegel bislang keine wesentliche Rolle spielen. Das ist bedauerlich, denn es gäbe einen enormen Bedarf an Anwendungen, die die Prinzipien Privacy by Design oder Privacy by Default berücksichtigen.

### 2.5.2 ABSEHBARE AUSWIRKUNGEN DER DS-GVO AUF DIE ROLLE DER KO-REGULIERUNG

Die DS-GVO stärkt das Instrument der Ko-Regulierung signifikant (siehe ausführlich dazu v. Braunmühl 2015: 231). In Bezug auf die Rechtsdurchsetzung ist hier insbesondere der neue Art. 38a zu nennen. Danach sollen zuvor akkreditierte private Kontrolleinrichtungen die Einhaltung der nach Art. 38 anerkannten Verhaltensregeln gewährleisten. Dabei sind sowohl an die Anerkennung der Verhaltensregeln (Art. 38) als auch an die Akkreditierung der privaten Kontrolleinrichtungen (Art. 38a) strenge Voraussetzungen geknüpft. Die Regelungen bilden ein deutlich besseres Fundament für die Ko-Regulierung, als es noch die auf Art. 27 der EU-Datenschutzrichtlinie basierende bisherige Gesetzeslage ermöglicht hat.

Gleichwohl ist zu kritisieren, dass die oben genannten Regelungen im Rahmen der DS-GVO bei einer erfolgreichen Annahme einer Verhaltensregel durch die Aufsichtsbehörden für die Gerichte jedoch keine Vermutungswirkung hinsichtlich der Rechtskonformität für behördlich anerkannte Kodizes vorsehen. Eine solche Vermutungswirkung existiert etwa im Produktsicherheitsrecht. Hier können Unternehmen, die sich einer Selbstregulierung angeschlossen haben, damit rechnen, dass ein Gericht oder eine Behörde im Wege des ersten Anscheins (Prima-facie-Beweis) zumindest davon auszugehen hätten, dass sich das Unternehmen, das die Standards in seiner Branche einhält, auch gesetzeskonform verhält. Umgekehrt können in Einzelfällen, wenn ein begründeter Verdacht besteht, dass die Standards veraltet sind, nicht den oben entwickelten Kriterien entsprechen oder im Einzelfall strengere Maßstäbe gelten müssen, staatliche Instanzen (Gerichte, Behörden) höhere Anforderungen stellen, sodass auch aus verfassungsrechtlichen Gründen die staatliche Kontrolle nicht aufgegeben, sondern nur zurückgenommen wäre. Hierdurch könnte den Unternehmen ein erheblicher Anreiz gegeben werden, sich an einer Ko-Regulierung zu beteiligen.

### 2.5.3 STÄRKEN- UND SCHWÄCHENANALYSE

Wie die Analyse zeigt, fordern die spezifischen Charakteristika der Informationsgesellschaft klassische Rechtsetzungs- und -durchsetzungsinstrumente heraus. Ko-Regulierungsaktivitäten in Form von Verhaltenskodizes, Gütesiegeln und Zertifizierungen könnten einen wichtigen zusätzlichen Beitrag leisten, um die Rechtsdurchsetzung zu verbessern und um Ansätzen wie Privacy by Design und Privacy by Default zum Durchbruch zu verhelfen.

Allerdings fehlt es bislang in Deutschland an Anreizen für Unternehmen, sich auf eine Ko-Regulierung einzulassen. Die in der DS-GVO vorgesehenen Regelungen zur Anerkennung von Verhaltenskodizes und Akkreditierung von Kontrolleinrichtungen könnten die Ausgangslage hierbei verbessern. Allerdings greifen diese Maßnahmen noch zu kurz. Nötig wäre es überdies, anerkannte Verhaltenskodizes mit einer wie oben beschriebenen Vermutungswirkung auszustatten.

# 3

# ZUSAMMENFASSUNG UND ABLEITUNG VON HANDLUNGSEMPFEHLUNGEN

In diesem Abschnitt werden die Ergebnisse der Analyse zusammenfassend dargestellt und Handlungsempfehlungen abgeleitet. Die Struktur orientiert sich an der Analyse der jeweiligen Rechtsdurchsetzungsinstrumente des zweiten Kapitels. Überdies werden im Abschnitt 3.7 Handlungsempfehlungen zur Verbesserung der Rechtsdurchsetzung aufgeführt, die über die analysierten Instrumente hinausgehen. Da sie jedoch im Diskurs zu diesem Thema genannt werden, hier im Rahmen dieser Studie aber nicht vertieft diskutiert werden konnten, werden sie der Vollständigkeit halber zumindest aufgelistet.

## 3.1 ZUSAMMENFASSENDE GESAMTBEWERTUNG: ES BESTEHT EIN BREITER HANDLUNGSBEDARF

In der zusammenfassenden Gesamtbewertung zeigt die Analyse, dass es bei der Rechtsdurchsetzung im Bereich des Verbraucherdatenschutzes einen breiten Handlungsbedarf gibt. Insbesondere gilt es, die Rechtsdurchsetzungsmöglichkeiten der Betroffenen zu verbessern, aber auch die staatliche Aufsicht in eine Lage zu versetzen, ihren Pflichten angemessen nachzukommen, und die Anreize für die Ko-Regulierung zu erhöhen.

Hinsichtlich der kollektiven Klagemöglichkeiten anerkannter Verbraucherverbände kommt die Analyse zu dem Ergebnis, dass die Bundesregierung mit den Änderungen am UKlaG jüngst eine wichtige Lücke in der Rechtsdurchsetzung geschlossen hat. Am System der betrieblichen Datenschutzbeauftragten sollte überdies in Deutschland weiter festgehalten werden. Die folgende Tabelle fasst die Gesamtbewertungen zusammen.

## 3.2 HANDLUNGSEMPFEHLUNGEN HINSICHTLICH DER RECHTSDURCHSETZUNG DURCH DIE BETROFFENEN

Die Stärken- und Schwächenanalyse der Rechtsdurchsetzung durch die Betroffenen zeigt, dass es eine gravierende Diskrepanz zwischen den Betroffenenrechten auf der einen Seite und der gelebten Praxis auf der anderen Seite gibt. So ist es für Verbraucher_innen trotz der Transparenzrechte nahezu unmöglich, einen angemessenen Überblick über Datenverarbeitungsvorgänge zu behalten, Verstöße zu erkennen und gegen diese vorzugehen. Auch stellt das Haftungsrecht im Bereich des Datenschutzes nur ein sehr stumpfes Schwert dar.

Diese Diskrepanz zwischen Theorie und Praxis wurde auf eine Reihe von Hindernissen zurückgeführt. Sie lässt sich durch die folgenden Maßnahmen reduzieren:

- **Datenschutzerklärungen vereinfachen:** Die Analyse zeigt, dass viele Verbraucher_innen Datenschutzerklärungen nicht lesen, da diese zu kompliziert, in einer unverständlichen Sprache verfasst und zu lang sind. Die Bundesregierung sollte daher Maßnahmen fördern, die darauf abzielen, Mehrebenenerklärungen einzuführen. Diese sollten so gestaltet sein, dass die wesentlichen Punkte am Anfang stehen und detailliertere Informationen bei Bedarf angezeigt werden können. Die Lesbarkeit sollte durch standardisierte Piktogramme unterstützt werden. Und die Erklärungen sollten maschinenlesbar gestaltet sein, sodass sie von den Endgeräten der Verbraucher_innen je nach individuellen Präferenzen ausgewertet werden können, damit die Verbraucher_innen gemäß ihren Vorstellungen handeln können. Überdies könnte erwogen werden, Datenschutzeinwilligungen mit einem „Ablaufdatum" zu versehen. Das im Rahmen des IT-Gipfels am 19.11.2015 präsentierte Muster für einen „One-Pager" ist ein wichtiger Schritt in die richtige Richtung. Dieses gilt es nun in der Praxis anzuwenden (BMJV 2015).

- **Freiheit der Einwilligungen gewährleisten und eine Differenzierung ermöglichen:** Wie dargestellt basiert das Datenschutzrecht auf dem Prinzip des Verbots mit Erlaubnisvorbehalt. Die freiwillige Einwilligung spielt hierbei eine zentrale Rolle. Allerdings liegt sie in der Praxis häufig nicht vor. So sind Verbraucher_innen oft nicht frei, über die Datenpreisgabe zu entscheiden, etwa weil sie kaum in der Lage sind, zwischen zwei gleichwertigen Anbietern auszuwählen. Inwieweit die Regelungen der DSG-VO

Tabelle 6
**Gesamtbewertung**

| | Zusammenfassung | Gesamtbewertung |
|---|---|---|
| **Betroffene** | Auf der einen Seite existiert ein umfassendes System von Betroffenenrechten. Auf der anderen Seite führt dieses System in der Praxis nicht dazu, dass Verbraucher_innen ausreichend informiert sind und ihre Rechte selbst durchsetzen können. Es existiert demnach eine gravierende Diskrepanz zwischen den Rechten und der gelebten Praxis. |  |
| **Staatliche Aufsicht** | Die staatliche Aufsicht stellt in Deutschland eine wesentliche Säule in der Rechtsdurchsetzung dar. Allerdings leidet sie an einer personellen und finanziellen Unterausstattung, und die Bußgeldrahmen sind nicht ausreichend hoch. Auch wird angemahnt, dass das föderale System der Rechtsauslegung zu unterschiedlichen Aufsichtsniveaus führt. |  |
| **Anerkannte Verbraucherverbände** | Bislang spielen anerkannte Verbraucherverbände lediglich eine marginale Rolle in der kollektiven Rechtsdurchsetzung, da die rechtlichen Grundlagen umstritten sind bzw. nicht vorliegen. Der Gesetzgeber hat hierauf mit Änderungen im UKlaG reagiert. Diese sollten zu einer spürbaren Verbesserung führen. Allerdings ist hierfür eine ausreichende Finanzierung der Rechtsdurchsetzungsaktivitäten bei den Verbraucherorganisationen notwendig. |  |
| **Betriebliche Datenschutzbeauftragte** | Grundsätzlich nehmen die betrieblichen Datenschutzbeauftragten eine wichtige Funktion in der Durchsetzung des Datenschutzes ein. Allerdings wird von einigen kritisiert, dass ihre Rolle noch stärker sein und ihr Beitrag zur Datensparsamkeit größer ausfallen könnte. |  |
| **Ko-Regulierung** | Es existiert in Deutschland noch eine Reihe von Hürden, und es mangelt an Anreizen, damit dieses Instrument von Unternehmen in angemessener Weise angenommen wird. |  |

Quelle: eigene Darstellung.

diesbezüglich spürbare Verbesserungen mit sich bringen werden, ist nicht eindeutig zu sagen. Denn die Vielzahl von Abwägungs- und nationalen Öffnungsklauseln wird dazu führen, dass die Auswirkungen der neuen Regelungen letztlich von der Auslegungs- und nationalen Ausgestaltungspraxis abhängen werden.

– **Datensparsamkeit so einfach wie möglich machen – Privacy by Design und Default fördern:** Die Verhaltensforschung zeigt, dass sich Verbraucher_innen an Voreinstellungen orientieren. Dies trifft auch auf den Datenschutz zu. So gab in einer Studie knapp die Hälfte der Befragten an, noch nie eine Voreinstellung bei einem Onlinedienst verändert zu haben (European Commission 2015: 92). Diese Tatsache verdeutlicht die Notwendigkeit, Datensparsamkeit durch das Design der Applikationen und durch Voreinstellungen so einfach wie möglich zu machen. Dieses Prinzip findet sich auch in Art. 23 der DS-GVO (Datenschutz durch Technik und Voreinstellungen). Um dieses Prinzip jedoch mit Leben zu füllen, bedarf es einer Verantwortungsübernahme durch Unternehmen, insbesondere im Wege der Konkretisierung durch Maßnahmen der Ko-Regulierung (siehe hierzu auch die Handlungsempfehlungen im Abschnitt 3.6). Ebenso wichtig ist die öffentlich geförderte Forschung in diesem Bereicht, wie sie derzeit etwa im Rahmen des BMBF-Forschungsschwerpunkts „IKT 2020: Datenschutz – Selbstbestimmt in der digitalen Welt" vorangetrieben wird. Solche Forschung sollte ausgebaut werden. Auch sollten die Anreize für Unternehmen erhöht werden, in entsprechende Techniken zu investieren.

– **Auskunftsersuchen vereinfachen:** Zwar verfügen Verbraucher_innen über das Recht, sich bei Unternehmen über die dort verarbeiteten Daten zu informieren. Allerdings wurde gezeigt, dass es in der Praxis aufwändig ist, von diesem Recht Gebrauch zu machen. Daher sollte die Bundesregierung prüfen, ob es nicht technische Möglichkeiten gibt, den Prozess der Beantragung von Auskunftsersuchen zu vereinfachen. So förderte das damalige Bundes-

ministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) etwa ein Innovationsvorhaben, in dem es darum ging, ein Datenschutz-Auskunftsportal zu entwickeln. Weil das Vorhaben jedoch darauf ausgelegt war, sich selbst durch Unternehmensbeiträge zu finanzieren und der Zuspruch vonseiten der Wirtschaft hierfür zu gering war, wurde es nie implementiert. Die Konzepte liegen jedoch vor und könnten umgesetzt werden.[34] Überdies bezieht sich das Auskunftsrecht heute oft nicht auf die zugrunde liegenden Algorithmen. Auch hier besteht ein Nachbesserungsbedarf (Sachverständigenrat für Verbraucherfragen 2016: 28).

– **Allgemeine Informationsaktivitäten für Verbraucher_innen über datenverarbeitende Prozesse erhöhen:** Verbraucherinformationsaktivitäten über datenverarbeitende Prozesse und die Betroffenenrechte sollten fortgesetzt und ausgebaut werden. Hierbei kommt u. a. den bei den Verbraucherorganisationen angesiedelten Marktwächter_innen eine wichtige Funktion zu. Sie sollten als „Seismografen" Problemfelder identifizieren und diese publik machen. Dadurch würde auch das allgemeine Datenschutzbewusstsein gestärkt. In der Ausrichtung der Informationsaktivitäten sollte zielgruppenspezifisch vorgegangen werden.

## 3.3 HANDLUNGSEMPFEHLUNGEN HINSICHTLICH DER STAATLICHEN AUFSICHT

Mit Blick auf die Rolle der staatlichen Aufsicht kommt die Analyse zu dem Ergebnis, dass die rechtlichen Grundlagen vom Prinzip her ausreichen. Allerdings wurden gravierende Defizite in der Praxis identifiziert, die die Effektivität der staatlichen Aufsicht schmälern. Diese sollten durch die folgenden Maßnahmen adressiert werden:

– **Personelle und finanzielle Bedarfe der Datenschutzaufsichtsbehörden aufzeigen und in einen Diskurs über Abhilfe einsteigen:** Die Analyse zeigt, dass die Datenschutzaufsichtsbehörden personell und finanziell unzureichend ausgestattet sind. Von einigen wird sogar angenommen, dass spätestens mit Inkrafttreten der DS-GVO eine Verdreifachung der Behördenausstattung notwendig werden wird (Schulzki-Haddouti 2015: 78). Um die Frage klären zu können, wie hoch der Bedarf tatsächlich ist, sollten die Landesdatenschutzbehörden gemeinsam mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen des Düsseldorfer Kreises eine Bestands- und Defizitanalyse der staatlichen Rechtsdurchsetzungspraxis erstellen. Diese gilt es dann auf Landes- und Bundesebene zu diskutieren und Abhilfe zu schaffen.

– **Vorbereitungen für eine bürgernahe und effektive Umsetzung des Datenschutzausschusses und der Koordinierungsmechanismen einleiten:** Wie dargestellt wird mit der DS-GVO der Datenschutzausschuss sowie ein Kohärenzmechanismus eingeführt. Für die föderale Aufsichtsstruktur in Deutschland müssen daher Lösungen gefunden werden, die den föderalen Anforderungen, gleichzeitig aber auch den Anforderungen nach Bürgernähe und Effektivität gerecht werden.

## 3.4 HANDLUNGSEMPFEHLUNGEN HINSICHTLICH DER RECHTSDURCHSETZUNG DURCH ANERKANNTE VERBRAUCHERVERBÄNDE

Die Analyse hat gezeigt, dass anerkannte Verbraucherverbände ihre Verbandsklagebefugnisse im Verbraucherdatenschutz bislang in der Regel wegen einer umstrittenen bzw. unzureichenden rechtlichen Grundlage nicht einsetzen können. Hierdurch ist die Rolle der Verbraucherverbände für die kollektive Rechtsdurchsetzung im Verbraucherdatenschutz geschmälert. Mit den Änderungen am UKlaG erhalten die Verbraucherverbände jedoch eine Rechtsgrundlage, um in diesem Bereich tätig zu werden. Gleichwohl wird der Erfolg des Einsatzes dieses Instruments insbesondere davon abhängen, dass die Verbraucherverbände mit ausreichenden Ressourcen ausgestattet sind. Inwieweit die öffentliche Förderung des Marktwächters hierzu bereits ausreicht, kann an dieser Stelle nicht beantwortet werden. Zu erwägen wäre zudem, dass abgeschöpfte Unrechtsgewinne in eine Stiftung einfließen, die dem Verbraucherschutz dient und mittelbar auch Verbraucherverbände finanziell unterstützt.

## 3.5 HANDLUNGSEMPFEHLUNGEN HINSICHTLICH DER RECHTSDURCHSETZUNG DURCH DIE BETRIEBLICHEN DATENSCHUTZBEAUFTRAGTEN

Die betrieblichen Datenschutzbeauftragten spielen grundsätzlich eine wichtige Rolle für die Selbstkontrolle der Unternehmen. Gleichwohl argumentieren einige, dass die Realität hinter dem Potenzial dieses Instruments zurückbleibt. So könnten sie noch einen wesentlich größeren Beitrag dafür leisten, die Rechtsdurchsetzung voranzutreiben. Hierfür ist es jedoch notwendig, den Mehrwert der betrieblichen Datenschutzbeauftragten für die Unternehmen selbst und für die Rechtsdurchsetzung sichtbarer zu machen. Denn häufig werden die Datenschutzbeauftragten von den Unternehmensführungen lediglich als Kostenposten wahrgenommen und nicht als diejenigen, die für den Geschäftserfolg einen Beitrag leisten. Auch ist die Funktion der Datenschutzbeauftragten für die Rechtsdurchsetzung wenig bekannt. Daher sollten Untersuchungen durchgeführt werden, die darauf abzielen, die Mehrwerte der betrieblichen Datenschutzbeauftragten für die Unternehmen und die Rechtsdurchsetzung im Allgemeinen aufzuzeigen. Der Ansatz „Privacy made in Germany" sollte gefördert und dessen Zusammenhang mit den betrieblichen Datenschutzbeauftragten dargelegt werden.

---

**34** Das Vorhaben „Datenschutz-Auskunftsportal" wurde von 2011 bis 2012 durch das Unabhängige Landeszentrum für Datenschutz (ULD), das IT-Unternehmen Consist Software Solutions GmbH sowie ConPolicy durchgeführt. Weitere Informationen hierzu finden sich unter: http://www.fisaonline.de/index.php?lang=dt&act=projects&p_id=4839 (29.2.2016).

## 3.6 HANDLUNGSEMPFEHLUNGEN HINSICHTLICH DER KO-REGULIERUNG

Gerade in der Informationsgesellschaft kann die Ko-Regulierung die Rechtssetzung und -durchsetzung sinnvoll ergänzen. Allerdings ist der Stellenwert der Ko-Regulierung heute in Deutschland noch nicht so groß wie in anderen Staaten. Grund dafür ist eine Reihe von Hürden, die der Ko-Regulierung entgegenstehen. Diese Hürden gilt es abzubauen. Hierfür sollten die folgenden Maßnahmen umgesetzt werden:

- **Mindeststandards entwickeln:** In Anlehnung an die EU-Principles for Better Self- and Co-Regulation sollten Mindestanforderungen an Ko-Regulierungsinitativen hinsichtlich der Standardsetzung und -durchsetzung entwickelt werden.
- **Rahmenbedingungen verbessern:** Die allgemeinen Rahmenbedingungen für die Ko-Regulierung sollten verbessert werden. Hierzu zählen 1) positive und negative Anreize (wie die öffentliche Förderung von Multi-Stakeholder-Prozessen sowie die Drohung staatlicher Regulierung), 2) Ansätze zur Lösung von Trittbrettfahrer-Problematiken (etwa durch die Einführung eines Gütesiegels für glaubwürdige Ko-Regulierung) und 3) die Erhöhung der Rechtssicherheit. Um die Rechtssicherheit zu erhöhen, bietet es sich an, eine rechtliche Vermutungswirkung hinsichtlich der Rechtskonformität für behördlich anerkannte Kodizes einzuführen (diese fehlt bislang sowohl in § 38a BDSG wie auch in Art. 38 ff. DS-GVO). Überdies sollten glaubwürdige Zertifizierungsansätze weiterentwickelt werden. Hierdurch könnten insbesondere Konzepte wie Privacy by Design und Privacy by Default gefördert werden.

## 3.7 WEITERFÜHRENDE PERSPEKTIVEN ZUR RECHTSDURCHSETZUNG

In der Diskussion über eine Verbesserung der Rechtsdurchsetzung werden neben den hier genannten Empfehlungen, die allesamt darauf abzielen, bestehende Instrumente wirksamer auszugestalten, auch noch andere, darüber hinausgehende Maßnahmen vorgeschlagen. Sie können an dieser Stelle nur aufgezählt, hinsichtlich ihrer Vor- und Nachteile aber nicht bewertet werden. Eine solche Bewertung muss an anderer Stelle erfolgen:[35]

- Naming & Shaming („Datenschutzpranger“);
- Maßnahmen zur Begrenzung von „Datenmacht“ (etwa durch Monopolbeschränkungen, Pluralismusförderung, Verknüpfungsbeschränkungen oder eine Datenverkehrssteuer);
- Maßnahmen, um eine „Bezahlkultur“ im Internet zu fördern, sodass die heute dominierende Werbefinanzierung diverser Angebote abgelöst wird;
- eine Kommerzialisierung der Daten, sodass Verbraucher_innen für ihre Daten und deren Nutzung eine finanzielle Vergütung erhalten (Monopolkommission 2015: K. 12, Tz. 84-90; Verbraucherzentrale Bundesverband 2015: 2–4).

35 Friedrich-Ebert-Stiftung 2015: 4.

# Abbildungsverzeichnis



# Abkürzungsverzeichnis

| | |
|---|---|
| AGB | Allgemeine Geschäftsbedingungen |
| BDSG | Bundesdatenschutzgesetz |
| BfDI | Bundesbeauftragte für den Datenschutz und die Informationsfreiheit |
| BMELV | Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz |
| BMJV | Bundesministerium der Justiz und für Verbraucherschutz |
| BSI | Bundesamt für Sicherheit in der Informationstechnologie |
| BVerfG | Bundesverfassungsgericht |
| DS-GVO | Datenschutz-Grundverordnung |
| EU | Europäische Union |
| EWR | Europäischer Wirtschaftsraum |
| GG | Grundgesetz |
| IKT | Informations- und Kommunikationstechnologien |
| RL | Richtlinie |
| SÜG | Sicherheitsüberprüfungsgesetz |
| TKG | Telekommunikationsgesetz |
| TMG | Telemediengesetz |
| UKlaG | Unterlassungsklagengesetz |
| UWG | Gesetz gegen den unlauteren Wettbewerb |
| vzbv | Verbraucherzentrale Bundesverband e. V. |

# Literaturverzeichnis


Baumann, Zygmunt; Lyon, David 2013: Daten, Drohnen, Disziplin – Ein Gespräch über flüchtige Überwachung, Berlin.

Bayerisches Landesamt für Datenschutzaufsicht 2015: Pressemitteilung – Datenschutz für Kinder, Ansbach.

Bergmann, Lutz; Möhrle, Roland; Herb, Armin 2015: Datenschutzrecht, München.

Bundesbeauftragte für Datenschutz und Informationsfreiheit 2013: 25. Tätigkeitsbericht 2013–2014, Bonn.

Bundesministerium der Justiz und für Verbraucherschutz (BMJV) 2015: Datenschutz auf einen Blick: „One-Pager" als Muster für transparente Datenschutzhinweise vorgestellt, Pressemitteilung vom 19.11.2015.

Braunmühl, Patrick v. 2015: Ansätze zur Ko-Regulierung in der Datenschutz-Grundverordnung, in: PinG 2015, S. 231.

Bräutigam, Peter 2012: Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, in: MMR 2012, S. 635.

Bräutigam, Peter; Schmidt-Wudy, Florian 2015: Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung, in: CR 2015, S. 56–63.

Brühann, Ulf 2011: Gutachterliche Stellungnahme – Vollharmonisierung oder Mindestharmonisierung – welchem Regelungsansatz folgt die DS-RL 95/46/EG?, Drucksache Innenausschuss des Deutschen Bundestages, 16(4)561 L.

Elbrecht, Carola; Schröder, Michaela 2015: Verbandsklagebefugnisse bei Datenschutzverstößen für Verbraucherverbände, in: K&R 2015, S. 361.

Erbs, Georg; Kohlhaas, Max 2015: Strafrechtliche Nebengesetze, München.

European Commission 2015: A Digital Single Market Strategy for Europe, Brüssel.

European Commission 2011: Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, Brüssel.
European Commission 2015: Special Eurobarometer 431: Data Protection, Brüssel.

Friedrich-Ebert-Stiftung (FES) 2015: Thesenpapier zum Fachgespräch: Instrumente der Rechtsdurchsetzung im Verbraucherdatenschutz – Bestandsaufnahme und Reformperspektiven, Berlin.

Gola, Peter; Schomerus, Rudolf 2015: BDSG, München.

Hansen, Marit 2015: Herausforderungen Verbraucherdatenschutz in der digitalen Welt, in: WISO Direkt 2015, S. 1.

Hauschka, Christoph E. 2010: Corporate Compliance, München.

Hoeren, Thomas; Sieber, Ulrich; Holznagel, Bernd 2015: Multimedia-Recht, München. Initiative D21 2014, D21-Digital-Index 2014, Berlin.

Lejeune, Mathias 2013: Datenaustausch mit den Vereinigten Staaten von Amerika, in: CR 2013, S. 822–828.

Monopolkommission 2015: Wettbewerbspolitik: Herausforderung digitale Märkte, Bonn.

Münchener Kommentar zum Bürgerlichen Gesetzbuch 2012: Schuldrecht Allgemeiner Teil §§ 241–432, München.

Nietsch, Thomas 2014: Zur .berprüfung der Einhaltung des Datenschutzrechts durch Verbraucherverbände, in: CR 2014, S. 272–278.

Plath, Kai-Uwe 2013: Bundesdatenschutzgesetz (BDSG), München.

Sachverständigenrat für Verbraucherfragen 2016: Digitale Welt und Handel: Verbraucher im personalisierten Online-Handel, https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/01192016_Digitale_Welt_und_Handel.pdf?__blob=publicationFile&v=2 (20.3.2016).

Schulzki-Haddouti, Christiane 2015: Zu kurz gekommen: Deutsche Datenschutzbehörden leiden unter Personalknappheit, in: C't 2015 (Heft 17), S. 76.

Simitis, Spiros 2014: Bundesdatenschutzgesetz, München.

Spindler, Gerald 2014: Datenschutz und Persönlichkeitsrechte im Internet, in: GRUR-Beilage 2014, S. 101.

Spindler, Gerald; Schuster, Fabian 2015: Recht der elektronischen Medien, München.

Spindler, Gerald; Thorun, Christian 2015: Eckpunkte einer digitalen Ordnungspolitik, Berlin.

Stiftung Warentest 2012a: Ausgespäht: Datenschutz bei Apps, test (6/2012), S. 38–43.

Stiftung Warentest 2012b: Shopping-Apps: Nur zwei sind sicher und gut (11/2012), S. 38–42.

Stiftung Warentest 2013: Heiter bis wolkig: Wetter-Apps (6/2013), S. 83–85.

Stiftung Warentest 2014: Spritpreis-Apps im Datenschutz-Test: Vier sind kritisch, https://www.test.de/Spritpreis-Apps-im-Datenschutz-Test-Vier-sind-kritisch-4663692-0/ (19.11.2015).

Taeger, Jürgen; Gabel, Detlev 2013: BDSG, Frankfurt a. M.

Verbraucherzentrale Bundesverband 2013: Modernisierung des europäischen Datenschutzrechts, Berlin.

Verbraucherzentrale Bundesverband 2014: Digitalisierung des Verbraucheralltags, Berlin.

Verbraucherzentrale Bundesverband 2015: Wettbewerbspolitik in digitalen Märkten aus Verbrauchersicht, Berlin.

Vulin, Danica 2012: Ist das deutsche datenschutzrechtliche Schriftformerfordernis zu viel des Guten?, in: ZD 2012, S. 414–418.

Walz, Stefan 1991: Das neue Bundesdatenschutzgesetz, Kompromiß als Leitprinzip, in: CR 1991, S. 364.

Weidlich-Flatten, Eva 2014: Verbraucherschutzverbände als Heilsbringer für den Datenschutz?, in: ZRP 2014, S. 196–198.

Impressum:


**Friedrich-Ebert-Stiftung**
Herausgeber: Abteilung Wirtschafts- und Sozialpolitik
Godesberger Allee 149, 53175 Bonn
Fax 0228 883 9205, www.fes.de/wiso

Bestellungen/Kontakt: wiso-news@fes.de



**ISBN 978-3-95861-297-6**

Titelmotiv: © Stefan Boness/VISUM
Gestaltung: www.stetzer.net
Druck: www.bub-bonn.de

FRIEDRICH EBERT STIFTUNG

www.fes-2017plus.de