

Verbraucherdatenschutz im Internet der Dinge

Irina Domurath, Lea Kosyra

SVRV Working Paper Nr. 3

Veröffentlichungen des Sachverständigenrats für Verbraucherfragen

Dezember 2016

Berlin, Dezember 2016
ISSN 2365-919X

Herausgeber:

Sachverständigenrat für Verbraucherfragen
beim Bundesministerium der Justiz und für Verbraucherschutz
Mohrenstraße 37
10117 Berlin

Telefon: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525
E-Mail: info@svr-verbraucherfragen.de
Internet: www.svr-verbraucherfragen.de

Diese Veröffentlichung ist im Internet abrufbar.
© SVRV 2016

Mitglieder des SVRV

Prof. Dr. Lucia Reisch (Vorsitzende)

Professorin für Interkulturelle Konsumforschung und europäische Verbraucherpolitik an der Copenhagen Business School

Dr. Daniela Büchel (stellv. Vorsitzende)

Mitglied der Geschäftsleitung REWE für die Bereiche Human Resources und Nachhaltigkeit

Prof. Dr. Gerd Gigerenzer

Direktor der Abteilung „Adaptives Verhalten und Kognition“ und des Harding-Zentrums für Risikokompetenz am Max-Planck-Institut für Bildungsforschung in Berlin

Helga Zander-Hayat

Leiterin des Bereichs Markt und Recht bei der Verbraucherzentrale Nordrhein-Westfalen

Prof. Dr. Gesche Joost

Professorin für das Fachgebiet Designforschung an der Universität der Künste und Internetbotschafterin der Bundesregierung im Gremium der „Digital Champions“ der EU

Prof. Dr. Hans-Wolfgang Micklitz

Professor für Wirtschaftsrecht am Europäischen Hochschulinstitut in Florenz

Prof. Dr. Andreas Oehler

Professor für Finanzwirtschaft an der Universität Bamberg und Direktor der Forschungsstelle Verbraucherfinanzen und Verbraucherbildung

Prof. Dr. Kirsten Schlegel-Matthies

Professorin für Haushaltswissenschaft an der Universität Paderborn

Prof. Dr. Gert G. Wagner

Professor für Empirische Wirtschaftsforschung und Wirtschaftspolitik an der Technischen Universität Berlin, Vorstandsmitglied des Deutschen Instituts für Wirtschaftsforschung und Max Planck Fellow am MPI für Bildungsforschung

Mitarbeitende des SVRV

Leiter der Geschäftsstelle: Thomas Fischer

Wissenschaftlicher Stab der Geschäftsstelle: Mathias Bug, Dr. Irina Domurath,
Dr. Christian Groß

Disclaimer

Die Working Papers decken Arbeiten ab, die im Arbeitszusammenhang des SVRV entstanden sind. Für die Inhalte tragen die jeweiligen Autorinnen und Autoren alleinige Verantwortung, sie spiegeln nicht unbedingt die Meinung des Rates wider.

Verbraucherdatenschutz im Internet der Dinge

Irina Domurath, Lea Kosyra

Abstract

Das Internet der Dinge beschreibt die Vernetzung von Alltagsgeräten im Internet zueinander. Seine Funktionalität basiert maßgeblich auf der Generierung von massenhaften und weit angelegten Datenströmen. Dabei kommt es zu Eingriffen in die Privatsphäre der Verbraucher. Obschon jegliche Datenerhebung und –verarbeitung entweder durch eine Einwilligung des Betroffenen oder einen anderen Legitimationstatbestand aus dem Datenschutzrecht legitimiert werden muss, ergeben sich erhebliche Schutzlücken, sowohl in materiell-rechtlicher als auch prozessualer Hinsicht. Dieses Working Paper beschäftigt sich mit der Frage, inwiefern die rechtliche Regulierung von Datenerfassungen und –verarbeitungen im Internet der Dinge und technische Maßnahmen zum Datenschutz die Probleme der Datenverarbeitung im Internet der Dinge lösen können.

Inhaltsübersicht

A.	Einleitung	5
B.	Vorverständnis & Aufbau	7
I.	Privatsphäre als schützenswertes Gut im Technikzeitalter	7
II.	Hypothese und Aufbau des Papiers	8
C.	Daten im IoT	9
I.	Datenströme im Smart Home	9
II.	Grundrechtliche Relevanz	11
III.	Einfachgesetzlicher Datenschutz: BDSG, TMG	13
D.	Zulässigkeit von Datenerhebungen im IoT	15
I.	Grundsätze des Datenschutzes	15
II.	Anwendbarkeit und Grundsätze des BDSG	16
III.	Zulässigkeit der Datenerhebung: Einwilligung und gesetzliche Erlaubnis	20
IV.	Zulässigkeit der Datenerhebung: AGB-Recht	31
V.	Beispiel: Zulässigkeit von Datenerhebungen durch die HCA	34
VI.	Sonderproblem Drittbetroffenheit	45
VII.	Zusammenfassung der materiell-rechtlichen Probleme	48
E.	Rechtsdurchsetzung	49
I.	Nationaler Rechtsschutz	49
II.	Internationale Rechtsdurchsetzung	69
III.	Beispiel: HCA und Rechtsschutz	78
IV.	Zusammenfassung der Probleme im Rechtsschutz	81
F.	Lösungsansätze: Datenschutz durch Recht und Technik	83
I.	Rechtsänderungen	83
II.	Datenschutz durch Technik	86
III.	Privacy by Default	100
IV.	Zertifizierung, Audit, Datenschutzsiegel	101
V.	Zusammenfassung: Datenschutz durch Technik	105
G.	Schlussbemerkung	106
H.	Literaturnachweise	108
I.	Annex	121
I.	Datenschutzerklärung HCA	121
II.	Export-Import-Standardvertrag	126

Inhaltsverzeichnis

A.	Einleitung	5
B.	Vorverständnis & Aufbau	7
I.	Privatsphäre als schützenswertes Gut im Technikzeitalter	7
II.	Hypothese und Aufbau des Papiers	8
C.	Daten im IoT	9
I.	Datenströme im Smart Home	9
II.	Grundrechtliche Relevanz	11
III.	Einfachgesetzlicher Datenschutz: BDSG, TMG	13
D.	Zulässigkeit von Datenerhebungen im IoT	15
I.	Grundsätze des Datenschutzes	15
II.	Anwendbarkeit und Grundsätze des BDSG	16
1.	Schutzbereich: Personenbezogene Daten	17
2.	Datenvermeidung und Datensparsamkeit	18
3.	Zweckgebundenheit	19
III.	Zulässigkeit der Datenerhebung: Einwilligung und gesetzliche Erlaubnis	20
1.	Anforderungen an die datenschutzrechtliche Einwilligung: § 4a BDSG	20
a.	Aufklärung	20
Rechtsgrundlage	20	
Probleme	21	
b.	Freiwilligkeit	22
Bestimmtheit	23	
Hervorhebung	23	
Ungleichgewichte	24	
Striktes Kopplungsverbot der DSGVO	26	
c.	Formerfordernisse	28
2.	Erforderlichkeit für Vertragszweck	28
a.	Zweckbindung für Geschäftszwecke	28
b.	Wahrung berechtigter Interessen	29
c.	Kopplungsverbot	30
IV.	Zulässigkeit der Datenerhebung: AGB-Recht	31
V.	Beispiel: Zulässigkeit von Datenerhebungen durch die HCA	34
1.	Datenerhebung und Verarbeitung der HCA	34
2.	Zulässigkeit nach BDSG	36
a.	Verantwortliche Stelle	36
b.	Einwilligung	36
c.	Eigene Geschäftszwecke § 28 BDSG	37
3.	Wirksamkeit nach AGB-Recht	39
a.	Datenschutzerklärung als AGB	39
b.	Klauselverbote mit Wertungsmöglichkeit, § 308 BGB	40
c.	Unangemessene Benachteiligung, § 307 BGB	41
d.	Rechtsfolgen	44
VI.	Sonderproblem Drittbetroffenheit	45
VII.	Zusammenfassung der materiell-rechtlichen Probleme	48
E.	Rechtsdurchsetzung	49
I.	Nationaler Rechtsschutz	49
1.	Individueller Rechtsschutz	49
a.	Auskunftsansprüche, §§ 19, 34 BDSG, Art. 15 DSGVO	49
b.	Berichtigungsansprüche, §§ 20, 35 BDSG, Arts. 16, 17 DSGVO	51
c.	Schadensersatzansprüche	54
2.	Kollektiver Rechtsschutz: Verbraucherzentralen & Marktwächter	56
a.	Verbandsklagebefugnis	56
b.	Stärkung des kollektiven Rechtsschutzes durch Marktwächter?	58
3.	Behördlicher Rechtsschutz	61
a.	System	61
b.	Maßnahmen - Übersicht	64

c.	Probleme	66
	Bußgeldfestsetzung.....	66
	Mangelnde Ausstattung.....	68
	Boykottierung	69
II.	Internationale Rechtsdurchsetzung.....	69
1.	Europäische Ebene.....	69
2.	Internationale Ebene	72
a.	Schutzbereich europäischer Vorschriften.....	72
b.	Datenschutzniveau	73
c.	Safe-Harbor	74
d.	Der Nachfolger: Privacy Shield	75
	Weitreichende Ausnahmen	76
	Fehlende Datenschutzgrundsätze	77
	Unzureichender Rechtsschutz.....	77
III.	Beispiel: HCA und Rechtsschutz.....	78
IV.	Zusammenfassung der Probleme im Rechtsschutz.....	81
F.	Lösungsansätze: Datenschutz durch Recht und Technik	83
I.	Rechtsänderungen	83
1.	Vertragsrecht & AGB-Kontrolle.....	83
2.	Drittbetroffenheit.....	84
3.	Rechtsdurchsetzung.....	84
II.	Datenschutz durch Technik.....	86
1.	Konzeptionelle Grundlagen: Code as Law – Law as Code - PETs	86
2.	Rechtliche Grundlagen: DSGVO und ePrivacy-Richtlinie	87
3.	Privacy by Design	89
a.	Grundsätze	89
b.	Parameter von Privacy by Design.....	91
c.	Diskussion	92
4.	PETs	95
a.	Technisches Identitätsmanagement.....	96
b.	Löschung, Anonymisierung und Pseudonymisierung	96
c.	DNT-Mechanismus	98
d.	Sticky Policies.....	99
III.	Privacy by Default	100
IV.	Zertifizierung, Audit, Datenschutzsiegel.....	101
1.	Vertragsrechtliche Lösung.....	101
2.	Marktorientierte & aufsichtsrechtliche Lösung	101
a.	Modelle und Vorteile	101
b.	Kritik & Lösungsansätze	103
V.	Zusammenfassung: Datenschutz durch Technik.....	105
G.	Schlussbemerkung.....	106
H.	Literaturnachweise	108
I.	Annex.....	121
I.	Datenschutzerklärung HCA.....	121
II.	Export-Import-Standardvertrag	126

A. Einleitung¹

Das sog. Internet of Things (IoT) beschreibt die Vernetzung von Gegenständen in einer internetähnlichen Struktur. Vernetzte Gegenstände haben eigene auf dem Mikrochip befindliche Identifikationsnummern (UID) und IP-Adressen und sind über Kabel oder kabellose Technik wie Satelliten, Telekommunikationsnetzwerke, Wi-Fi oder Bluetooth miteinander verbunden. Viele dieser Gegenstände werden durch den Einbau von Sensoren (z.B. bei Wearables), die Sammlung und Aggregation von Daten, und Self-Learning Software zunehmend „smart“.² Eines der meist diskutierten Anwendungsfelder ist neben vernetzten Fahrzeugen und Versicherungsscoreing das sog. Smart-Home, in dem verschiedene Produkte, wie Küchengeräte, Stromzähler, Fernseher, Smartphones u.a. Gegenstände miteinander vernetzt sind

Cisco Systems hat bereits eine Zukunftsvision vom Internet of Everything (IoE), das nicht nur vernetzte Gegenstände, sondern auch Personen, Daten und Prozesse umfasst. Dies ist die Vision einer vernetzten Welt, in der durch Vernetzung von Regierungs- und Verwaltungsaktivitäten, Kriminalitätsraten sinken sollen, Produktivität gesteigert werden soll, Staus vermieden werden, Investition in Umwelttechnik steigen und allgemeines Wirtschaftswachstum befördert werden sollen.³ Das IoE beruht auch auf der Weiterentwicklung des sog. Internet of Humans (IoH), welches auf der Integration der Menschen in das Internet beruht - mit der Quantified-Self-Bewegung als zentrale Datenquelle: „As the controlled Things become smarter, enabled by machine learning and artificial intelligence, it is likely that the need for human input will gradually decrease. The Things that today require such guidance to be aware of what the human user prefers will in the future be immersed into the environment in which they operate.“⁴

Unabhängig von dieser Zukunftsvision, werden für das IoT bereits mannigfaltige juristische Probleme diskutiert. Zum Beispiel wird untersucht, ob und inwiefern das BGB adäquat auf verbraucherrelevante Probleme reagieren kann. Der Deutsche Juristentag 2016 (DJT 2016) beispielsweise sieht relativ wenige Handlungsimperative. Er hat sich in seinen Beschlüssen gegen die Einführung eines neuen Vertragstypus für digitale Inhalte ausgesprochen. Dagegen sollen bestimmte Vorschriften in die bestehende Systematik von Verträgen eingefügt werden, z.B. eine dem § 453 I BGB nachempfundenen Regelung für Miet- und Werklieferungsverträge, oder eine Pflicht von Anbietern, digitaler Dienste in Dauerschuldverhältnissen nach dem jeweiligen aktuellen Stand der Technik zu erbringen.⁵

¹ Die Autorinnen danken Hans-W. Micklitz für hilfreiche Anmerkungen. Etwaige Fehler liegen in der Verantwortung der Autorinnen.

² Dazu Greengard, *The Internet of Things*, (MIT Press, 2015), S. 15-17.

³ Bradley et al, „Internet of Everything (IoE) Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector“, <http://internetofeverything.cisco.com/vas-public-sector-infographic/> (zuletzt abgerufen am 30.11.2017).

⁴ ABI Research, „Internet of Things vs. Internet of Everything: what's the difference?“, (2014), *ABI Research Whitepaper*, S. 5, <<https://digitalstrategy.nl/files/Internet-of-Things-vs-Internet-of-everything-by-ABI-June-2014.pdf>> (zuletzt abgerufen am 30.11.2016).

⁵ Beschlüsse des 71. Deutschen Juristentags, Essen 2016. Für die Überprüfung der Notwendigkeit, einen neuen Vertragstypus für digitale Inhalte einzuführen, hatte sich aber Hummelmeier in ihrem

Hier befinden sich die Beschlüsse des Juristentags durchaus im Widerspruch zu anderen Autoren, die das BGB in Bezug auf verbraucherrelevante Probleme in Vertragsbeziehungen, die digitale Inhalte (welcher Art auch immer) betreffen, für nicht adäquat halten. Aufgrund der strukturell bedingten Schlechterstellung von Verbrauchern beim Erwerb von digitalisierten Produkten oder Dienstleistungen gegenüber herkömmlichen Produkten und Dienstleistungen, beschreibt Wendehorst beispielweise eine strukturelle Erosion von Eigentum und Besitz, die durch Änderungen des BGB aufgefangen werden sollen.⁶

Außerdem ergibt sich ein Problem aus der Verknüpfung von Verträgen mit der Nutzung persönlicher und/oder nutzergenerierter Daten. Eine relativ unkritische Meinung wird hier vom DJT 2016 in seinen Beschlüssen vertreten. Insbesondere die Daten, die innerhalb eines Schuldverhältnisses über § 241 II BGB und die konkretisierende Rechtsprechung anfallen und genutzt werden, seien ausreichend geschützt. Eine erhebliche Regelungslücke wird nur in den Fällen gesehen, in denen Daten auf einem Datenträger gespeichert sind, der weder im Eigentum noch im Besitz desjenigen steht, der durch die Löschung oder Veränderung der Daten geschädigt wird. Eine kritischere Meinung wird dagegen zum Beispiel von der Verbraucherzentrale NRW eingenommen, die sich in einem Sammelband u.a. mit den Problemen der Datensicherheit und Überwachung auseinandersetzt.⁷ Auch Wendehorst schätzt den Regelungsbedarf im Schuldrecht für Datenschutzprobleme höher ein.⁸

Ein weiteres, viel diskutiertes Problem des IoT kann im Datenschutzrecht verortet werden. Die vernetzten Gegenstände senden zumeist Daten durch das Standard Internet oder eigene Netzwerke aus, wobei massive Datenmengen generiert werden. Die Beobachtung, dass ungeachtet der innovativen Aspekte im IoT, aufgrund ubiquitärer Datentransfers – die u.a. Handys, Fahrzeuge, biometrische Identifikation, Wearables, Microchips, Gesundheitsakten und Body Scanners umfassen - die Privatsphäre in Gefahr ist bzw. praktisch nicht mehr existiert,⁹ ist inzwischen ein Allgemeinplatz geworden. Die neuen Gefahren für die Privatsphäre ergeben sich aus dem „function creep“¹⁰ von IoT-Geräten, welche oftmals Funktionen erfüllen können, die im ursprünglichen Produktionsprozess nicht vorgesehen waren: So können Daten nicht nur für personalisierte Dienstleistungen benutzt werden,

Referat auf dem DJT 2016 ausgesprochen, s. *Thesen des 71. Deutschen Juristentags*, Essen 2016, <http://www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf> (zuletzt abgerufen am 30.11.2016)

⁶ Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016): Sie hatte auch gegen eine vorgehobene Rolle der Gerichte in der Anpassung von Generalklauseln argumentiert, da etwaige Rechtsunsicherheit angesichts der schnellen Entwicklungen nicht immer gewährleistet sei.

⁷ Bala/Schuldzinski (Hrsg.), *Schöne neue Verbraucherwelt? Big Data, Scoring und das Internet der Dinge*, (Beiträge zur Verbraucherforschung Band 5, Verbraucherzentrale NRW 2016).

⁸ Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016), S. 67-69.

⁹ S. z.B. N.N., „Der Digitale Mensch“, (2016), *Spektrum Kompakt Der digitale Mensch*; auch: Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 1-2.

¹⁰ Dazu Wisman, „Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things“, (2013), *European Journal of Law and Technology*, Vol. 4, No. 2

sondern auch für ursprünglich nicht bei der Datenerhebung vorgesehenen Profiling von Kunden.

Eine umfassende Darstellung aller Problembereiche ist in einem Working Paper nicht möglich. Vielmehr ist das Ziel, die Hauptdebatten darzustellen, um aufzuzeigen, wo die größten zu bewältigenden Problemen liegen. Als inhaltliche Restriktion soll außerdem noch erwähnt sein, dass es nicht um das Erstellen von Kundenprofilen o.ä. (Scoring) gehen soll. Der Sachverständigenrat wird sich mit diesem Thema in 2017 beschäftigen.

B. Vorverständnis & Aufbau

I. Privatsphäre als schützenswertes Gut im Technikzeitalter

Dem Papier liegt das Vorverständnis zugrunde, dass die Privatsphäre ein schützenswertes Gut ist, das sowohl einen intrinsischen Wert hat als auch anderen Zielen, wie der verfassungsrechtlich garantierten Freiheiten, dient. Das Konzept der Privatsphäre umfasst nicht nur die Unantastbarkeit des Körper und Geistes, sondern auch den Schutz und das Geheimnis persönlicher Daten, das Recht „in Ruhe gelassen zu werden“, die vernünftige Vertraulichkeit von Kommunikation zwischen Personen unabhängig davon wo, wie und in welcher Form sie stattfindet, sowie die Freiheit vor unzulässiger, ungesetzlicher oder unverhältnismäßiger Überwachung, ob in der Öffentlichkeit oder in privaten Orten.¹¹ Die Privatsphäre ist damit nicht nur für freie Meinungsäußerung, Bewegungsfreiheit, Gleichheit und damit für demokratische Teilhabe unabdinglich.¹² Sie garantiert auch die Freiheit von Fremdbestimmung (z.B. durch die Kontrolle von Datenflüssen) und die persönliche Freiheit, autonome Entscheidungen zu fällen.¹³

Die Relevanz der Privatsphäre schlägt sich besonderes im internationalen Wissenschafts- und Policy-Diskurs nieder. Während auf der einen Seite Unternehmensinteressen stehen, die das Ende der Privatsphäre ankündigen („You have zero privacy anyway. Get over it.“¹⁴; Privatsphärenschutz sei keine „social norm“ mehr¹⁵), gibt es zahlreiche Initiativen, die Privatsphärenschutz zum Beispiel mit technischen Mitteln propagieren und erforschen (dazu unten). Parallel dazu gibt es Anstrengungen für Grundrechte-Deklarationen im Internetzeitalter.

In diesem proklamiert z.B. die Deklaration der Internetrechte des Italienischen Parlaments¹⁶ neben dem Recht auf informationelle Selbstbestimmung, Datenschutz, auf Zugang zum Internet, auf Wissen und Bildung, auf und dem Recht auf Vergessenwerden weitere

¹¹ So Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 16.

¹² Dazu *ibid.*, S. 20-21.

¹³ Diese Auffassung ist auch im Volkszählungsurteil des BVerfG (BVerfG Urteil vom 15.12.1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil)) artikuliert und wird im Verlauf diskutiert.

¹⁴ <<http://archive.wired.com/politics/law/news/1999/01/17538>> (zuletzt abgerufen am 30.11.2016).

¹⁵ <<https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>> (zuletzt abgerufen am 30.11.2016).

¹⁶ <http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_in_glese.pdf> (zuletzt abgerufen am 30.11.2016).

Grundsätze, wie Netzneutralität und Nichtdiskriminierung. Darüber hinaus postuliert Artikel 9 das Recht seine eigene Identität im Internet aufzubauen; dazu gehört auch das Recht auf Aufklärung über Algorithmen und Wahrscheinlichkeitsmodelle, die zum Aufbau und der Weitergabe von Profilen benutzt werden. Mit ihrer grundlegenden Gewichtung von Internetrechten, gegenüber denen andere Bedürfnisse wie Sicherheit und das Funktionieren des Markts auch zurücktreten können, bezieht die Deklaration klar Stellung gegen die Verflechtung von unwiderstehlichem technischen Fortschritt und dem Vorrang ökonomischer Logik.¹⁷

In Bezug auf technischen Fortschritt erkennt dieses Papier an, dass die sich ausbreitende Nutzung sog. Privacy-Invasive Technologies (PITs) das IoT prägt. Der Begriff der PITs bezieht sich auf technische Produkte (Hardware und Software), welche eine besondere Gefahr für die Privatsphäre darstellen und dafür benutzt werden kann, das Recht auf Privatsphäre und das Recht auf Datenschutz zu verletzen.¹⁸ Dazu gehören insbesondere auch Techniken, die menschliche Sinne verstärken oder ersetzen, wie z.B. Identifikationstechnik und erweiterte Bildertechnik. Die Gefahren für die Privatsphäre, die von neuen PITs ausgehen, sind außerdem radikal, einzigartig und neu und betreffen alle Dimensionen der Privatsphäre. Wie bereits oben erwähnt, unterliegen viele IoT-Geräte darüber hinaus einem „function creep“, der eine oftmals unvorhergesehene Ausweitung der Funktionen der Geräte umschreibt. Damit sind die Eingriffe in die Privatsphäre durch PITs nicht nur bereits von vornherein angelegt, sondern auch unvorhersehbar. Aus diesen Gründen müssen, auf der normativen Ebene, Regeln zum Schutz der Privatsphäre die Eingriffe in die Privatsphäre durch technische Geräte und Komponenten thematisieren.

II. Hypothese und Aufbau des Papiers

Die diesem Papier zugrundeliegende Hypothese ist, dass Privatsphärenschutz im IoT durch technische Maßnahmen erfolgen kann, die rechtliche Maßnahmen unterstützen. Eine Durchsicht der Literatur im Bereich von Recht und Technik in dieser Hinsicht belegt, dass entsprechende Diskussionen um Privacy by Design, Privacy by Default und sog. PETs (Privacy-Enhancing Technologies) bereits seit zwei Jahrzehnten stattfinden.

Die Untersuchung der Hypothese erfolgt in mehreren Schritten. Zunächst werden die Datenströme im IoT sowie ihre grundrechtliche sowie einfachgesetzliche Relevanz dargestellt (C). Danach wird untersucht, inwiefern die bestehenden rechtlichen Normen,

¹⁷

<http://www.camera.it/application/xmanager/projects/leg17/attachments/upload_file/upload_files/000/000/194/Internet_Lib_inglese.pdf> (zuletzt abgerufen am 30.11.2016); damit geht die Deklaration auch über die existierenden menschen- und grundrechtlichen Anforderungen hinaus. Die Charter der Grundrechte der EU stipuliert in Artikel 7 die Achtung des Privat- und Familienlebens, des Familienlebens, und Kommunikation. Artikel 8 Charter schreibt den Schutz personenbezogener Daten fest. Art. 8 II Charter legt fest, dass neben der Einwilligung in bzw. gesetzlicher Grundlage für Datenverarbeitung, auch eine Zweckbindung „nach Treu und Glauben“ vorliegen muss. In dieser Hinsicht normiert die Charter ein Verständnis einer „schwachen“ Zweckbindung von Datenerhebungen, die v.a. im privaten Bereich keine Bindung über Treu und Glauben i.S.e. Selbstbindung hinaus.

¹⁸ Dazu Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 50.

insbesondere die des BDSG und der DSGVO die Privatsphäre der Betroffenen schützen und welche Probleme bestehen; es wird zwischen dem materiell-rechtlichen Normrahmen (D) und dem prozessualen Rechtsrahmen zur Durchsetzung der Verbraucherrechte (E) unterschieden. Am Beispiel der Home Connect App (HCA), über die Haushaltsgeräte verschiedener Hersteller verbunden und gesteuert werden können, werden die Normen und Probleme illustriert. Dann werden rechtliche und technische Lösungsansätze dargestellt (F).

C. Daten im IoT

Bei vernetzten Produkten ergeben sich verschiedene datenschutzrechtlich erhebliche Prozesse, die verschiedene Schutzgüter betreffen können. Das Smart Home eignet sich besonders für eine umfassende Darstellung, da im Smart Home verschiedene Anwendungsfelder und Produktkomponenten zusammenkommen. Generell besteht das Smart Home aus Sensoren, Aktoren, Speichermedien und Kommunikationskanälen, über die Daten zur individuellen Steuerung der verschiedenen Komponenten in Kommunikations-, Betriebs- und Haushaltstechnik ausgetauscht werden.¹⁹ Diese Techniken im Smart Home sind PITs, da sie darauf angelegt sind, Handlungen von Verbrauchern in ihrem privaten Bereich zu erfassen und entweder selbst auszuwerten oder sie zur Auswertung an andere Systeme übermitteln.

I. Datenströme im Smart Home

Betriebstechnisch kann eine Infrastruktur vorliegen mit der Energie- oder Lüftungsbedarf gesteuert wird. Zum Beispiel ermittelt moderne Heiz- und Klimatechnik durch Daten über die Anzahl der Personen im Raum den erforderlichen Bedarf an Heizleistung und kann dabei auch individuelle Präferenzen der Anwesenden beachten. Im Bereich der Haushaltstechnik werden zum Beispiel Backöfen, Kühlschränke, Waschmaschine, Kaffeevollautomaten miteinander vernetzt. So kann z.B. über die Home Connect App (HCA) der Backofen im Einklang mit einem ausgewählten Rezept vorgeheizt werden oder der Spülmaschinenvorgang verfolgt werden. Benachrichtigungen werden versandt, wenn die Spülmaschinentabs zu Neige gehen und über eine Kühlschrankkamera lässt sich der Inhalt des Kühlschranks einsehen.

Der Journalist Marco Maas hat 130 Geräte in seinem Smart Home, darunter Lampen, Steckdosen, Rauchmelder, Bewegungsmelder, Schließsensoren, Smart-Bed, Audioboxen und Luftqualitätsmesser.²⁰ 90 Sensoren generieren etwa 600 MB Daten pro Tag.²¹ Er benutzt das Amazon Echo, ein Audio-Gerät, das über einen sprachgesteuerten Computer mit Wi-Fi und Bluetooth eine Audio-Schnittstelle zu verschiedenen Internetdiensten

¹⁹ S. dazu Skistims, *Smart Homes: Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, (Nomos Verlag, 2016), S. 68ff.

²⁰ Zu seinem Smart-Home Projekt, <<http://www.spiegel.de/netzwelt/gadgets/smart-home-in-st-pauli-technik-in-jeder-ecke-a-1061903.html>> (zuletzt abgerufen am 30.11.2016).

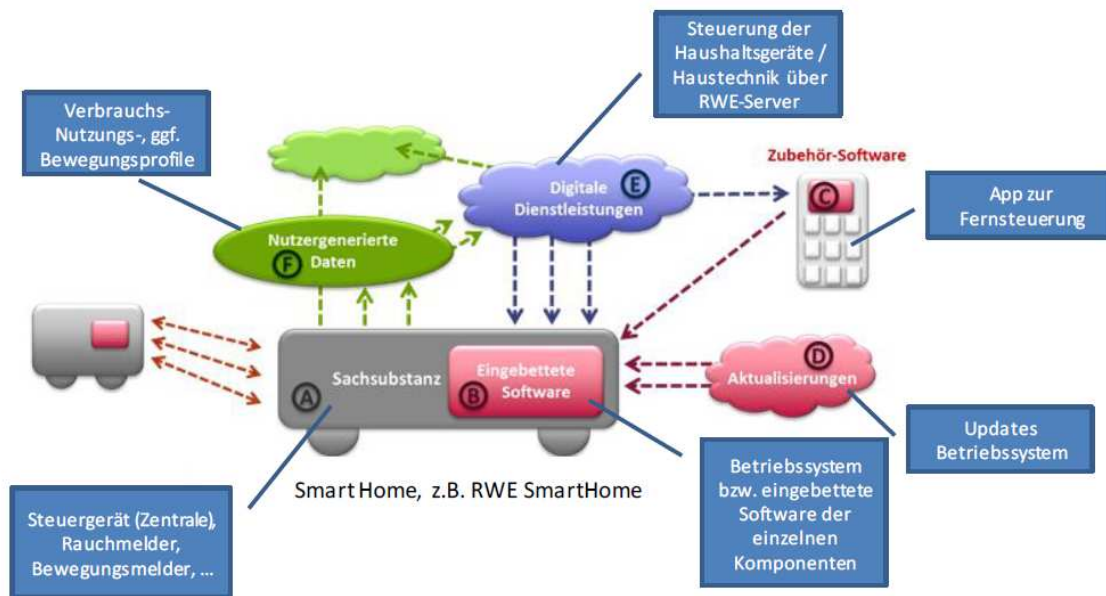
²¹ Sensoren sind Funkteilnehmer, die eine physikalische Größe aufnehmen und in eine elektrische Größe umwandeln; diese Größe wird digitalisiert und in einen Datensatz eingefügt, der an andere Funkteilnehmer gesendet werden kann.

²² Beispiele aus dem Smart Home sind Rauchmelder, Bewegungsmelder oder Heizkörperthermostate.

(Musikdienstleister, Internetpodcasts, etc.) anbietet. Auch Google hat mit seinem Google Home eine Art digitalen Assistenten geschaffen, der auf Zuruf Musik abspielt, Licht ein- und ausschaltet und Informationen bereitstellt.

Die verschiedenen Produkte und Produktkomponenten im Smart Home lassen sich wie folgt schematisch darstellen:

Abbildung 1: Anwendungsfelder im Smart Home²²



Zum Beispiel senden Bewegungsmelder (Sachsubstanz A) Daten an andere Produkte wie zum Beispiel Lichtschalter oder Heizungsanlagen. Mit WLAN-Anschluss ausgestattete Waschmaschinen sind über Apps (Zubehör-Software C) fernsteuerbar. Der Smart-TV sendet über sein Betriebssystem (B), welche über Updates (D) aktualisiert wird, oft auch zwangsweise, die mit Sprachsteuerung interpretierten Befehle an einen digitalen Dienstleister wie zum Beispiel Online-Videotheken (E). Nutzergenerierte Daten (F) sind für die Funktion smarter Produkte von entscheidender Bedeutung. Sie stellen die Basis für die Funktionsweise aller smarten Produkte oder von digitalen Dienstleistungen dar und werden oft in einer Cloud gespeichert.

Die Generierung von Daten erfolgt im Smart Home entweder durch direkte oder indirekte Steuerung. Allerdings wird die direkte Steuerung technischer Systeme (z.B. durch die bewusste Eingabe von Befehlen durch Tastatur, Maus oder kapazitive Displays) durch indirekte Interaktionstechniken zwischen Mensch und Maschine, bei denen natürliche Handlungen des Nutzers durch das System als Systembefehle interpretiert werden, und der

²² Gabriel et al, „Eigentums- und Besitzverhältnisse im Internet der Dinge: Markstudie“, (Institut für Innovation und Technik (iit) 2016), erstattet von Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016), S. 6.

vollständigen Automatisierung von Entscheidungsprozessen mehr und mehr abgelöst.²³ Ein Beispiel für indirekte Steuerung im Smart Home ist die Mimiksteuerung von Musikanlagen oder Lichtquellen, durch die angepasst auf bestimmte Emotionen reagiert wird (Dämpfung des Lichts, Einspielen bestimmter Musik) oder das Rausgehen aus einem Raum, was das Ausschalten des Lichts zur Folge hat.

Die Komplexität der Datenübertragungen und –nutzungen wurden auch in dem vom LG Frankfurt entschiedenen Samsung Smart TV – Fall²⁴ deutlich. Die Verbraucherzentrale NRW hatte in ihren der Klage vorausgehenden Versuchen drei verschiedene Datenübertragungswege im Samsung Smart TV identifiziert: Zum einen über einen im Fernseher integrierten Webbrowser und das HbbTV-Netzwerk, über welchen interaktive Inhalte und personalisierte Werbung an den Kunden zu senden; zum anderen über das sog. SmartHub (einer Art digitalen Videothek), über welche persönliche Programmvorschau übermittelt werden kann und der Nutzer Apps wie Facebook oder Skype installieren kann; schlussendlich werden Daten wie die IP-Adresse auch an einen Samsung Server übertragen, damit aktuelle Firmenware heruntergeladen oder die Spracheinstellungen bestimmt werden können.

Auch die Datenschutzerklärung der Home Connect App (HCA-Datenschutzerklärung),²⁵ welche Hausgeräte unterschiedlicher Marken steuern kann, macht die Relevanz und Art der Daten für die Funktion des Smart Homes klar. Über die App werden bestimmte Daten erhoben und gespeichert, z.B. Nutzer-Stammdaten / Bestandsdaten (E-Mail-Adresse, Geburtsdatum, Spracheinstellungen etc.), Geräte-Stammdaten (Seriennummer und Netzwerksadapternummer), Geräte-Nutzungsdaten (voreingestellte Grundeinstellungen, Temperaturänderungen, Schließen der Tür, etc.), sowie App-Nutzungsdaten (verwendete Funktionalitäten, Klickverhalten, Auswahl in Dropdown-Menüs, etc.).

II. Grundrechtliche Relevanz

Die technischen Systeme, die im Smart Home zum Einsatz gelangen sind darauf angelegt, persönliche Daten und Informationen über Aktivitäten der Verbraucher zu sammeln und direkt oder indirekt auszuwerten. Damit stellen diese Systeme PITs da, die eine besondere Gefahr, wenn nicht sogar schon einen technisch angelegten Eingriff in die Privatsphäre hervorrufen.

Die Datenerhebungen und –übertragungen im Smart Home sind grundrechtlich relevant.²⁶ Verfassungsrechtlich ist der Schutz im Recht auf informationelle Selbstbestimmung

²³ Dazu im Detail Skistims, *Smart Homes – Rechtsprobleme intelligenter Haussysteme unter besondere Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, (Nomos Verlag, 2016), S. 60ff.

²⁴ LG Frankfurt am Main, Urteil vom 10.06.2016, 2-03 O 364/15.

²⁵ Die Datenschutzerklärung kann in Annex I eingesehen werden.

²⁶ Dazu Skistims, *Smart Homes, Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, (Nomos Verlag, 2016), Kapitel 6. Die folgenden Ausführungen basieren auf diesem Kapitel mit seinen weiteren Nachweisen, soweit nicht anders angegeben.

verankert.²⁷ Die erstmalige Erhebung, weitere Verarbeitung und sonstige Verwendung personenbezogener Daten fällt in den Schutzbereich der informationellen Selbstbestimmung, welche einen Teil des allgemeinen Persönlichkeitsrecht i.S.d. Art. 2 I i.V.m. Art. 1 I GG darstellt. Im Volkszählungsurteil des BVerfG auf Grundlage der Art 2 I und 1 I GG wurde das Recht auf informationelle Selbstbestimmung konkretisiert. Es umfasst das Recht des Einzelnen, grundsätzlich „selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Informationelle Selbstbestimmung ist seitdem die notwendige Vorbedingung tatsächlicher Freiheit, sowohl im Verhältnis zum Staat als auch im Verhältnis zu privaten Akteuren.²⁸

Der Schutzbereich des allgemeinen Persönlichkeitsrechts umfasst auch die Möglichkeit durch einen Zugriff auf das System einen Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild der Persönlichkeit zu erhalten.²⁹ Im Smart Home geht es insbesondere um die Gewinnung von Persönlichkeitsprofilen durch die Verknüpfung von Kontextdaten (Häufigkeit, Art und Intensität der Nutzung oder soziale und innere Zustände der Nutzer) aus Sensorik, intuitiven Benutzerschnittstellen und spezifischen Algorithmen, durch die auch allein stehende bedeutungslose Daten einen neuen Stellenwert zur Profilierung erhalten können. Damit lassen sich zahlreiche Rückschlüsse auf die tägliche Lebensführung, mediales Konsumverhalten oder Eigenarten des Haushalts ableiten, wie z.B. Arbeitszeiten, Schulzeiten, Krankenhausaufenthalte, Urlaubsreisen. Dabei reicht die Möglichkeit der zweckwidrigen Verwendung der generierten Daten für die Eröffnung des Schutzbereichs des allgemeinen Persönlichkeitsrechts in Form des „Computergrundrechts“ aus.

Außerdem umfasst Art. 2 I i.V.m. Art. 1 I GG das Recht auf die Vertraulichkeit und Sicherheit informationstechnischer Systeme, welches das BVerfG in seiner Online-Überwachungsentscheidung³⁰ ableitete. Demnach hat der Einzelne ein grundrechtlich erhebliches Schutzbedürfnis für eigengenutzte komplexe informationstechnische Systeme gegenüber der Möglichkeit, dass sie infolge ihrer Vernetzung infiltriert, ausgespäht und manipuliert werden, da der Einzelne immer mehr auf die Nutzung informationstechnischer Systeme angewiesen sei und vertrauen müsse. Probleme von Überwachung und ungewollter Identifikation kommen im Smart Home insbesondere durch die Benutzung von RFID (Radio Frequency Identification) und anderen kabellosen Techniken auf, die die Transmission von Informationen ermöglichen.³¹ Die Anfälligkeit von Smart-Home-Geräten sind mit Hinweis auf einfach mögliche Abhörung, Speicherausspähung oder Malware

²⁷BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83 (Volkszählurteil)

²⁸ Buchner, *Informationelle Selbstbestimmung im Privatrecht*, (Mohr Siebeck, 2006), S. 87.

²⁹BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07 - BVerfGE 120, 274, 314 (Online Durchsuchungen).

³⁰BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07 - BVerfGE 120, 274, 306ff (Online Durchsuchungen).

³¹

<<https://poseidon01.ssrn.com/delivery.php?ID=907117081025013120100021005065120072026032046009065078108122096067126125070087013025032052096126039015001115024021092004103026022053075009102101080087001110065003021111125080068083071065023075083088119006080111024028086006126104073119008065088&EXT=pdf>> (zuletzt abgerufen am 30.11.2016).

Attacken inzwischen von IT-Sicherheitsexperten untersucht.³² Insbesondere durch Geräte, die nicht durch ein persönliches, sondern nur ein werkseitig gesetztes Passwort geschützt sind, kann Schadsoftware übernommen und für Cyberangriffe missbraucht werden.³³ Durch einfache Eingabe des Administratoren-Befehls „admin/admin“ können werkskonfigurierte Sicherheitseinstellungen in Geräten systematisch ausgehebelt werden. Dabei wird insbesondere die sicherheitstechnische Anfälligkeit von Cloud-Diensten ausgenutzt.³⁴ Entsprechende Gesetzesinitiativen zur Änderung des StGB werden diskutiert.³⁵

Über das allgemeine Persönlichkeitsrecht hinaus sind weitere Grundrechte für Datenerhebungen und –übertragungen im Smart Home einschlägig. Die Vertraulichkeit der Inhalte der Kommunikation und ihrer Umstände ist von dem Schutz laufender Kommunikationsvorgänge des Art. 10 I GG erfasst, wenn Individualkommunikation der Nutzer über telekommunikationsbasierte Übertragungstechniken durch das Haussystem initiiert oder empfangen wird, sofern diese über rein automatische vermittelten Austausch von Informationen zur technischen Zwecken hinaus geht. Damit bildet Art. 10 I GG einen speziellen Bereich der Privatsphäre ab, dessen Schutzbereich in dem Moment endet, in dem der Übertragungsvorgang beendet ist. Dagegen bleibt Art. 2 I i.V.m. Art. 1 I GG anwendbar, insofern als dass ein Herrschaftsverhältnis (zum Beispiel durch die Nutzung eines stationären Systemanschlusses oder Handys die sich in der Wohnung befinden) an den gespeicherten Daten besteht. Außerdem kann das Eigentumsrecht des Nutzers gem. Art. 14 GG berührt sein, soweit der Nutzer des Anschlusses Eigentümer des Hauses und damit auch des Haussystems ist.

III. Einfachgesetzlicher Datenschutz: BDSG, TMG

Einfachgesetzlich ist das Recht der informationellen Selbstbestimmung über Daten durch das BDSG geschützt. Regelungsziel des Datenschutzes ist dabei nicht der Schutz von Daten als solchen, sondern der Schutz des einzelnen Betroffenen vor Gefahren für die freie Entfaltung seiner Persönlichkeit.³⁶ Das BDSG nennt als Schutzgegenstand das „Persönlichkeitsrecht“ (§1 Abs. 1 BDSG).³⁷ Beim BDSG handelt es sich sowohl um ein

³² Mit Bezug auf Smart TV Apps:

<<https://www.nds.rub.de/media/nds/veroeffentlichungen/2015/08/31/SmartTvAttacks.pdf>> (zuletzt abgerufen am 30.11.2016).

³³ <<http://fm4.orf.at/stories/1773571/>> (zuletzt abgerufen am 30.11.2016)

³⁴ So zuletzt bei einem Denial-of-Service Angriff im IoT im Oktober 2016, s. z.B.:

<<http://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/>> (zuletzt abgerufen am 30.11.2016).

³⁵ Bundesregierung, *BT-Drucksache 18/10182 Gesetzentwurf des Bundesrates, Entwurf eines Strafrechtsänderungsgesetzes – Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – Digitaler Hausfriedensbruch*; (Drucksache 18/10182 02.11.2016), abweichende Stellungnahme der Bundesregierung auf S. 30; die rechtlichen Implikationen bleiben in diesem datenschutzrechtlichen Working Paper ausgeklammert.

³⁶ Schulz/Gola, *Gesamtes Arbeitsrecht Nomos Kommentar*, Boecken/Düwell/Diller/Hanau (Hrsg.), 2016, Nomos Verlag, Rn. 1 zu § 1 BDSG.

³⁷ Gola/Klug/Körffer, *Kommentar zum Bundesdatenschutzgesetz*, Gola/Schomerus (Hrsg.) 12. Auflage 2015, C.H. Beck Verlag, Rn. 6 zu § 1 BDSG.

Schutzgesetz³⁸ zugunsten des Rechts auf informationelle Selbstbestimmung als auch um ein Eingriffsgesetz.³⁹

Was die Art der Daten angeht, müssen Bestands- und Nutzungsdaten unterschieden werden. Bestandsdaten i.S.d. § 14 TMG sind solche personenbezogenen Daten des Nutzers, die für die „Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über Telemediendienste erforderlich sind. Damit sind also Daten gemeint, wie z.B. Name, E-Mail-Adresse, Postadresse oder Geburtsdatum.⁴⁰ Dagegen beziehen sich Nutzungsdaten i.S.d. § 15 TMG auf solche personenbezogenen Daten, die zur Ermöglichung der Nutzung und Abrechnung notwendig sind. Dazu gehören Merkmale zur Identifikation, Angaben über Umfang der Nutzung, sowie über die in Anspruch genommenen Telemedien, also Seitenabrufe oder Downloads. Solche Daten sind im IoT besonders interessant für Unternehmen, weil sich durch sie Rückschlüsse auf die Präferenzen der Nutzer ziehen lassen. Ob solche Daten, die nicht unmittelbar für die Zwecke in §§ 14, 15 TMG notwendig sind - also sog. Inhaltsdaten wie z.B. freiwillige Angaben wie Geschlecht, Anzahl der Kinder, Beziehungsstatus oder persönlichen Vorlieben wie Musikgeschmack und Hobbys - auch Nutzungsdaten i.S. dieser Vorschriften sind, ist umstritten: Während ein Teil der Literatur diese als Unterfall der Nutzungsdaten i.S.d. § 15 TMG ansieht, wenden andere §§ 27ff BDSG an.⁴¹

Tabelle 1: Übersicht - Datenerfassungen und rechtliche Einordnung

Datenerfassungen im IoT	Grundrechte	Einfachgesetzliche Normen
- Erhebung & Verwendung persönlicher Daten - Gewinnung von Persönlichkeits- und Nutzungsprofilen - Problem: Ausspähung, unzulässige Weitergabe an Dritte	Informationelle Selbstbestimmung, Art. 2 I i.V.m. Art. 1 I GG	- BDGS, TMG, TKG (für Bestands- und Nutzungsdaten) - BGB: AGB, vertragliche Haupt- und Nebenpflichten
- Abhörung von Sensoren - Problem: Speicherausspähung, z.B. in der Cloud; Malware-Attacken, durch Implantierung von Viren in Software	Vertraulichkeit und Sicherheit informationstechnischer Systeme, Art. 2 I i.V.m. Art. 1 I GG	- Geräte- und Produktsicherheitsgesetz (GPSG) - Bereichsspezifische Vorschriften, geändert durch IR-Sicherheitsgesetz: z.B. TMG, TKG - BGB: AGB, vertragliche Haupt- und Nebenpflichten
- Übermittlung von Sprachnachrichten, schriftlichen Nachrichten, Bildern, Videos an Cloud-Dienste u.a. Speichermedien - Problem: Ausspähung,	Vertraulichkeit der Information, Art. 10 I GG	- BDSG, TMG, TKG (Nutzungsdaten)

³⁸ Ibid., Rn. 3 zu § 1 BDSG.

³⁹ Ibid., Rn. 16 zu § 1 BDSG.

⁴⁰ Bauer, „Personalisierte Werbung auf Social Community-Websites - Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen“, (2008), *MultiMedia und Recht*, Heft 7, S.435-438, S. 436.

⁴¹ Zu dem Meinungsstreit ibid., S. 436.

unzulässige Weitergabe an Dritte		
- Inhalt von Bildern und Videos; Übermittlung an Cloud-Dienste u.a. Speichermedien - Problem: Ausspähung, unzulässige Weitergabe an Dritte	Art. 2 I i.V.m. Art 1. I GG,	- UrhG, KUG (Recht am eigenen Bild)

Welche bereichsspezifischen Regelungen im konkreten Fall anwendbar sind, bestimmt sich nach der Art der Datenerhebung. Nach dem sogenannten Schichtenmodell⁴² ist ausschlaggebend welche Ebene funktionell betroffen ist.⁴³ Bezüglich des Inhalts sind die Vorschriften des BDSG zu beachten, für die Transportbehälterebene gilt das TMG und der Datentransport selbst unterliegt dem TKG.⁴⁴ Darüber hinaus dient das BDSG auch in Fällen in denen das TKG oder TMG einschlägig ist, als Auffangtatbestand und ist sodann subsidiär anwendbar.⁴⁵ In diesem Papier konzentrieren wir uns auf die Vorschriften des BDSG und der TMG und TKG.

D. Zulässigkeit von Datenerhebungen im IoT

I. Grundsätze des Datenschutzes

Die rechtlichen Rahmenbedingungen für den Schutz der Privatsphäre in Deutschland sind von internationalen Richtlinien beeinflusst. Die OECD Richtlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Datenverkehr stellen Grundsätze auf, die auf nationaler Ebene angewandt werden sollen. Diese Grundsätze sind im Einzelnen:

- Grundsatz 7 - Collection Limitation Principle:
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Grundsatz 8 - Data Quality Principle:
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- Grundsatz 9 - Purpose Specification Principle:
The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- Grundsatz 10 -Use Limitation Principle:

⁴² Schaar, *Datenschutz im Internet: Die Grundlagen*, (C.H. Beck Verlag, 2002), Rn. 247 ff.

⁴³ Ulbricht, *Praxishandbuch Big Data Wirtschaft – Recht – Technik*, Dorschel (Hrsg.) (Springer Gabler Verlag, 2015), S. 175.

⁴⁴ Ibid.

⁴⁵ Ibid.

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except with the consent of the data subject; or by the authority of law.

- Grundsatz 11 - Security Safeguards Principle:

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

- Grundsatz 12 -Openness Principle:

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- Grundsatz 13 - Individual Participation Principle:

Individuals should have the right:

- to obtain from a data controller, or otherwise, confirmation of
- whether or not the data controller has data relating to them;
- to have communicated to them, data relating to them
 - within a reasonable time;
 - at a charge, if any, that is not excessive;
 - in a reasonable manner; and
 - in a form that is readily intelligible to them;
- to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

- Grundsatz 14 -Accountability Principle:

A data controller should be accountable for complying with measures which give effect to the principles stated above.

II. Anwendbarkeit und Grundsätze des BDSG

Das BDSG ist sachlich bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten anwendbar, §1 II BDSG. Für die Verarbeitung personenbezogener Daten ist gem. des Verbots mit Erlaubnisvorbehalt in § 4 I BDSG entweder eine gesetzliche Erlaubnis oder die Einwilligung des Betroffenen erforderlich. Dieser Ansatzpunkt reflektiert das grundlegende Verbotsprinzip im deutschen Datenschutzrecht.⁴⁶ Soweit eine Datenvermeidung nicht möglich ist, gilt das Gebot der Datensparsamkeit.⁴⁷ Beim BDSG handelt es sich sowohl um ein Schutzgesetz⁴⁸ zugunsten des Rechts auf informationelle Selbstbestimmung als auch um

⁴⁶Schulz, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition, C.H. Beck Verlag 2016, Einleitung zu § 3a BDSG.

⁴⁷Grapentin, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 139 zu § 34 des Datenschutzes.

⁴⁸Gola/Klug/Körffner, *Kommentar zum Bundesdatenschutzgesetz*, Gola/Schomerus (Hrsg.) 12. Auflage 2015, C.H. Beck Verlag, Rn. 3 zu § 1 BDSG.

ein Eingriffsgesetz.⁴⁹ Insofern stellt das BDSG ein Gesetz dar, in dem das Grundrecht der informationellen Selbstbestimmung konkretisiert ist, auch Hinblick auf mögliche Beschränkungen durch Rechte anderer.

1. Schutzbereich: Personenbezogene Daten

Gem. § 1 Abs. 1 BDSG ist der Anwendungsbereich des BDSG dann eröffnet, wenn es sich um personenbezogene Daten handelt. Im Umkehrschluss bedeutet das, dass andere nicht-personenbezogene Daten nicht den Regelungen und Vorgaben zum Umgang mit den im BDSG relevanten Daten unterliegen. Insbesondere gilt für sie nicht das Verbotsprinzip, da sie generell nicht als über das BDSG geschützt angesehen werden. Vielmehr kommen hier andere Regelungen in Betracht.

Der Begriff der personenbezogenen Daten ist weit zu fassen: Daten sind personenbezogen, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind⁵⁰ oder diese Zuordnung zumindest mittelbar erfolgen kann (personenbeziehbare Daten).⁵¹ Klar zuzuordnen sind der Name, die Telefonnummer sowie Kreditkarten- oder Personalnummern. Personenbezogene Daten sind aber auch Kontodaten, Kfz-Kennzeichen, das Aussehen, die Kundennummer oder die Anschrift zählen zu den personenbezogenen Daten.⁵² Das gilt selbst dann, wenn die Zuordnungsinformationen nicht allgemein bekannt sind. Entscheidend ist lediglich, dass es möglich ist, die Daten mit nicht unverhältnismäßig großem Aufwand einer bestimmbar Person zuzuordnen.⁵³ Zu dieser Art personenbezogener Daten gehören u.a. statische und dynamische IP-Adressen.⁵⁴

Bestimmbar personenbezogene Daten sind auch solche, die mithilfe von Referenzdaten einer Person zugeordnet werden können, wie zum Beispiel statistische und dynamische IP-Adressen oder Cookies, da diese als Identifikatoren zu natürlichen Personen im Internet genutzt werden können; dabei kommt es nicht auf die Identität oder Intentionen der verantwortlichen Stelle an.⁵⁵ Auch Wahrscheinlichkeitsaussagen, wie zum Beispiel errechnete Kreditwürdigkeit oder Prognosen über zukünftiges Nutzer- oder Kaufverhalten oder Kreditwürdigkeit, sind personenbezogene Daten; dies beinhaltet auch die Zuordnung zu bestimmten Nutzer- oder Käufertypen oder Kaufkraftklassen.⁵⁶

Damit stellen die im Smart Home anfallenden Daten in großen Teilen personenbezogene Daten dar. Solche Daten sind beispielsweise Angaben über Alter oder Wohnort des

⁴⁹ Ibid., Rn. 16 zu § 1 BDSG.

⁵⁰ Ibid., Rn. 10 zu § 3 BDSG.

⁵¹ vgl. BGH, Urteil vom 15.05.1991 - VIII ZR 38/90 (Celle) - Formulklauseln in einem Wohnungsmietvertrag.

⁵² BAG, Beschluß vom 27.05.1986 - 1 ABR 48/84 (Düsseldorf) - Mitbestimmung bei Telefondatenerfassung.

⁵³ Gola/Klug/Körffer, *Kommentar zum Bundesdatenschutzgesetz*, Gola/Schomerus (Hrsg.) 12. Auflage 2015, C.H. Beck Verlag, Rn. 2-12 zu § 3 BDSG.

⁵⁴ Unlängst EuGH-Urteil in Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, EU:C:2016:779, para 49.

⁵⁵ Weichert, *Bundesdatenschutzgesetz Kompaktcommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage 2016, Bund Verlag, Rn. 14-15 zu § 3 BDSG mit weiteren Nachweisen.

⁵⁶ Ibid., Rn. 18 zu § 3 BDSG mit weiteren Nachweisen.

Verbrauchers oder sein Nutzerverhalten und seine Präferenzen im Smart TV. In der Datenschutzerklärung der HCA unterfallen alle Datenkategorien personenbezogenen Daten, also die Nutzer- und Gerätestammdaten, aufgrund derer eine direkte Identifikation des Nutzer möglich ist, sowie die Geräte- und App-Nutzungsdaten, mithilfe derer Profilbildung ermöglicht wird. Für die Zwecke dieser Untersuchung kann dahingestellt bleiben, ob und inwiefern Geo-Daten personenbezogene Daten i.S.d. BDSG sind, da etwaige Bewegungsdaten im Smart Home immer im privaten Kontext anfallen und daher personenbezogen sind i.S.d. BDSG. Dies gilt insbesondere dann, wenn der Anbieter einer digitalen Dienstleistung im IoT ein über die Vertragserfüllung hinaus gehendes kommerzielles Ziel verfolgt.⁵⁷ Dies liegt daran, dass Geräte- und Nutzerdaten erst dann kommerziell wertvoll werden, wenn sie mit parallel erfassten Daten verknüpft werden (beispielsweise: Tageszeit + Nutzung oder Alter + Stromverbrauch); durch diese Verknüpfung wird die Rückverfolgung der Daten auf einzelne Personen einfacher möglich.

Anonymisierung nach Art. 3 VI BDSG hebt den Personenbezug von Daten auf; damit wird dann das BDSG unanwendbar.⁵⁸ Bei der Anonymisierung entfällt der Personenbezug entweder durch Löschung der Identifikationsmerkmale (für diesen Lösungsprozess ist das BDSG noch anwendbar). Daten sind jedoch nur dann anonym, wenn der Personenbezug nicht mehr herstellbar, also eine Re-anonymisierung nicht mehr oder, in Anbetracht der modernen Datenverarbeitung nur unter unverhältnismäßig großem Aufwand möglich ist.⁵⁹ Werden jedoch Daten von einer verantwortlichen Stelle ohne Personenbezug an Dritte weitergegeben, obliegt der weitergebenden Stelle die Verpflichtung, die Zwecke und Möglichkeiten der Verwendung durch den Empfänger und z. B. die Voraussetzungen für die Übermittlungstatbestände der §§ 28, 29 BDSG festzustellen.

2. Datenvermeidung und Datensparsamkeit

Nach den Grundsätzen der Datenvermeidung und Datensparsamkeit soll schon die Entwicklung und Auswahl von Datenverarbeitungssystemen und die Ausgestaltung der konkreten Datenverarbeitungsprozesse so umgesetzt werden, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden. Personenbezogene Daten sollen nach Möglichkeit gar nicht erst anfallen, wenn aber doch, soll die Anzahl so gering wie möglich gehalten werden.⁶⁰ Ein Datenverarbeitungsvorgang soll von den verantwortlichen Stellen demnach so datensparsam wie nur möglich ausgestaltet werden.⁶¹ Ziel ist nicht die

⁵⁷ Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016), S. 47.

⁵⁸ So die h.L., s. Dorner, „Big Data und Dateneigentum“, (2014), *Computer und Recht*, Band 30, Heft 9, S. 628.

⁵⁹ Gola/Klug/Körffner, *Kommentar zum Bundesdatenschutzgesetz*, Gola/Schomerus (Hrsg.) 12. Auflage 2015, C.H. Beck Verlag, Rn. 43-44 zu § 3 BDSG.

⁶⁰ Dieser Absatz basiert auf dem Dokument *Datenschutzgerechtes eGovernment*, S. 14

<http://www.bfdi.bund.de/SharedDocs/Publikationen/PM29-04HandreichungDatenschutzgerechtesGovernment.html>

(zuletzt aufgerufen am 30.11.2016).

⁶¹ Schulz, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition, C.H. Beck Verlag 2016, Rn. 36 zu § 3a BDSG.

Reduzierung der Datenmenge als solche, sondern die Reduzierung des Personenbezuges der genutzten personenbezogenen Daten.⁶²

Um dies zu erreichen sind zwei Möglichkeiten denkbar: Die Reduzierung der Quantität der verarbeiteten personenbezogenen Daten und die qualitative Verringerung der Eingriffstiefe. Das Prinzip der Datenvermeidung und Datensparsamkeit in § 3 S. 1 BDSG appelliert an die potenziellen verantwortlichen Stellen schon vor einer etwaig geplanten Datenerhebung und Datenverarbeitung und geht damit in zeitlicher Hinsicht über die Vorgabe des materiell-rechtlichen Erforderlichkeitsgrundsatzes hinaus.⁶³ In § 3 S. 2 BDSG wird das in Satz 1 zum Ausdruck gebrachte Prinzip der Datenvermeidung konkretisiert. Die Daten der Betroffenen sollen wenn möglich in anonymisierter oder pseudonymisierter Form erhoben oder verarbeitet werden.⁶⁴ Der Aufwand der dafür aufgewendet werden muss, muss nach § 3 S. 2 BDSG aber auch in angemessenem Verhältnis zum Erfolg stehen.⁶⁵ Die Gebote der Datenvermeidung / Sparsamkeit sind bei sämtlichen Formen der Verarbeitung personenbezogener Daten als übergeordneter Grundsatz zu beachten⁶⁶

3. Zweckgebundenheit

Das OECD Purpose Specification Principle besagt, dass Daten gelöscht oder zerstört werden müssen, sobald die Speicherung nicht mehr erforderlich ist. Das Prinzip ist deswegen von grundlegender Bedeutung, weil nur unter Angabe des Zwecks der Datenerhebung, eine informierte Einwilligung in die Datenerhebung überhaupt gegeben werden kann (zur Einwilligung, s.u.).

Gleichermaßen zielt das OECD Use Limitation Principle darauf ab, dass Daten nicht für Zwecke benutzt werden, die über die ursprünglichen Ziele der Datenerhebung hinausgehen. Darüber hinaus dient der Grundsatz der Verhinderung des sog. Function Creep, mit dem die Diskrepanz zwischen ursprünglichem Ziel der Datenerhebung und der tatsächlichen Verwendung der Daten beschrieben wird.⁶⁷

Im deutschen Recht ist die Zweckbindung als verfassungsrechtliches Datenschutzprinzip aus dem Volkszählungsurteil abzuleiten, in welchem das BVerfG den Gesetzgeber verpflichtet hat, die Verwendungszwecke personenbezogener Daten im Eingriffsgesetz bereichsspezifisch und präzise zu bestimmen. Dies bedeutet, dass jede Form der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch eine Behörde einer gesetzlichen Grundlage bedarf.⁶⁸

⁶² Ibid., Rn. 37 zu § 3a BDSG.

⁶³ Ibid., Rn. 40 zu § 3a BDSG.

⁶⁴ Gola/Klug/Körffer, *Kommentar zum Bundesdatenschutzgesetz*, Gola/Schomerus (Hrsg.) 12. Auflage 2015, C.H. Beck Verlag, Rn. 7 zu § 3a BDSG.

⁶⁵ Ibid., Rn. 7 zu § 3a BDSG.

⁶⁶ Schulz, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition, C.H. Beck Verlag 2016, Rn. 14 zu § 3a BDSG.

⁶⁷ Dazu Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 37-38.

⁶⁸ Dazu Härting, „Zweckbindung und Zweckänderung im Datenschutzrecht“, (2015), *Neue Juristische Wochenschrift*, Heft 45, S. 3265-3328, S. 3284.

Im BDSG wird die Zweckbindung der Datenerhebung, -nutzung und -verarbeitung zwar an vielen Stellen erwähnt, bleibt allerdings ohne praktische Bedeutung.⁶⁹ So führt z.B. die Festlegung eines Zwecks durch den Datenverarbeiter lediglich zu einer Selbstbindung nach Treu und Glauben; auch die Verpflichtung zur Information über den Verarbeitungszweck gem. § 4a I 2 BDSG führt nur zur Selbstbindung.⁷⁰

III. Zulässigkeit der Datenerhebung: Einwilligung und gesetzliche Erlaubnis

Für die Zulässigkeit von Datenerhebungen und – verarbeitungen im IoT kommt es nach dem BDSG grundsätzlich darauf an, ob entweder die Einwilligung des Betroffenen (§ 4 BDSG) oder eine gesetzliche Erlaubnis vorliegt (in Frage kommen im IoT insbesondere die Verwertung für geschäftsmäßige Zwecke, §§ 28, 29 BDSG). Die entsprechenden Vorschriften in der DSGVO sind Art. 6 I lit. a zur Einwilligung und lit. b zur Erfüllung von Geschäftszwecken.

1. Anforderungen an die datenschutzrechtliche Einwilligung: § 4a BDSG

Gem. § 4 I BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur aufgrund gesetzlicher Erlaubnis oder Einwilligung des Betroffenen zulässig. Die Anforderungen an die Einwilligung werden in §§ 4a BDSG, 13 TMG konkretisiert. In Art. 7 DSGVO sind ebenfalls Bedingungen für die Einwilligung festgeschrieben. Die Normen reflektieren das OECD Collection Limitation Principle.

a. Aufklärung

Rechtsgrundlage

Für die Wirksamkeit einer Einwilligung ist erforderlich, dass der Betroffene über die Datenerhebung selbst sowie den Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hingewiesen wird, § 4 a I S. 1 BDSG, § 13 I TMG. Dieser Norm kommt grundlegende Bedeutung zu, da ohne die entsprechende Information des Betroffenen dieser gar nicht weiß ob überhaupt Daten erhoben werden und ob er dem zustimmen möchte oder nicht. Die Bedeutung wurde auch in dem Samsung-Fall deutlich, in welchem das LG Frankfurt entschied, dass ein Unterlassungsanspruch gegen den Verkäufer des Samsung Smart-T V aufgrund einer Irreführung i.S.d. § 5a II, 8 UWG i.V.m. § 13 I TMG bestehe, da die Käufer der Samsung Smart-TV Geräte nicht darüber hingewiesen wurden, dass schon bei bloßem Anschluss des Geräts an das Internet die Gefahr besteht, dass personenbezogene Daten erhoben und verwendet werden.⁷¹ Die Verpflichtung zur Unterlassung traf den Verkäufer im Rahmen der Störerhaftung. Damit betont das LG Frankfurt die grundlegende Wichtigkeit der Informationspflicht als Ausfluss des Rechts auf informationelle Selbstbestimmung.⁷²

⁶⁹ Das gleiche gilt für Art. 6 lit. b) S. 1 EU-DSRL; dazu Härtling, „Zweckbindung und Zweckänderung im Datenschutzrecht“, (2015), *Neue Juristische Wochenschrift*, Heft, 45, S. 3265-3328, S. 3284.

⁷⁰ Gammann, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 39 zu § 14 BDSG.

⁷¹ LG Frankfurt am Main, Urteil vom 10.06.2016, 2-03 O 364/15, Entscheidungsgrund 6.

⁷² Ibid.

Die Einwilligung muss außerdem nach § 4a Abs. 1 Satz 2 BDSG bestimmbar sein. Bestimmbar ist die Einwilligung, wenn der Betroffene die Tragweite seines Einverständnisses erkennen kann, was wiederum dann der Fall ist, wenn dieser weiß unter welchen Bedingungen welche Daten genutzt werden.⁷³ Die Reichweite der Einwilligung geht also so weit, wie der Betroffenen durch Aufklärung in die Lage versetzt wird, Art, Bedeutung und Tragweite der Preisgabe seiner personenbezogenen Daten abzuschätzen.⁷⁴

§§ 4 a I S. 2 BDSG, 13 I TMG legen fest, dass der Betroffene über den „Zweck“ von Erhebung, Verarbeitung oder Nutzung aufgeklärt werden muss. Fraglich ist jedoch, ob weitergehende Informationen, wie z.B. mögliche Drittempfänger von Daten, auch von § 4a I S. 2 BDSG erfasst sind. Entgegen dem Wortlaut des § 4a I S. 2 BDSG, aber aufgrund einer Analogie zu § 13 I TMG wird eine breitere Auslegung erwogen, so dass der Betroffenen über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung zu unterrichten ist, um eine bewusste Einwilligungserklärung abgeben zu können.⁷⁵ Anderenfalls sei es für den Betroffenen nicht möglich, zu beurteilen ob die mit der Datenerhebung verfolgten Zwecke auch mit geringerer Erhebungsdichte erreicht werden könnten.⁷⁶ Die Analogie zu § 13 I TMG wird auch über eine richtlinienkonforme Auslegung gestützt: Art. 10 der EU-DSRL verpflichtet die Mitgliedstaaten, dafür Sorge zu tragen, dass der Betroffene Informationen über den für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung, sowie weitere Informationen, beispielsweise betreffend Datenempfänger, Freiwilligkeit der Beantwortung von Fragen, sowie das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich ihn betreffender Daten erhält, sofern dies notwendig ist, um eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Probleme

Im Hinblick auf die grundlegende Bedeutung der Aufklärung über Zweck und Umfang der Datenerhebungen mithilfe von IoT-Geräten, sind die unlängst veröffentlichten Ergebnisse eines „Privacy Sweeps“ des Global Privacy Enforcement Network (GPEN)⁷⁷ beunruhigend:

„A global investigation into the privacy conditions of more than 300 ‘Internet of Things’ smart devices has found alarming shortfalls in the management of personal data by developers and suppliers.

The study – involving twenty-five data protection authorities – looked at the ways in which companies communicated with their customers regarding the security of their

⁷³ Vgl. OLG Köln, Urteil vom. 17.6.2011 – 6 U 8/11, CR 2012, 130ff. = ITRB 2012, 10 (Karthäuser) Rz. 17

⁷⁴ Helfrich, *Handbuch Multimedia-Recht Rechtsfragen des elektronischen Geschäftsverkehrs*, Hoeren/Sieber/Holznapel (Hrsg.), (C.H. Beck Verlag, 2015), Rn 46 in 42. Ergänzungslieferung, Teil 16.1 Einführung und Grundbegriffe des Datenschutzes.

⁷⁵ So ibid., Rn 48 in 42. Ergänzungslieferung, Teil 16.1 Einführung und Grundbegriffe des Datenschutzes.

⁷⁶ So ibid., Rn 49-50 in 42. Ergänzungslieferung, Teil 16.1 Einführung und Grundbegriffe des Datenschutzes.

⁷⁷ Informationen von der Website des irischen Datenschutzbeauftragten:

<<https://www.dataprotection.ie/docs/23-9-2016-International-Privacy-Sweep-2016/i/1597.htm>> (zuletzt abgerufen am 30.11.2016). In Deutschland haben sich der Landesbeauftragte für den Datenschutz Baden-Württemberg und das Bayerische Landesamt für Datenschutzaufsicht beteiligt.

personal data. In Ireland, the Office of the Data Protection Commissioner (DPC) investigated nine devices, ranging from smart electricity meters to fitness trackers, and its national findings were broadly in line with global trends (See Note for Editors below).

The international report into company communications with customers about data privacy rights showed that:

- 72% failed to explain how customers could delete their information.
- 68% failed to properly explain how information was stored.
- 60% failed to adequately explain to customers how their personal information would be collected and processed.
- 38% failed to include easily identifiable contact details if customers had privacy concerns.

The regulatory authorities involved are now considering what action is to be taken against those who are found to be in breach of legislation.

John Rogers, Senior Investigations Officer, who coordinated the Irish sweep said:

“There can be no doubt as to the benefits of modern technology in our everyday lives, but the introduction of this technology must be done in a clear and transparent manner and not adversely impact on privacy rights. The findings of our sweep show that much more needs to be done to meet data protection standards.

“Companies making these devices must make it clear to consumers about how their personal information is being collected and used and how consumers may delete their information if they wish.

“The Office of the Data Protection Commissioner is planning to scale up investigative and audit work in this area in 2017 and we have already begun to schedule audits of devices in the technology sector. The purpose of these audits will be to gauge compliance with the Data Protection Acts and to work with companies to ensure that their products are meeting the required standards.”

The sweep was coordinated by the Global Privacy Enforcement Network (GPEN). GPEN is an informal network of data protection agencies from around the globe. Its aim is to foster cross-border cooperation among privacy regulators in an increasingly global market.”

b. Freiwilligkeit

Gemäß § 4 a Abs. 1 Satz 1 und 2 BDSG wird die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, wobei der Betroffene auf den vorgesehenen Zweck der Datenverarbeitung hinzuweisen ist. Gem. Artikel 2 lit h) der EU-Datenschutzrichtlinie 95/46/EG (EU-DSRL),⁷⁸ in deren Licht das BDSG interpretiert werden muss, ist die Freiwilligkeit sogar integraler Bestandteil der Definition von „Einwilligung“. Art 2 lit h) EU-DSRL legt fest, dass eine Einwilligung „ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage“ abgegeben sein muss.

⁷⁸ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L-281/ 31, 23.11.1995 S. 0031 – 0050.

Artikel 7 IV der DSGVO legt für die Bewertung der Freiwilligkeit außerdem die Einschätzung zugrunde, ob die Daten für die Erfüllung des Vertrages erforderlich sind. In dieser Hinsicht verschwimmen die Grenzen zwischen Datenerhebungen, die aufgrund von Einwilligung zulässig sind, und solchen, die in der Erreichung des Geschäftszwecks ihre gesetzliche Grundlage haben (§ 28 BDSG, dazu unten).

Bestimmtheit

Die Einwilligung muss daher „bestimmt“ sein, d.h. es muss deutlich sein, unter welchen Bedingungen welche Daten genutzt werden dürfen, damit der Betroffene die Tragweite seines Einverständnisses überhaupt erkennen kann.⁷⁹ Hier spielt eine Rolle, dass Datenschutzerklärungen für Verbraucher oft gar nicht nachvollziehbar sind, da sie entweder den Umfang der Datenerhebung und –verarbeitung nur unpräzise erklären, und oft keine Klarheit über die Lösbarkeit der Daten sowie deren Weitergabe an Dritte hergestellt wird.⁸⁰ Um das Erfordernis der Bestimmtheit zu erfüllen, müssen die Daten übersichtlich aufgelistet sein und es muss für den „verständigen Leser“ unzweifelhaft zu erkennen sein, auf welche Daten sich die Einwilligung erstreckt. Selbst die Bezeichnung „vergleichbare Daten“ wurde als konkret genug bezeichnet; dies gilt allerdings nicht für sensitive Daten i.S.d. § 3 IX BDSG.⁸¹ Es geht dabei nicht darum, wie weitreichend die Datenerhebung, in die eingewilligt wird, ist, sondern nur darum, dass dem Leser klar sein muss, in was er einwilligt.⁸² Dies bedeutet, dass die Voraussetzungen an die Gewährung der Einwilligung nur die Erkenntnis des Betroffenen schützen, nicht aber die Daten selbst. Die genaue Tragweite der Einwilligung wird damit vom Prinzip der Privatautonomie umfasst und unterliegt nur im Rahmen einer AGB-Kontrolle bestimmten Beschränkungen (dazu unten).

Hervorhebung

§ 4 a I S. 4 BDSG ist außerdem zu entnehmen, dass die Einwilligung, wenn sie zusammen mit anderen Erklärungen erteilt wird, besonders hervorgehoben werden muss. Durch dieses Erfordernis soll verhindert werden, dass die Einwilligung bei Formularverträgen im so genannten Kleingedruckten versteckt wird und der Betroffene sie durch seine Unterschrift erteilt, ohne sich ihrer und ihres Bezugsgegenstands bewusst zu sein, weil er sie übersieht.⁸³ Mit der DSGVO wird die Idee der „differenzierten Einwilligung“ eingeführt, wonach in verschiedene Datenverarbeitungsvorgänge getrennt eingewilligt werden muss (Erwägungsgrund 32). Damit soll komplexen Globaleinwilligungen, durch die der Betroffene

⁷⁹Simitis, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8.Auflage 2014, Nomos Verlag, Rn. 77 zu § 4a BDSG.

⁸⁰Dies hat die Stiftung Warentest herausgefunden, s. *Test 3/2016*, S. 57 – 61.

⁸¹OLG Köln Urteil vom 17.06.2011, Az. 6 U 8/11, Rz 31.

⁸²Ibid., Rz 33 mit Verweis auf BGH, Urteil vom 11. 11. 2009 - VIII ZR 12/08 (OLG Köln) (Happy Digits).

⁸³So in Anlehnung an BGH, Urteil vom 16.7.2008 – VIII ZR 348/06 (*Payback*) – dieses Verfahren betraf allerdings nicht die datenschutzrechtliche Konformität oder Anforderungen an die Einwilligung, sondern Werbung unter Verwendung elektronischer Post und § 7 II, III UWG; BGH, Urteil vom 11.11.2009 – VIII ZR 12/08, (OLG Köln) (*HappyDigits*).

Datenerhebungen und –verarbeitungen nur in ihrer Gesamtheit akzeptieren oder ablehnen kann, entgegengewirkt werden.⁸⁴

Die Hervorhebung der Einwilligung bedeutet auch, dass für den Betroffenen erkennbar sein muss, welche Daten aufgrund einer Einwilligung und welche Daten aufgrund des Erlaubnistatbestands des §§ 29, 29 BDSG erhoben und verarbeitet werden. Dies bedeutet, dass ein Verkäufer oder Anbieter nicht die Einwilligung des Betroffenen einholen kann, um die Zweifel an der Zulässigkeit der Datenverarbeitung auszuschließen, obwohl diese auf Basis von § 28 BDSG erlaubt ist.⁸⁵ So ist es auch zu verstehen, dass § 28 BDSG nicht einschlägig ist, wenn der Umfang der Datenverarbeitung selbst im Schuldverhältnis ausdrücklich geregelt ist; dann ist der Erlaubnistatbestand der Einwilligung gem. § 4 einschlägig.⁸⁶

Ungleichgewichte

An der Freiwilligkeit kann es fehlen, wenn ein klares Ungleichgewicht zwischen dem Betroffenen und dem Verantwortlichen besteht.⁸⁷ Im Falle einer strukturellen Unterlegenheit, derzufolge der Verbraucher keine Verhandlungsmacht gegenüber dem Verwender einer Datenschutzerklärung bzw. dem Anbieter eines Produkts oder Dienstleistung hat und faktisch keine Abweichung von Datenschutzerklärungen verhandeln werden kann, könnte allerdings davon ausgegangen werden, dass bereits eine etwaige Einwilligung nicht „ohne Zwang“ erfolgt. An der Möglichkeit einer freien Entscheidung kann es fehlen, wenn die Einwilligung in einer Situation wirtschaftlicher oder sozialer Schwäche oder Unterordnung erteilt wird oder wenn der Betroffene durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe seiner Daten verleitet wird.⁸⁸

Anders ist der Fall gelagert, wenn sich zwei Privatrechtssubjekte nicht auf Augenhöhe gegenüber stehen und deren Handeln dementsprechend nicht mehr autonom erfolgen kann: In diesem Fall ist bei der Ausgestaltung und Anwendung der zivilrechtlichen Normen besonders auf die Grundrechtsinteressen der einzelnen Parteien Rücksicht zu nehmen. Dies bedeutet, dass den Grundrechten im Privatrechtsbereich nur Rechnung getragen werden kann, wenn einfachgesetzliche Normen bestehen. Repressiv schützt das Zivilrecht somit Persönlichkeitsrechte/Grundrechte, indem es insbesondere Schadensersatz- und Entschädigungsansprüche bei Verletzung zubilligt. Für Verträge jeder Art bedeutet dies wiederum, dass diese sich grundsätzlich an den einfachgesetzlichen Bestimmungen zu orientieren haben und diesen nicht zuwiderlaufen dürfen. Es liegt allerdings auch an den staatlichen Stellen, zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in

⁸⁴ Schantz, „Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht“, (2016), *Neue Juristische Wochenschrift*, Heft 26, S. 1841-1847, S.1845.

⁸⁵ Dazu s. auch Wedde, *Bundesdatenschutzgesetz Kompaktkommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage 2016, Rn. 14a zu § 28 BDSG.

⁸⁶ Wolff, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition, C.H. Beck Verlag 2016, Rn. 26 zu § 28 BDSG.

⁸⁷ BGH, Urteil vom 16.07.2008 - VIII ZR 348/06; s.a. Schantz, „Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht“, (2016), *Neue Juristische Wochenschrift*, Heft 26, S. 1841-1847, S.1845.

⁸⁸ Z. B. BGH, Urteil vom 16.07.2008 – VIII ZR 348/06.

eine Fremdbestimmung umkehrt.⁸⁹ Die rechtliche Reglementierung der Privatrechtsverhältnisse hat dafür zu sorgen, dass nicht unbegrenzt das Recht des Stärkeren gilt.⁹⁰ Dies wird auch teilweise in der Literatur diskutiert.⁹¹

Ob eine strukturelle Ungleichheit tatsächlich auch in der Rechtsanwendung eine Rolle für das Vorliegen der Freiwilligkeit spielen wird, ist jedoch fraglich. Dies belegen die Verhandlungen über den entsprechenden Artikel 7 der DSGVO. Auch wenn Artikel 7 der DSGVO ausdrücklich normiert, dass der Verantwortliche nachweisen können muss, dass die Datenverarbeitung auf einer Einwilligung beruht, wurde kritisiert, dass Artikel 7 die Freiwilligkeit in Situationen klaren Ungleichgewichts zwischen Verantwortlichem und Betroffenen nicht grundsätzlich ausschließt. zahlreiche Regelungsvorschläge, die die Voraussetzung der Freiwilligkeit der Einwilligung hätten stärken können, keinen Eingang in die Endfassung der DSGVO gefunden haben.⁹² Der ursprüngliche Kommissionsentwurf⁹³ hatte in Erwägungsgrund 43 Satz 1 nicht nur auf die besondere Sachlage im Obrigkeitsverhältnis von Bürgern zu Behörden sondern auch explizit auf Ungleichgewichte im Arbeitsverhältnis hingewiesen. Allerdings findet sich diese Einschränkung der Möglichkeit, Einwilligung zur Legitimation von Datenverarbeitungen im Beschäftigtenverhältnis zu erteilen, nicht im verabschiedeten Text der DSGVO wieder.⁹⁴ Damit bleibt es bei der Trennung der Anforderungen zwischen der Datenerhebung und –verarbeitung durch staatliche Behörden auf der einen Seite und der Datenerhebung und –verarbeitung durch private Unternehmen auf der anderen.

Dieses Ergebnis ist aus der hier eingenommenen Perspektive des Privatsphärenschutzes bedenklich, da im IoT Verträge meist massenhaft und ohne qualifiziertes Erklärungsbewusstsein des Nutzers geschlossen werden: Der Kauf eines SmartTV oder einer SmartWaschmaschine impliziert nicht nur einen Kaufvertrag über das Gerät mit dem Händler, sondern gleichzeitig eine Vielzahl von vertraglichen Dauerschuldverhältnissen mit

⁸⁹ BVerfG, Beschluss des Ersten Senats vom 19.10.1993 - 1 BvR 567, 1044/89 --, BVerfGE 89, 214 (232).

⁹⁰ BVerfG, Beschluss des Ersten Senats vom 19.10.1993 - 1 BvR 567, 1044/89 --, BVerfGE 89, 214 (232); Jarass, *Kommentar zum Grundgesetz*, Jarass/Pieroth (Hrsg.), 13. Auflage 2014, C.H. Beck Verlag, Rn. 16 zu Art. 16 GG sowie Rn. 115 zu Art. 20 GG.

⁹¹ Z.B. Weichert, „Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung“, (2001), *Neue Juristische Wochenschrift*, Heft 20, S. 1463-1469, S. 1463.

⁹² Z.B.: Kühling/Martini, „Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?“, (2016), *Europäische Zeitschrift für Wirtschaftsrecht*, Heft 12, S. 448-454, S. 451.

⁹³ Europäische Kommission, Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Brüssel, den 25.1.2012, KOM(2012) 11 endgültig, 2012/0011 (COD).

⁹⁴ Kühling/Martini, „Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?“, (2016), *Europäische Zeitschrift für Wirtschaftsrecht*, Heft 12, S. 448-454, S. 451.

dem Produzenten des Geräts, dem Produzenten der eingebauten Software und nachträglich installierter Applikationen, dem Erbringer von Cloud-Diensten etc.⁹⁵

Striktes Kopplungsverbot der DSGVO

Artikel 7 IV und Erwägungsgrund 43 DSGVO machen die Freiwilligkeit davon abhängig, ob die Einwilligung in Datenverarbeitungsprozesse als zwingende Bedingung für die Durchführung eines Vertrages formuliert ist, obwohl der Verarbeiter die Daten dafür eigentlich nicht benötigt. Das strikte Kopplungsverbot des Art 7 IV DSGVO geht auf das Europäische Parlament zurück (Art. 7 IV 2 EP-E). Es bedeutet, dass die Freiwilligkeit und mithin die Wirksamkeit der Einwilligung fortan entfallen soll, wenn an ihre Erteilung das „Ob“ der Durchführung eines Kausalgeschäfts gekoppelt wird, das mit der konkreten Datennutzung oder dem Umfang der erhobenen Daten in keinem sachlichen Zusammenhang steht.⁹⁶

Dies bedeutet, dass bisher erteilte Einwilligungen nicht ohne Weiteres wirksam bleiben, wenn sie gegen Art. 7 IV DSGVO verstoßen. Dies hat der Düsseldorfer Kreis beschlossen.⁹⁷ Ausscheiden werden künftig auch Opt-out-Lösungen, bei denen die Einwilligung dadurch erfolgen soll, dass der Betroffene von einer vorkonfigurierten Abwahlmöglichkeit (etwa per Häkchen in einem Kästchen) keinen Gebrauch macht. Der BGH hatte bereits Klauseln, die durch Opt-Out unanwendbar wurden, für unwirksam erklärt.⁹⁸ Die expliziten Erfordernisse der Unmissverständlichkeit und Eindeutigkeit der Einwilligungserklärung wie in Erwägungsgrund 32 S. 1, 2 DSGVO verlangen grundsätzlich Opt-in-Lösungen.

Artikel 7 IV DSGVO geht über die bisherige deutsche Lösung in § 28 IIIb BDSG hinaus,⁹⁹ welche sich nur auf die Kopplung der Einwilligung zu Adresshandel und Werbung mit Abschluss eines Vertrages bezieht. Auf die entsprechende Regelung des § 28 III 1 BDSG wird unten noch einzugehen sein.

Das strikte Kopplungsverbot wird in der Literatur jedoch teilweise kritisch gesehen.¹⁰⁰ Zunächst verhindere es das im Internet gängige Modell der „Bezahlung mit den eigenen Daten“. Dagegen kann jedoch auch eingewandt werden, dass solchen Fälle, in denen Daten gegen Leistungen „eingetauscht“ werden, ohnehin eine Umgehung des Verbotsprinzips

⁹⁵ Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016) S. 50-51.

⁹⁶ Kaiser, <<https://www.projekt29.de/datenschutzblog29/anforderungen-an-die-einwilligung-gemaess-der-eu-dsgvo>> (zuletzt abgerufen am 30.11.2016).

⁹⁷ Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 13./14.09.2016), <https://www.la-bayern.de/media/dk_einwilligung.pdf> (zuletzt abgerufen am 2.11.2016).

⁹⁸ BGH, Urteil vom 16.7.2008 – VIII ZR 348/06 (Payback).

⁹⁹ Kühling/Martini, „Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?“, (2016), *Europäische Zeitschrift für Wirtschaftsrecht*, Heft 12, S. 448-454, S. 451.

¹⁰⁰ Z.B.: Schantz, „Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht?“, (2016) *Neue Juristische Wochenschrift*, Heft 26, S. 1841-1847, S.1845.

darstellen, weil die Freiwilligkeit der Einwilligung fehlt.¹⁰¹ Dazu wird im Verlauf dieses Papiers noch einmal kritisch eingegangen. Eine weitere Kritik gegen das strikte Kopplungsverbot des Art. 7 IV DSGVO besteht in der systemfremden Auslagerung des Kopplungsverbots aus dem Bereich der Datenerhebung zu eigenen Geschäftszwecken in das Einwilligungsmodell. Es wird argumentiert, dass das Kopplungsverbot des § 28 BDSG bereits die Zwangslagen erfasst, in denen der Betroffene nicht auf alternative Anbieter ausweichen kann. So kann eine Koppelung von Hard- und Software zu prohibitiv hohen Wechselkosten führen. Bei sozialen Netzwerken dürfte es viele Nutzer abschrecken, dass sie die meisten ihrer Kontakte verlieren, wenn sie zu einem anderen Anbieter wechseln. Damit schieße es über das Ziel der Gewährleistung der informationellen Selbstbestimmung hinaus.

Allerdings ist auch gegen diese Kritik zu argumentieren, dass das Kopplungsverbot tatsächlich Zwängen der Verbraucher beim Abschluss von Verträgen Rechnung trägt. Es ist inzwischen allgemein anerkannt, dass Verbraucher oft keine andere Wahl haben, als die AGB eines Unternehmens zu akzeptieren, wenn sie das zugrundeliegende Produkt oder die Dienstleistung erwerben wollen.¹⁰² Dies könne sogar völlig rational sein, da es zu dem Zeitpunkt, in dem der Verbraucher die AGB liest, schon zu einem signifikanten Aufwand (Aussuchen des Produkts bzw. der Dienstleistung, Preises und Anbieters) gekommen ist, zu dem das Lesen der oftmals langen und komplexen AGB nur beitragen würde, ohne dass der Verbraucher davon tatsächlich einen Nutzen hätte. Am Ende habe der Verbraucher doch keine Möglichkeit, auf den Inhalt der AGB Einfluss zu nehmen.

Fraglich ist, ob eine Kopplungspraxis, die nach dem Datenschutzrecht unzulässig wäre, auch eine unlautere Geschäftspraxis i.S.d. UWG darstellt.¹⁰³ Im Lauterkeitsrecht sind Kopplungspraktiken nicht grundsätzlich ausgeschlossen, da die Anlockungswirkung eines guten Angebots auch eine erwünschte Folge des Leistungswettbewerbs sein kann.¹⁰⁴ In diesem Sinne hat der EuGH unlängst gegen die Unlauterkeit einer Vorinstallation von Software auf einem Computer entschieden.¹⁰⁵ Allerdings ist fraglich, ob dieses Urteil verallgemeinert werden kann, da es sich lediglich auf die vom französischen Kassationsgerichtshof vorgelegte Frage bezog, ob fehlenden Preisangaben für einzelne Programme eine irreführende Geschäftspraxis i.S.d. Art. 5 Abs. 4 Buchst. a und Art. 7 der Lauterkeitsrichtlinie 2005/29 darstellen. Der EuGH kam zu dem Ergebnis, dass sich allein aus den fehlenden Preisangaben keine Irreführung ergebe, da das Fehlen einer Preisangabe für die einzelnen Programme weder geeignet sei, den Verbraucher daran zu hindern, eine informierte geschäftliche Entscheidung zu treffen, noch dazu, ihn zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Daher sei Preis der

¹⁰¹ Conrad/Hausen, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), 2. Auflage, C.H. Beck Verlag 2016, Rn.150-152 zu § 36 Datenschutz der Telemedien.

¹⁰² S. z.B. Elshout et al. *Study on consumers' attitudes towards Terms and Conditions (T&Cs)*, (2016), European Commission, Directorate-General for Justice and Consumers, S. 16-17, 20ff.

¹⁰³ Dazu auch Schmechel, *Verbraucherdatenschutz nach der EU-Datenschutzgrundverordnung*, (SVRV Working Paper Series Nr. 4/2016, Sachverständigenrat für Verbraucherfragen 2016), S.16-17.

¹⁰⁴ Dazu: Ohly, „Das neue UWG – Mehr Freiheit für den Wettbewerb?“, (2004), *Gewerblicher Rechtsschutz und Urheberrecht*, Heft 11, S.889-900, S. 897, m.w.N.

¹⁰⁵ Dazu auch Case C-310/15, Vincent Deroo-Blanquart v. Sony Europe Limited, Rechtsnachfolgerin der Sony France SA, EU:C:2016:633.

einzelnen Programme keine wesentliche Information im Sinne von Art. 7 Abs. 4 der Richtlinie 2005/29.

Die Diskrepanz zwischen dem strikten datenschutzrechtlichen Kopplungsverbot und den weniger strengen Maßstäben für eine Irreführung im Lauterkeitsrecht kann auf die unterschiedliche Schutzzwecke und Regelungsansätze zurückgeführt werden. Das Datenschutzrecht schützt das allgemeine Persönlichkeitsrecht durch ein generelles Verbot mit Erlaubnisvorbehalt. Dagegen kennt das UWG kein solches generelles Verbot von unlauteren geschäftlichen Handlungen, sondern sieht diese nur dann als unzulässig wenn, wenn sie geeignet sind, die Interessen von Marktteilnehmern spürbar zu beeinträchtigen, § 3 I UWG. Die unterschiedlichen Regelungsansätze reflektieren die unterschiedliche Bedeutung von Schutzgütern: Das Datenschutzrecht bezieht sich auf personenbezogene Daten, die unmittelbar die Privatsphäre berühren, während das Lauterkeitsrecht Handlungsfreiheit im geschäftlichen Verkehr schützt. Die Privatsphäre der Handelnden ist nicht per se Schutzgut im geschäftlichen Verkehr. Wenn allerdings die Privatsphäre durch geschäftliches Handeln und die Betroffenheit von personenbezogenen Daten berührt ist, ist das Datenschutzrecht mit seinem höheren Schutzniveau für Kopplungspraktiken einschlägig.

c. Formerfordernisse

Die Zulässigkeit der Einwilligung nach §4a BDSG ist außerdem an Formerfordernisse gebunden. Um sicher zu stellen, dass die Einwilligung einen bewussten und autonomen Willensakt darstellt, muss sie wirksam hervorgehoben werden.¹⁰⁶ Hier wird auf den durchschnittlich informierten und verständigen Verbraucher abgestellt, der einer vorformulierten Einwilligungserklärung die der Situation angemessene Aufmerksamkeit entgegenbringt; der oberflächliche Verbraucher wird hier nicht geschützt. Generell kann die Einwilligung gem. §§ 13 TMG, 94 TKG eine Einwilligung auch elektronisch erfolgen.

2. Erforderlichkeit für Vertragszweck

Für Vertragsbeziehungen im IoT kommt für die Zulässigkeit von Datenerhebung-, verarbeitung und –nutzung neben der Einwilligung insbesondere die gesetzliche Erlaubnisnorm des § 28 BDSG, Art. 6 I lit.b) DSGVO in Betracht, welcher die Erhebung, Veränderung oder Übermittlung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke erlaubt. Der Begriff der Geschäftszwecke erfasst alle Prozesse, die als Mittel zum Zweck zur Erfüllung von Abwicklung von Verträgen dienen.¹⁰⁷

a. Zweckbindung für Geschäftszwecke

Gem. § 28 I Nr. 1 BDSG ist eine Datenerhebung und –speicherung zulässig, wenn diese beispielsweise für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses mit dem Betroffenen erforderlich ist. Hier geht es um eine Zweckbindung von Datenerhebungen und –verarbeitungen. Die Zweckbestimmung leitet sich

¹⁰⁶ BGH, Urteil vom 16.07.2008 - VIII ZR 348/06 (OLG München) (Payback) Para 24.

¹⁰⁷ Bundesregierung, *BT-Drucksache 07/1027 Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundes-Datenschutzgesetz — BDSG)*, (Drucksache 07/1027 21.09.1973), Amtliche Begründung zum Regierungsentwurf S. 27.

unmittelbar aus den dem Rechtsgeschäft zugrunde liegenden Willenserklärungen ab; es geht also nicht um einseitige Vorstellungen des Verkäufers oder Dienstleisters oder des betroffenen Verbrauchers.¹⁰⁸ Zwischen dem Rechtsgeschäft und der Datenspeicherung muss ein unmittelbarer sachlicher Zusammenhang bestehen.¹⁰⁹ Für die Erforderlichkeit kommt es ebenfalls nicht auf einseitige Vorstellungen, sondern auf eine objektiv feststellbare Erforderlichkeit an, unter Berücksichtigung der datenschutzrechtlichen Grundsätze der Datenvermeidung und Datensparsamkeit.¹¹⁰ Erforderlichkeit bedeutet, dass sich der Geschäftszweck oder das angestrebte Ziel ohne diese Daten nicht erreichen ließe. Solche berechtigten Interessen können bestehen im Falle der Kundenwerbung, der Abwehr von Vermögensschäden im wirtschaftlichen Bereich durch Speicherung von Daten über kriminelles wirtschaftsschädigendes Verhalten (Beispiel Schufa), oder im Versicherungsbereich der Speicherung von Daten über Angehörige und bei Schlechtrisikenkarteien.¹¹¹

Die Rechtsfolgen einer mangelnden Zweckbindung sind jedoch unklar. Obwohl der Wortlaut der §§ 28, 29 BDSG („... zulässig, wenn...“) nahe legt, dass eine Datenerhebung unzulässig ist, wenn sie nicht vom Geschäftszweck umfasst ist, legt Härting dar, dass sich den §§ 4, 28, 29 BDSG kein allgemeiner Grundsatz der Zweckbindung entnehmen lässt:¹¹² allzu leicht lasse sich eine Zweckänderung bewirken, für welche gem. §28 II BDSG bereits die Wahrung berechtigter Interesse ausreicht, wenn kein Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen überwiegen.

Ob Art. 5 I lit. b DSGVO, welcher den Zweckbindungsgrundsatz für die Erhebung und Weiterverarbeitung von personenbezogenen Daten festschreibt, eine echte Neuerung darstellt, bleibt abzuwarten. Denn auch hier bleiben die Rechtsfolgen einer mangelnden Zweckbindung unklar. Die Erfüllung der Zweckbindung ist keine Zulässigkeitsvoraussetzung für Datenverarbeitungen gem. Art. 6 DSGVO. Art. 6 DSGVO macht die Zulässigkeit der Verarbeitung in lit. a und b wiederum entweder von einer Einwilligung oder der Erforderlichkeit für den Vertragszweck abhängig. Unzulässigkeit folgt also nicht schon allein aus der mangelnden Zweckbindung der Datenerhebung und –verarbeitung.

b. Wahrung berechtigter Interessen

Gem. § 28 I Nr. 2 BDSG sind Datenerhebung und –verarbeitung auch zulässig, soweit sie zur Wahrung berechtigter Interessen erforderlich sind und keine schutzwürdigen Interessen des Betroffenen entgegenstehen. Unter solche zulässigen Interessen fallen alle

¹⁰⁸ Wedde, *Bundesdatenschutzgesetz Kompaktcommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage, Bund Verlag 2016, Rn. 16 zu § 28 BDSG; auch konkludent möglich: Wolff, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition, C.H. Beck Verlag 2016, Rn. 14-18 zu § 28 BDSG.

¹⁰⁹ Ambs, *Erbs/Kohlhaas Strafrechtliche Nebengesetze*, Häberle (Hrsg.), Band 17 2016, C.H. Beck Verlag, Rn. 4 zu § 28 BDSG.

¹¹⁰ Wedde, *Bundesdatenschutzgesetz Kompaktcommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage 2016, Bund Verlag, Rn. 17 zu § 28 BDSG.

¹¹¹ Ambs, *Erbs/Kohlhaas Strafrechtliche Nebengesetze*, Häberle (Hrsg.), Band 17 2016, C.H. Beck Verlag, Rn. 8 zu § 28 BDSG.

¹¹² Härting, „Zweckbindung und Zweckänderung im Datenschutzrecht“ (2015), *Neue Juristische Wochenschrift*, Heft 45, S. 3284-3288, S.3288.

tatsächlichen, d.h. auch wirtschaftliche und ideelle, Interessen, soweit sie von der Rechtsordnung gebilligt werden.¹¹³ § 28 I Nr. 2 BDSG stellt jedoch keinen Auffangtatbestand dar, der eine nicht nach Nr. 1 legitimierte Datenverarbeitung erlaubt.¹¹⁴

Der Hinweis auf die „berechtigten Interessen“ umschreibt einen Kompromiss im Widerstreit zwischen der informationellen Selbstbestimmung der Betroffenen und dem Informationsbedarf Dritter. In der Interessenabwägung soll es allerdings wegen der allgemeinen Formulierung des § 28 I Nr. 2 BDSG und im Hinblick auf seinen Zweck, den Verwendungsspielraum für Datenerhebungen und –nutzung einzuschränken, auf eine möglichst restriktive Auslegung ankommen.¹¹⁵ Die einschränkende Wirkung der Interessenabwägung ist unter Beachtung der informationellen Selbstbestimmung gerechtfertigt.¹¹⁶ Wohl dürften daher im Zweifel die schutzwürdigen Interessen des Betroffenen die Interessen des datenerhebenden Unternehmens überwiegen. Dies sei zumindest dann der Fall, wenn die Daten Rückschlüsse auf Verhalten, Aufenthaltsorte oder Gewohnheiten des Betroffenen erlauben und nicht lediglich technischen Zwecken dienen.¹¹⁷ Außerdem dürfen verantwortliche Stellen gespeicherte Daten nicht zweckentfremden oder mithilfe des § 29 I Nr. 1 andere Schranken zur Datenübermittlung umgehen.¹¹⁸

Wendehorst¹¹⁹ schlägt vor, im Wege der teleologischen Reduktion die Legimitationstatbestände der *Geschäftszwecke* oder *berechtigten Interessen* nur dann anzuwenden, wenn die Datenerhebung und –verarbeitung nicht nur der Vertragserfüllung oder der Wahrung berechtigter Interessen sondern auch für ein darüber hinausgehendes kommerzielles Interesse des Anbieters dient. In solchen Fälle habe die Datenverarbeitung auch eine Entgeltfunktion, weshalb eine Privilegierung ausscheide. Überzeugenderweise stellt sie hier auf den *effet utile* Grundsatz im EU-Recht ab, wonach das Unterlaufen der Einwilligungsvoraussetzungen und der damit verbundenen Schutzmechanismen nicht dem Willen des EU-Gesetzgebers entsprechen könne.

c. Kopplungsverbot

Für den Sonderfall der Datenerhebung und –verarbeitung für Zwecke des Adresshandels oder der Werbung, für welche eine Einwilligung dem. § 28 III 1 BDSG erforderlich ist, normiert § 28 III b BDSG ein Kopplungsverbot. Dieses besagt, dass die verantwortliche

¹¹³ BGH: Entscheidung vom 22.05.1984 - VI ZR 105/82 zitiert in: Spindler/Nink, *Recht der elektronischen Medien Kommentar*, Spindler/Schuster (Hrsg.), 3. Auflage 2015, C.H. Beck Verlag, Rn. 7-11 zu § 28 BDSG.

¹¹⁴ Simitis, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 99 zu § 28 BDSG.

¹¹⁵ So: Simitis, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 98 zu § 28 BDSG.

¹¹⁶ Wedde, *Bundesdatenschutzgesetz Kompaktcommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage 2016, Bund Verlag, Rn. 52 zu § 28 BDSG.

¹¹⁷ So Roßnagel, „Fahrzeugdaten – wer darf über sie entscheiden?“, (2014), *Straßenverkehrsrecht*, Heft 8, S. 281-287, S. 285.

¹¹⁸ S. dazu Simitis, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 99 zu § 28 BDSG.

¹¹⁹ Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016), S. 52-53.

Stelle sich die Einwilligung des Betroffenen nicht auf dem Wege verschaffen darf, dass sie hiervon den Abschluss eines „Monopol-Vertrages“ abhängig macht. Dieses Verbot ist aufgrund seiner Einschränkung der Vertragsgestaltungsfreiheit auf die Fälle begrenzt, in denen dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Gegenleistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.¹²⁰ Dabei wird davon ausgegangen, dass der Betroffene keine tatsächliche Wahl darüber hat, ob er seine Daten preisgeben möchte oder nicht.

Für die Feststellung der Unzumutbarkeit ist eine niedrige Schwelle anzusetzen.¹²¹ Im Rahmen eines Kaufvertrages kann es beispielsweise unzumutbar sein, wenn es generell möglich ist, eine Ware bei einem anderen Anbieter zu bekommen, ohne eine Einwilligung in etwaige Werbemaßnahmen zu erteilen, dies aber mit einem erhöhten Zeitaufwand für die neue Suche verbunden ist oder wenn gleiche oder vergleichbare Produkte bei anderen Anbietern nur zu schlechteren Konditionen erhältlich sind.¹²² Dies bedeutet, dass es nicht ausreicht, dass eine bestimmte Leistung generell anderweitig verlangt werden kann. Obschon dieser Regelungsansatz auch aus verbraucher- und datenschutzrechtlicher Perspektive positiv erscheint, muss beachtet werden, dass das Koppelungsverbot in erster Linie der Gefahr des Missbrauchs von Marktmacht von datenerhebenden Unternehmen dient.¹²³

IV. Zulässigkeit der Datenerhebung: AGB-Recht

Sofern die Datenerhebung und –nutzung auf einer vom Unternehmen vorformulierten Erklärung beruht, sind neben den datenschutzrechtlichen Bestimmungen auch die §§ 305 BGB anwendbar. Eine Integrierung von der Einwilligung in die AGB ist grundsätzlich zulässig.¹²⁴

Ob Datenschutzerklärungen einer ABG-Kontrolle unterworfen werden sollen ist zwar umstritten; es gibt aber eine deutliche Tendenz, Datenschutzerklärungen als AGB anzusehen, wenn die Definition von AGB in § 305 BGB erfüllt sind. Datenschutzerklärungen sind dann AGB, wenn sie in den Nutzungsvertrag mit dem Anwender einbezogen und damit

¹²⁰ Wolff, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 165 zu § 28 BDSG.

¹²¹ Wedde, *Bundesdatenschutzgesetz Kompaktkommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage 2016, Bund Verlag, Rn. 134 zu § 28 BDSG; zur Anwendung auf Fälle einer marktbeherrschenden Stellung: Bundesregierung, *Bundestag Drucksache 17/12011 Kleine Anfrage der Abgeordneten Dorothea Steiner, Oliver Krischer, Dr. Hermann E. Ott, Hans-Josef Fell, Bärbel Höhn, Sven-Christian Kindler, Ute Koczy, Sylvia Kotting-Uhl, Undine Kurth (Quedlinburg), Nicole Maisch und der Fraktion BÜNDNIS 90/DIE GRÜNEN*, (Drucksache 17/12011, 30. 03.01.2013), S. 33.

¹²² Dazu Wedde, *Bundesdatenschutzgesetz Kompaktkommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage 2016, Bund Verlag, Rn. 134-138 zu § 28 BDSG.

¹²³ Ibid., Rn. 136 zu § 28 BDSG

¹²⁴ Redeker, *Handbuch Multimedia-Recht Rechtsfragen des elektronischen Geschäftsverkehrs*, Hoeren/Sieber/Holznapel (Hrsg.), (C.H. Beck Verlag, 2015), Rn 111 in 42. Ergänzungslieferung, Teil 12 Vertragsrecht für Internetdienste; BGH, Urteil vom 27.01.2000 - I ZR 241/97 (OLG Stuttgart) (Telefonwerbung VI).

entgegen der gesetzgeberischen Intention nicht als Unterrichtung ausgestaltet sind.¹²⁵ Es kommt entscheidend darauf an, dass der Verwender für sich allein die rechtsgeschäftliche Gestaltungsfreiheit in Anspruch nimmt und der Vertragspartner keinen Einfluss darauf nehmen kann, sondern nur, ob er die vorformulierte Erklärung abgeben will oder nicht.¹²⁶

In der Rechtsprechung ist die Tendenz erkennbar, Datenschutzerklärungen als AGB anzusehen, da selbst Bestimmungen mit bloßem Informations- und Hinweischarakter als Geschäftsbedingungen qualifiziert werden.¹²⁷ Dies kann auch mit Hinweis auf vergleichbare Schutzbedürftigkeit erklärt werden: Die AGB-Kontrolle soll den Interessen der Verbraucher bei der durch Verwendung vorformulierter Klauseln verursachten Störung der Privatautonomie Rechnung tragen.¹²⁸ Die Notwendigkeit einer gerichtlichen Kontrolle liegt darin, dass bei einem individuell ausgehandelten Vertrag davon ausgegangen werden kann, dass der Vertragsinhalt dem Interesse und Willen beider Parteien entspricht, bei AGB, die von lediglich einer Vertragspartei vorgegeben werden ist dies typischerweise nicht der Fall.¹²⁹ Die §§ 305 ff. sind also eine korrigierende Reaktion auf die Inanspruchnahme einseitiger Vertragsgestaltungsmacht durch den Verwender.¹³⁰ In derselben Situation steckt i.d.R. auch der Adressat einer Datenschutzerklärung: Er kann die einzelnen Bestimmungen nicht aushandeln und diskutieren. Zudem wird der Vertrag nicht zustande kommen, wenn der Verbraucher nicht auch die Datenschutzerklärungen annimmt.

Allerdings hat der Bundesgerichtshof in mehreren Entscheidungen¹³¹ Datenschutzerklärungen zwar an sich der AGB-Kontrolle unterworfen, aber in Ermangelung der Existenz besonderer Rechtsvorschriften betreffend die näheren Bedingungen der Einwilligung usw. eine Abweichung oder Ergänzung von Rechtsvorschriften und damit die Voraussetzung des § 307 III 1 BGB aber verneint und daher keine Missbrauchskontrolle vorgenommen. Um diese Umgehungsmöglichkeit der AGB-Kontrolle für Datenschutzregelungen zu verhindern, schlägt Wendehorst vor,¹³² das AGB-Recht dahingehend zu ändern, dass eine Missbrauchskontrolle auch bei Datenschutzerklärungen vorgenommen werden kann. Konkret schlägt sie vor, den Wortlaut § 307 III BGB so zu

¹²⁵ Kremer, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 58 zu § 28 Apps und Social Media; LG Berlin Urteil vom 30. 4. 2013 – 15 O 92/12; Kremer, „Datenschutzerklärungen von Social Media Diensten: Anwendbares Recht und AGB-Kontrolle“, (2014), *Recht der Datenverarbeitung*, Heft 2, S. 73-83, S. 82.

¹²⁶ Tinnfeld/Buchner/Petri, *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, (De Gruyter Verlag, 2012), S. 348, dazu auch: Pohle, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn.208 zu § 35 Das Recht der Kommunikationsnetze und Dienste.

¹²⁷ Z.B. LG Berlin, Urteil vom 30.04.2013 - 15 O 92/12.

¹²⁸ Lehmann-Richter, *beck-online.GROSSKOMMENTAR*, Artz (Hrsg.), C.H.Beck Verlag, Stand 01.10.2016, Rn. 8 zu § 305 BGB.

¹²⁹ Grüneberg, *Bürgerliches Gesetzbuch Kommentar*, Palandt (Hrsg.), 74. Auflage 2015, C.H. Beck Verlag, Rn. 3 zu Vor § 305 BGB.; Schmidt-Salzer, *Das Recht der Allgemeinen Geschäfts- und Versicherungsbedingungen*, (Duncker & Humblot Verlag, 1977).

¹³⁰ BGH, Urteil vom 19.11.2009 - III ZR 108/08 (OLG München); BGH, Urteil vom 24.05.1995 - XII ZR 172/94 (Düsseldorf).

¹³¹ BGH, Urteil vom 16.07.2008, VIII ZR 348/06 – *Payback*; Urteil vom 11.11.2009, VIII ZR 12/08 – *HappyDigs*.

¹³² Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016), S.74.

ändern, dass kein Bezug mehr zu abweichenden Rechtsvorschriften genommen wird. Stattdessen soll die Formulierung der Richtlinie 93/13 eingefügt werden, wonach auch in der deutschen Rechtsordnung dann klar gestellt wird, dass sich die AGB-Kontrolle nicht auf den Hauptgegenstand des Vertrages beziehen soll.

Die rechtlichen Rahmenbedingungen für die Wirksamkeit der datenschutzrechtlichen Einwilligung innerhalb von AGB basieren insbesondere auf dem Transparenzgebot des § 307 I 2 BGB. Dies bedeutet beispielsweise, dass eine Klausel nicht als Bevollmächtigung zur Weitergabe von Daten an Dritte „zur Formulierung von bedarfsgerechten Angeboten und Informationen“ formuliert ist, da diese Formulierung dazu führen kann, dass der Verwender die Daten eigenmächtig weitergibt.¹³³ Ein Verstoß liegt ebenfalls vor, wenn die Einwilligungserklärung an versteckter Stelle mitten in einem vorformulierten Text untergebracht ist.¹³⁴

Gem. §4a I S. 4 BDSG muss die Einwilligung für ihre Gültigkeit außerdem besonders hervorgehoben werden. Dies trägt dem Schutz des Betroffenen Rechnung, dass dieser die Einwilligung nicht überliest und diese sodann erteilt, ohne sich ihrer und ihres Bezugsgegenstands bewusst zu sein.¹³⁵

In diesem Sinne hat der BGH auch eine Opt-out-Erklärung für unwirksam erklärt. In seinem Payback-Urteil stellt er fest, dass die Klausel

„Mit meiner Unterschrift erkläre ich mich einverstanden, dass die von mir oben angegebenen Daten sowie die Rabattdaten (Waren/Dienstleistungen, Preis, Rabattbetrag, Ort und Datum des Vorgangs) für an mich gerichtete Werbung (z.B. Informationen über Sonderangebote, Rabattaktionen) per Post und mittels gegebenenfalls von mir beantragter Services (SMS oder E-Mail-Newsletter) sowie zu Zwecken der Marktforschung ausschließlich von der L-GmbH und den Partnerunternehmen gemäß Nr. 2 der beiliegenden Hinweise zum Datenschutz gespeichert und genutzt werden.

(...)

☐ Hier ankreuzen, falls die Einwilligung nicht erteilt wird.“

der Inhaltskontrolle nach §§ 307 I 1, II Nr. 1 BGB nicht stand hält soweit sie sich auf die Zusendung von Werbung auf elektronischem Wege bezieht.

Festzuhalten ist also, dass Datenschutzerklärungen der AGB-Kontrolle unterfallen können und damit auch nicht überraschend oder mehrdeutig i.S.d. § 305c BGB sein und dürfen nach § 307 BGB den Vertragspartner nicht entgegen Treu und Glauben benachteiligen.

¹³³ LG Dortmund, Urteil vom. 23.2.2007 – 8 O 194/06; vgl. auch OLG Köln, Urteil vom 23.11.2007 – 6 U 95/07.

¹³⁴ LG Bonn, Urteil vom 31.10.2006 – 11 O 66/06.

¹³⁵ BGH, Urteil vom 16.07.2008 – VIII ZR 348/06, vgl. auch OLG Hamm, Urteil vom 17.02.2011 – I-4 U 174/10.

V. Beispiel: Zulässigkeit von Datenerhebungen durch die HCA

Im Anwendungsbereich dieses beschriebenen Rechtsrahmens werden im Folgenden die Bestimmungen der Datenschutzerklärung der bereits erwähnten Home Connect auf ihre Rechtmäßigkeit nach den Vorschriften des BDSG, TMG und BGB überprüft.

1. Datenerhebung und Verarbeitung der HCA

Im Rahmen der HCA gibt es neben der Datenschutzerklärung auch Nutzungsbedingungen für die HCA sowie Nutzungsbedingungen für das Home Connect System. Die Nutzungsbedingungen der HCA werden mit Abschluss der Registrierung bindende Vertragsgrundlage für die Nutzung der HCA. Die Nutzungsbedingungen für das Home Connect System werden zwischen Nutzer und der Home Connect GmbH bindend, sobald die Registrierung über die HCA abgeschlossen ist.

In den Nutzungsbedingungen für das Smart Home System findet sich unter Punkt 13 „Datenschutzrechtliche Einwilligung“ ein Abschnitt zum Thema Datennutzung. Dieser lautet:

„Sie willigen ein, dass die Home Connect GmbH Ihre Registrierungsdaten, Daten aus der Nutzung der App und Daten aus der Nutzung des Hausgeräts ("Personenbezogenen Daten") erheben, verarbeiten und nutzen darf, um Ihre möglichen Interessen an bestimmten Produkten und Dienstleistungen der Home Connect GmbH und von Dritten für Werbezwecke zu ermitteln und entsprechend dieser ermittelten Interessen Produkt- und Dienstleistungsinformationen innerhalb der App darzustellen. Die für diese Zwecke verarbeiteten Personenbezogenen Daten umfassen: Registrierungsdaten: Vor- und Nachname, E-Mail-Adresse, durch die Verbindung mit dem Hausgerät automatisch erhobene Informationen zur Art und zum Model des Haushaltsgeräts. Daten aus der Nutzung der App: Verwendete Funktionen und Bereiche der App, erteilte Befehle zur Steuerung des Hausgeräts, aufgerufene Rezeptempfehlungen, IP-Adresse, Interaktion mit Werbeeinblendung. Daten aus der Nutzung des Hausgeräts: Art und Model des Hausgeräts, verwendete Programme, Standort des Hausgeräts, Wasserhärte am Standort des Hausgeräts und Nutzungsweise des Hausgeräts“

Damit ist klar, dass über die HCA verschiedene Arten von Daten gesammelt und verarbeitet werden: Registrierungsdaten, App-Nutzungsdaten und Gerätenutzungsdaten.

In Nr. 1 der Datenschutzerklärung der HCA ergibt sich weiterhin folgende Aufteilung von Daten: Nutzer-Stammdaten (a), Geräte-Stammdaten (b), Geräte-Nutzungsdaten (c) und App-Nutzungsdaten (d).

Nutzer-Stammdaten sind Bestandsdaten i.S.d. §§ 28 I Nr. 1 BDSG, 14 I TMG, die für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses zwischen dem App-Anbieter und dem Verbraucher über die Nutzung der App erforderlich sind. Hierunter fallen die Daten, die bei einer Registrierung angegeben werden müssen (Registrierungsdaten). Nr. 1 lit. a) der HCA enthält diesbezüglich folgende Aufzählung von Nutzer-Stammdaten:

- Angaben, die Sie im Rahmen der Registrierung machen, wie:
 - Vor- und Nachname
 - E-Mail-Adresse (Benutzerkennung)
 - das Land, indem Sie Ihr(e) Hausgerät(e) betreiben
 - Passwort als Zugriffsschutz.
- Informationen, die wir im Zusammenhang mit der Registrierung erheben und speichern:
 - Spracheinstellung Ihres mobilen Endgerätes
 - Einverständnis mit der Geltung der Nutzungsbedingungen und Bestätigung der Kenntnisnahme der Datenschutzerklärung
 - Status des Nutzerkontos (aktiviert/deaktiviert)
 - App Tracking-Voreinstellung (erfolgt in Abhängigkeit der Landeswahl, siehe dazu unten 5.)

Geräte-Stammdaten umfassen Informationen über die mit der App verbundenen Haushaltgeräte; diese sind auch Bestandsdaten i.S.d. §§ 28 I Nr. 1 BDSG, 14 I TMG.

- Marke des Hausgerätes (z.B. Bosch oder Siemens)
- Seriennummer und ggf. Fabrikationsdatum des Hausgerätes (sog. E-Nummer und FD-Nummer, diese Angaben finden sich auch auf dem Typenschild des Hausgerätes)
- Die eindeutige Kennung des im Hausgerät eingesetzten Netzwerkadapters (sog. MAC-Adresse). Diese Daten werden im Rahmen der „Hausgerät verbinden“-Funktion für jedes verbundene Hausgerät Ihrem Nutzerkonto zugeordnet.

Gerätenutzungsdaten sind dagegen die personenbezogenen Daten, ohne die die App nicht verwendet werden kann. Dies ist in der Regel die IP-Adresse und falls erforderlich Kennung oder Standort. Die Zulässigkeit ihrer Erhebung und Verwendung richtet sich nach § 15 TMG. Laut Nr. 1 lit b) sind die von der Home Connect erhobenen Geräte-Stammdaten:

- Vorgenommene Grundeinstellungen, Programmauswahl und Programmeinstellungen am Hausgerät oder über die App,
- Gerätezustandsdaten wie Umgebungsbedingungen, Zustände von Bauteilen, Zustandsänderungen am Hausgerät (z.B. Wechsel des Betriebsmodus, Öffnen oder Schließen der Türe/des Frontpanels, Temperaturänderungen, Füllstände) und Zustandsmeldungen des Hausgerätes (z.B. Gerät ist überhitzt, Wassertank ist leer etc.).

App-Nutzungsdaten sind gem. Nr. 1 lit) wiederum Inhaltsdaten, die sich aus der Interaktion des Nutzers mit der App ergeben, wie z.B. verwendete Funktionalitäten der App, Klickverhalten in Bezug auf Bedienelemente der App, Auswahl in Dropdown-Menüs,

Einstellungen von On/Off-Schaltern. Solche Daten werden gem. Nr. 5 der HCA von Adobe Analytics in Irland ausgewertet. Die Sammlung von App-Nutzungsdaten kann gem. Nr. 5 HCA außerdem vom Nutzer aktiviert oder deaktiviert werden.

2. Zulässigkeit nach BDSG

Die Anwendbarkeit des BDSG für die HCA ergibt sich aus dem Territorialprinzip:¹³⁶ Wenn personenbezogene Daten durch Unternehmen mit Sitz bzw. einer Niederlassung im Inland, soweit letztere effektiv und tatsächlich datenverarbeitende Tätigkeiten ausführt, erhoben, verarbeitet und genutzt werden, finden gemäß § 1 Abs. 2 und Abs. 5 Satz 1 BDSG dieses Gesetz und die datenschutzrechtlichen Regelungen der § 11 ff. TMG über den Verweis in § 3 Abs.3 Nr. 4 TMG Anwendung.¹³⁷ Apps sind Telemediendienste und unterliegen den Rechtsvorschriften des TMG. Beim TMG handelt es sich um eine bereichsspezifische Regelung, deren Ziel es ist, die generellen Anforderungen des BDSG in besonders datenschutzsensiblen Bereichen zu präzisieren und weiterzuentwickeln.

a. Verantwortliche Stelle

In Bezug auf die gesetzlichen Anforderungen muss zwischen dem Vertrieb und der Nutzung der App unterschieden werden. Aus datenschutzrechtlicher Sicht bringt der Vertrieb der App keine Besonderheiten mit sich.¹³⁸ Verantwortliche Stelle ist beim Vertrieb der App der App-Store-Betreiber. Da der Betreiber bei der Nutzung der App nach der Installation keinen Einfluss mehr hat, ist nun der Anbieter verantwortliche Stelle¹³⁹ und hat dafür zu sorgen, dass die Pflichten des BDSG, soweit nicht das TMG vorrangig anzuwenden ist, eingehalten werden.¹⁴⁰

Die Datenschutzerklärung der HCA erklärt, dass die Home Connect GmbH mit Sitz in München die verantwortliche Stelle für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten im Zusammenhang mit der HCA ist.

b. Einwilligung

Für die App als Telemediendienst gilt § 13 TMG (vgl. § 33 BDSG): Der Anbieter muss den Nutzer über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten informieren. Diese Information muss bereits vor Beginn des Nutzungsvorgangs erfolgen, so dass die Datenschutzerklärung bereits im App-Store oder mindestens vor dem Start der App zum Abruf bereitgehalten werden muss. Darüber hinaus muss die – gut lesbare – Datenschutzerklärung auch während der Nutzung der App jederzeit abrufbar sein. Eine bloße Verlinkung auf die Datenschutzerklärung einer Webseite ist nicht ausreichend. Bei einer elektronischen Einwilligung sind die Voraussetzungen des § 13 TMG zu beachten.

¹³⁶ Kremer, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 48 zu § 28 Apps und Social Media.

¹³⁷ Sachs/Meder, „Datenschutzrechtliche Anforderungen an App-Anbieter - Prüfungen am Beispiel von Android-Apps“, (2013), *Zeitschrift für Datenschutz*, Heft 7, S. 303-308, S. 304.

¹³⁸ Kremer, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 46 zu § 28 Apps und Social Media.

¹³⁹ Kremer, „Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices“, (2002), *Computer und Recht*, Heft 7, S. 438-446, S. 439.

¹⁴⁰ Kremer, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 48 zu § 28 Apps und Social Media.

Liegen weder eine gesetzliche Erlaubnis noch eine Einwilligung des Betroffenen vor, ist die Datenverarbeitung gesetzeswidrig.

Eine Datenschutzerklärung für die HCA (nachfolgend „App“) ist grundsätzlich vorhanden. Diese ist auch vor Installation der App auffindbar.

Die Datenschutzerklärung der HCA klärt außerdem über die Datenübermittlung an Dritte auf.

Zur Realisierung der App und der darüber angebotenen Dienstleistungen arbeiten wir mit verschiedenen Dienstleistern zusammen. Soweit wir diese Dienstleister zur streng weisungsgebundenen Datenverarbeitung als Auftragsdatenverarbeiter verpflichtet haben, bedarf eine Datenverarbeitung durch diese Dienstleister keiner Einwilligung durch Sie. Die entsprechenden Dienstleister können ihren Sitz im Ausland haben, weshalb auch eine grenzüberschreitende Weitergabe der Daten ins Ausland möglich ist.

In anderen Fällen, soweit für die Weitergabe ihrer personenbezogenen Daten an Dienstleister aus datenschutzrechtlichen Gründen Ihre Einwilligung erforderlich ist, informieren wir Sie gesondert und übermitteln Ihre Daten nicht ohne Ihre vorherige Einwilligung.“

Insgesamt ist zweifelhaft, ob in die in der Datenschutzerklärung der HCA beschriebene Datennutzung wirksam eingewilligt werden kann. Auf der einen Seite trägt die Erklärung den Zulässigkeitsvoraussetzungen in dem Sinne Rechnung, dass der Betroffene über eine Einwilligung gesondert informiert wird. Inwiefern diese Aufklärung den datenschutzrechtlichen Voraussetzungen genügt, ist für die Autorinnen nicht absehbar, da die diesbezügliche Datenschutzerklärung nicht im Internet zu finden ist. Auf der anderen Seite fehlt es an der Bestimmtheit der Aufklärung insbesondere in Bezug auf die Weitergabe von Daten an Dritte. Es wird nicht deutlich, unter welchen Bedingungen Daten genutzt werden dürfen. Es ist nicht klar, was unter „soweit wir diese Dienstleister zu streng weisungsgebundenen Datenverarbeitung als Auftragsdatenverarbeiter verpflichtet haben, bedarf eine Datenverarbeitung ... keiner Einwilligung durch sie“ zu verstehen ist. Es ist nicht klar, wer diese Dienstleister sind, noch welche Daten genau an diese im Rahmen einer „Auftragsdatenverarbeitung“ weitergeleitet werden.

c. Eigene Geschäftszwecke § 28 BDSG

Fraglich ist ob die Verwendung und Erhebung von personenbezogenen Daten durch die HCA auf Grundlage von § 28 BDSG erlaubt ist. Punkt 2 der Datenschutzerklärung beschreibt die Verwendungszwecke:

„ Die genannten Datenkategorien nutzen wir – und soweit dafür ihr Einverständnis erforderlich nur mit Ihrem Einverständnis – zur

- Bereitstellung der Funktionalitäten der App sowie der über die App angebotenen Dienste [Nutzer-Stammdaten, Geräte-Stammdaten, Geräte-Nutzungsdaten]
- Beseitigung von Störungen [Geräte-Stammdaten, Geräte-Nutzungsdaten]

- Verbesserung der Benutzerfreundlichkeit der App [App-Nutzungsdaten]
- Verbesserung unseres Produkt- und Dienstleistungsangebots, insbesondere im Hinblick auf nicht genutzte Programme und sonstige Funktionen der App und des Hausgerätes [Geräte-Nutzungsdaten, App-Nutzungsdaten]“

Die Autorinnen halten die Datenschutzerklärung der HCA für teilweise unzulässig gem. § 28 I Nr. 1 BDSG. Wie oben ausgeführt, leitet sich die Zweckbestimmung aus den dem Rechtsgeschäft zugrunde liegenden Willenserklärungen ab; es muss ein unmittelbarer sachlicher Zusammenhang geben zwischen Datenerhebung und Geschäftszweck geben. Dabei sind die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten. Vor diesem Hintergrund muss der Geschäftszweck ohne die Daten nicht erreichen lassen.

Hinsichtlich der Bereitstellung der Funktionalität der App und ihrer Dienste sowie der Beseitigung von Störungen gibt es einen sachlichen Zusammenhang zwischen Datenerhebung und Geschäftszweck. Die Nutzer- und Gerätestammdaten sind erforderlich, um den Nutzer und Empfänger der Dienstleistungen zu identifizieren. Dazu gehört auch die IP-Adresse des Nutzers, welche nach § 15 TMG zulässigerweise erhoben werden kann. Damit sind diese Daten notwendig für die Funktionalität der App und ihrer Dienste. Ebenso ist die Beseitigung von Störungen abhängig von diesen Daten und notwendig für die Erreichung des Vertragszwecks und der Erbringung der Vertragsleistung (Zur-Verfügung-Stellen einer funktionsfähigen App).

Allerdings erscheinen die Erhebung und Verarbeitung von App- und Gerätenutzungsdaten nicht für Zwecke der Verbesserung der Benutzerfreundlichkeit und des Produkts- und Dienstleistungsangebots erforderlich. Die Erbringung der Leistung (funktionsfähige App) hat zunächst einmal nichts mit ihrer Benutzerfreundlichkeit zu tun. Dabei handelt es sich nicht um zugrundeliegende Vertragszwecke, sondern vielmehr um Kundenservice und –bindungszwecke. Sie sind nicht erforderlich, um die Funktionalität der App an sich zu gewährleisten. Daher sind unter Berücksichtigung der Grundsätze der Datenvermeidung und Datensparsamkeit die Erhebung und Verwertung der App- und Gerätenutzungsdaten zu solchen Zwecken nicht gem. § 28 I Nr. 1 BDSG zulässig.

Die Erhebung und Verarbeitung von App- und Gerätenutzungsdaten ist auch nicht nach § 28 I Nr. 1 BDSG zulässig, da in der Abwägung zwischen dem berechtigten wirtschaftlichen Interesse des die App anbietenden Unternehmens und dem schutzwürdigen Interesse des Betroffenen letzteres überwiegt. Wie oben erwähnt, muss das Interesse an der Datennutzung im Hinblick auf seinen Zweck, den Verwendungsspielraum für Datenerhebungen und –nutzung einzuschränken und dem Recht der informationellen Selbstbestimmung dagegen möglichst weite Geltung auch in Anbetracht von Einschränkungen zu verschaffen, restriktiv ausgelegt werden. Aus den Daten über die Nutzung der App und des Haushaltgeräts lassen sich Rückschlüsse auf das Verhalten und die Nutzungsgewohnheiten des Betroffenen schließen. Damit geht es nicht mehr um eine rein technische Nutzung der Daten, sondern um das Verstehen von Nutzungs- und Verhaltensmustern, die es dem datenerhebenden Unternehmen ermöglichen, Produkte und Dienstleistungen entsprechend anzupassen.

Es lässt sich festhalten, dass die HCA in mehrerer Hinsicht nicht den Anforderungen des TMG und des BDSG genügt. Hinsichtlich der Einwilligung ist es zumindest unter Zugrundlegung der Datenschutzerklärung (unter Nichtberücksichtigung der Einholung gesonderter Einwilligungen) unzulässig, nicht konkret den Umfang der Einwilligung zu benennen und von der Datenerhebung und –speicherung zu Geschäftszwecken abzutrennen. Der Verbraucher wird hier nicht in eine Lage versetzt, in der er sein Recht auf informationelle Selbstbestimmung in Kenntnis der tatsächlichen Sachlage ausüben kann. Darüber hinaus sind die Bestimmungen bezüglich der Daten von App- und Gerätenutzung nicht vom Vertragszweck gedeckt. Ob darüber hinaus eine Einwilligung vom Betroffenen eingeholt wird, hängt von der AGB-Kontrolle ab.

Es bleibt weiterhin festzustellen, dass die in den AGB enthaltene Einwilligung jedenfalls nicht den neuen Rahmenbedingungen der DSGVO gerecht wird. Gem. Erwägungsgrund 32 soll eine Einwilligung „differenziert“ möglich sein, d.h. verschiedene Datenverarbeitungsvorgänge bedürfen getrennten Einwilligungen. Eine solche Differenzierung ist in den AGB der HCA AGB nicht möglich. Vielmehr wird eine Globaleinwilligung für alle Datenverarbeitungsprozesse (mit Ausnahme der App-Nutzungsdaten, s. Nr. 5 der Datenschutzerklärung der HCA) verlangt.

3. Wirksamkeit nach AGB-Recht

Damit also die Datenschutzerklärung der HCA einer AGB-Kontrolle unterzogen werden kann, muss es sich bei ihr auch um AGB handeln. Vorliegend gibt es neben der Datenschutzerklärung auch Nutzungsbedingungen für die HCA sowie Nutzungsbedingungen für das Home Connect System. Für die Nutzungsbedingungen für die HCA gilt, dass diese mit Abschluss der Registrierung bindende Vertragsgrundlage für die Nutzung der HCA, werden.

a. Datenschutzerklärung als AGB

In den Nutzungsbedingungen für das Smart Home System findet sich unter Punkt 13 „Datenschutzrechtliche Einwilligung“ ein Abschnitt zum Thema Datennutzung:

„Sie willigen ein, dass die Home Connect GmbH Ihre Registrierungsdaten, Daten aus der Nutzung der App und Daten aus der Nutzung des Hausgeräts ("Personenbezogenen Daten") erheben, verarbeiten und nutzen darf, um Ihre möglichen Interessen an bestimmten Produkten und Dienstleistungen der Home Connect GmbH und von Dritten für Werbezwecke zu ermitteln und entsprechend dieser ermittelten Interessen Produkt- und Dienstleistungsinformationen innerhalb der App darzustellen. Die für diese Zwecke verarbeiteten Personenbezogenen Daten umfassen: Registrierungsdaten: Vor- und Nachname, E-Mail-Adresse, durch die Verbindung mit dem Hausgerät automatisch erhobene Informationen zur Art und zum Model des Haushaltsgeräts. Daten aus der Nutzung der App: Verwendete Funktionen und Bereiche der App, erteilte Befehle zur Steuerung des Hausgeräts, aufgerufene Rezeptempfehlungen, IP-Adresse, Interaktion mit Werbeeinblendung. Daten aus der Nutzung des Hausgeräts: Art

und Model des Hausgeräts, verwendete Programme, Standort des Hausgeräts, Wasserhärte am Standort des Hausgeräts und Nutzungsweise des Hausgeräts“

Diese datenschutzrechtliche Einwilligung ist für eine unbestimmte Anzahl von Verträgen vorformuliert, die der App-Anbieter dem Verbraucher vorlegt. Der Verbraucher hat zumeist keine andere Wahl, als diese zu akzeptieren. Nach der oben genannten Definition handelt es sich zumindest hierbei um AGB, welche einer Inhaltskontrolle nach den §§ 305 ff. BGB unterzogen werden kann.

b. Klauselverbote mit Wertungsmöglichkeit, § 308 BGB

Zunächst könnte untersucht werden, ob die Bestimmungen der Datenschutzerklärung der HCA gegen § 308 BGB verstößt. § 309 BGB erscheint nicht einschlägig.

Beispielsweise ist zu untersuchen, ob Nr. 8 der Datenschutzerklärung gegen § 308 BGB verstößt. Der Punkt ist mit „Änderung der Datenschutzerklärung“ überschrieben und besagt:

Im Zuge der Weiterentwicklung der App – unter anderem bedingt durch die Implementierung neuer Technologien oder die Einführung neuer Dienstleistungen – kann es erforderlich werden, diese Datenschutzerklärung anzupassen. Home Connect behält sich das Recht vor, die vorliegende Erklärung nach Bedarf zu ändern oder zu ergänzen. Home Connect wird immer die aktuelle Fassung der Datenschutzerklärung in der App hinterlegen, so dass Sie sich jederzeit über die aktuelle Fassung der Datenschutzerklärung informieren können.

Diese Klausel könnte einen unzulässigen Änderungsvorbehalt darstellen, § 308 Nr. 4. Danach ist die Vereinbarung eines Rechts des Verwenders, die versprochene Leistung zu ändern oder von ihr abzuweichen, unzulässig, wenn nicht die Vereinbarung der Änderung oder Abweichung unter Berücksichtigung der Interessen des Verwenders für den anderen Vertragsteil zumutbar ist. Das LG Berlin hat in einem Fall die Google-Nutzungsbedingungen betreffend¹⁴¹ geurteilt, dass eine Klausel zur Aktualisierung gegen §§ 307 I i.V.m. II Nr. 1, 307 II, 308 Nr. 4 BGB verstößt, da nach der kundenfeindlichsten Auslegung die beanstandete Klausel so zu verstehen ist, dass sich die Änderung der Bedingungen auch auf bereits getroffene Vereinbarungen auswirkt, was nach § 305 Abs. 2 BGB unzulässig ist. In Bezug auf Punkt 8 Änderung der Datenschutzerklärung bedeutet das, dass auch diese Klausel nach der verbraucherfeindlichsten Auslegung dahingehend verstanden werden muss, dass sich die Änderung der Bedingungen auf die getroffenen Vereinbarungen in der Datenschutzerklärung auswirkt. Aus der Klausel ergibt sich jedoch, dass man sich jederzeit über die aktuelle Fassung der Datenschutzerklärung informieren kann, welche in der App hinterlegt ist. In diesem Zusammenhang wird der Verbraucher jedoch nicht darüber aufgeklärt, ob überhaupt eine Änderung stattfand. Dies müsste er dann sozusagen selbst herausfinden. Das ist ihm nicht zumutbar, da dies eine permanente Kontroll- und Prüfpflicht bedeuten würde. Die Klausel ist nach § 308 Nr. 4 BGB unwirksam. Die jederzeitige Abänderbarkeit der Datenschutzbestimmungen verstößt zudem gegen die §§ 4, 4a BDSG,

¹⁴¹ LG Berlin, Urteil vom 19.11.2013 - 15 O 402/12.

wonach die Einwilligung klar und auf eine hinreichend bestimmte Datenerhebung und -nutzung beschränkt sein muss.

c. Unangemessene Benachteiligung, § 307 BGB

Bedenken bestehen jedoch bezüglich § 307 I 1 BGB, wonach eine unangemessene Benachteiligung entgegen Treu und Glauben vorliegt. Danach ist im Zweifel eine unangemessene Benachteiligung des Vertragspartners anzunehmen, wenn von den wesentlichen Grundgedanken des (dispositiven) Gesetzesrechtes in einer nicht zu vereinbarenden Weise abgewichen wird. Der Schwerpunkt der Prüfung liegt also in der Klärung der Frage, ob eine Abweichung vom materiellen Gesetzesrecht vorliegt.

Nr. 4 „Übermittlung oder Weitergabe Ihrer Daten an Dritte“ der HCA-Datenschutzerklärung könnte hier auf Vereinbarkeit mit § 307 II NR. 1 BGB überprüft werden. Sie besagt:

Zur Realisierung der App und der darüber angebotenen Dienstleistungen arbeiten wir mit verschiedenen Dienstleistern zusammen. Soweit wir diese Dienstleister zur streng weisungsgebundenen Datenverarbeitung als Auftragsdatenverarbeiter verpflichtet haben, bedarf eine Datenverarbeitung durch diese Dienstleister keiner Einwilligung durch Sie. Die entsprechenden Dienstleister können ihren Sitz im Ausland haben, weshalb auch eine grenzüberschreitende Weitergabe der Daten ins Ausland möglich ist.

In anderen Fällen, soweit für die Weitergabe Ihrer personenbezogenen Daten an Dienstleister aus datenschutzrechtlichen Gründen Ihre Einwilligung erforderlich ist, informieren wir Sie gesondert und übermitteln Ihre Daten nicht ohne Ihre vorherige Einwilligung.

Das LG Berlin hat in seinem Urteil bezüglich der Google-Nutzungsbedingungen¹⁴² eine Klausel zur Datensicherheit im Falle eines Unternehmenszusammenschlusses oder –erwerbs für unzulässig gem. § 307 Abs. 1 i.V.m. Abs. 2 Nr. 1 BGB, §§ 12 ff. TMG, §§ 4, 4a BDSG erklärt, da sich die Klausel auf zukünftige Umstände bezieht. Eine solche zukünftige Weitergabe könne nur durch Einwilligung des Verbrauchers im Bedarfsfalle legitimiert werden. Eine Blanko-Einwilligung ohne Hinweise auf konkrete Umstände erfüllt nicht die Anforderungen an eine wirksame Einwilligung. Soweit sich Google darauf berief, dass bei Unternehmenszusammenschlüssen keine Weitergabe der Daten an Dritte erfolge, handelte es sich lediglich um einen Teilaspekt der verwendeten Klausel. Dem Verbraucher sei bei Abgabe seiner Willenserklärung nicht hinreichend deutlich, an wen seine Daten möglicherweise weitergegeben werden und ob diese, wie von Google behauptet, „vertraulich“ behandelt werden. Ähnlich liegt der Fall hier: Es wird lediglich behauptet, dass dritte Dienstleister zur „weisungsgebundenen Datenverarbeitung“ verpflichtet seien; eine konkrete Nennung dieser Dienstleister erfolgt nicht. Außerdem wird eine grenzüberschreitende Weitergabe der Daten ins Ausland als potenziell möglich in Aussicht gestellt: In diesem Zusammenhang stellen sich mehrere klärungsbedürftige Fragen: In welches Ausland werden die Daten übermittelt? Darüber hat der App-Nutzer keine Kontrolle,

¹⁴² LG Berlin, Urteil vom 19.11.2013 - 15 O 402/12.

da diese „überall“ sein könnten. Zudem werden auch die Drittdienstleister nicht offen gelegt. Zwar sind diese ausweislich der Bestimmung streng weisungsgebunden, es ist aber dennoch unklar zu welchem Zweck genau die Daten weitergegeben werden. „Weisungsgebundenheit“ schließt zudem das vertrauliche Behandeln nicht ein. Eine Einwilligung, zur Datenweitergabe an unbekannte zwar weisungsgebundene Drittdienstleister, für nicht erforderlich zu bestimmen, hat sodann die Nichtigkeit nach § 307 Abs. 2 Nr. 1 BGB zur Folge.

Auch Nr. 5 zur Erfassung der App-Nutzung könnte gegen § 307 II Nr. 1 BGB verstoßen. Der Wortlaut der Nr. 5 ist wie folgt:

Die App bietet die Möglichkeit zur Erfassung von App-Nutzungsdaten (siehe oben 1.d.) und setzt dazu den Dienst Adobe Analytics von Adobe Systems Software Ireland Limited, ... (nachfolgend „Adobe“) ein.

Soweit die Funktion „Nutzungsdaten erfassen“ aktiviert ist, werden App-Nutzungsdaten an einen Server von Adobe gesendet, die eine Analyse der Benutzung der App durch Sie ermöglichen (siehe oben 1.d.). Die App-Nutzungsdaten werden in der Regel an einen Server von Adobe in den USA übertragen und dort gespeichert. Für diese App wurde die IP-Anonymisierung aktiviert, so dass die von Ihnen verwendete IP-Adresse zuvor gekürzt wird. Im Auftrag von Home Connect wird Adobe diese Informationen benutzen, um Ihre Nutzung der App auszuwerten und um Reports über die App-Aktivitäten für Home Connect zusammenzustellen. Die im Rahmen von Adobe-Analytics von Ihrem mobilen Endgerät übermittelte IP-Adresse wird ohne Ihr gesondertes Einverständnis nicht mit anderen Daten von Adobe oder von Home Connect zusammengeführt.

Sie können die Erfassung von App-Nutzungsdaten (inkl. Ihrer IP-Adresse) durch Adobe sowie die Verarbeitung dieser Daten durch Adobe steuern, indem Sie die Funktion „Nutzungsdaten erfassen“ aktivieren oder deaktivieren. Je nach Rechtslage in Ihrem Land kann es sein, dass die Funktion „Nutzungsdaten erfassen“ standardmäßig aktiv ist.

Zunächst ist festzustellen, dass die Verkürzung der IP-Adresse ein geeignetes Mittel der Anonymisierung ist und datenschutzrechtlichen Vorgaben entspricht.¹⁴³ Die Zusammenführung der IP-Adresse mit anderen Daten von Adobe Analytics oder der HCA wird nicht ohne eine abzurufende Einwilligung geschehen.

Allerdings ist die Zulässigkeit der Aktivierungs- bzw. Deaktivierungsfunktionen der HCA fraglich. Wiederum das LG Berlin hatte geurteilt, dass eine Regelung dem Transparenzgebot widerspreche, wenn es Sache des Verbrauchers wird, sich die Bedingungen, die auf sein Nutzungsverhältnis anzuwenden sind, zusammenzusuchen. Aus der Klausel selbst ist nicht klar erkennbar, welche Konditionen auf sein konkretes Rechtsverhältnis anwendbar sind. So

¹⁴³ Der Sächsische Datenschutzbeauftragte hat Richtlinien in diesem Sinne veröffentlicht, <<https://www.saechsdsb.de/ipmask>> (zuletzt abgerufen am 30.11. 2016).

weiß er nicht, ob die Funktion „Nutzungsdaten erfassen“ schon als Voreinstellung aktiviert ist oder nicht. Ist dies der Fall werden Benutzungsanalysen durchgeführt. Wo diese stattfinden ist zudem unklar, da in der Bestimmung von „in der Regel USA“ die Rede ist. Zwar wird ausgesagt, dass die Verarbeitung der Daten durch Adobe gesteuert werden kann, indem die Funktion „Nutzungsdaten erfassen aktiviert oder deaktiviert werden kann“ – es ist jedoch fraglich, ob dann jegliche Benutzungsanalyse unterlassen wird, da dies nicht explizit aus der Bestimmung hervorgeht. Die Klausel verstößt somit nach Auffassung der Verfasserinnen gegen das Transparenzgebot und ist nach § 307 Abs. 2 Nr. 1 BGB unwirksam.

Außerdem könnte Punkt 2 der HCA-Datenschutzerklärung ebenfalls nach § 307 Abs. 2 Nr. 1 BGB unwirksam sein:

Die genannten Datenkategorien nutzen wir – und soweit dafür Ihr Einverständnis erforderlich nur mit Ihrem Einverständnis – zur

- Bereitstellung der Funktionalitäten der App sowie der über die App angebotenen Dienste (1.a.-c.)
- Beseitigung von Störungen (1.b. und c.)
- Verbesserung der Benutzerfreundlichkeit der App (1.d.)
- Verbesserung unseres Produkt- und Dienstleistungsangebots, insbesondere im Hinblick auf nicht genutzte Programme bzw. häufig genutzte Programme und sonstige Funktionen der App und des Hausgerätes (1.c. und d.)

Das LG Berlin hat in einer Entscheidung über die Datenschutzklauseln von Apple¹⁴⁴ entschieden, dass eine Pauschaleinwilligung in verschiedene Datenerhebungen zu verschiedenen Zwecken unwirksam gem. §§ 307 I i.V.m. II Nr. 1 BGB, 4, 4a BDSG, 12, 13 TMG ist, da sie den Eindruck einer zwingenden, nicht zu verhindernden Einwilligung seitens des Verbrauchers erweckt. In Nummern 1 und 2 der HCA-Datenschutzerklärung sind die einzelnen Datenkategorien einzelnen Zwecken zugeordnet; allerdings ist zumindest die Formulierung „Verbesserung der Benutzerfreundlichkeit der App und Verbesserung unseres Produkt- und Dienstleistungsangebots, insbesondere im Hinblick auf nicht genutzte Programme bzw. häufig genutzte Programme und sonstige Funktionen der App und des Hausgerätes“ beinahe identisch mit der dem LG Berlin vorliegenden rechtswidrigen Klausel von Apple.¹⁴⁵ Folgt man der Argumentation des LG Berlin kann man darin ebenfalls eine Pauschaleinwilligung sehen, die den Eindruck einer zwingenden, nicht zu verhindernden Einwilligung seitens des Verbrauchers, weckt. Die Klausel wäre danach ebenfalls gemäß § 307 Abs. 2 Nr. 1 BGB unwirksam.

¹⁴⁴ LG Berlin, Urteil vom 30.04.2013 - 15 O 92/12.

¹⁴⁵ LG Berlin, Urteil vom 30.04.2013 - 15 O 92/12.

d. Rechtsfolgen

Generell bleibt der restliche Vertrag bestehen und von der Unwirksamkeit einer AGB-Klausel unberührt, § 306 I BGB. Die Klauselrichtlinie regelt nicht, wie die unverbindliche Klausel ersetzt wird.¹⁴⁶ Ob und wie die Lücken geschlossen werden, ist Sache der Mitgliedstaaten.¹⁴⁷

Durch das gesetzliche Verbot der geltungserhaltenden Reduktion, das von der Rechtsprechung ausgestaltet wurde, soll dem Normzweck des AGB-Rechts Rechnung getragen werden.¹⁴⁸ Konnte der Verwender von AGB darauf vertrauen, eine unzulässige Klausel werde im Streitfall vom Gericht auf das gerade noch zulässige Maß reduziert, wäre nicht der Anreiz gegenüber dem Verwender gesetzt, unzulässige Klauseln zu vermeiden.¹⁴⁹ Nach allgemeiner Ansicht kommt allerdings für die Verbandsklage eine geltungserhaltende Reduktion ebenso wenig in Betracht, wie eine ergänzende Vertragsauslegung.¹⁵⁰ Grund dafür ist, dass es anders als im Individualprozess, um einen allgemeinen, rein vorbeugenden Schutz des Rechtsverkehrs vor unangemessenen Bestimmungen geht und sich ein solcher Schutz mit einer geltungserhaltenden Reduktion nicht verträgt.¹⁵¹

Die Wechselwirkung zwischen AGB-Recht und Datenschutzrecht ist nicht ganz klar. Wendehorst argumentiert wegen des Verweises auf Richtlinie 93/13/EG¹⁵² für einen umfassenden Prüfungsmaßstab für AGB- und Einwilligungskontrolle gleichermaßen. Darüber hinaus dürften dieselben Umstände, die eine AGB-Klausel unwirksam machen, auch zu einer Unwirksamkeit der datenschutzrechtlichen Einwilligung führen.¹⁵³ Damit dürfte auch

¹⁴⁶ Basedow, *Münchener Kommentar zum BGB*, Säcker/Rixecker/Oetker/Limberg (Hrsg.), 7. Auflage 2016, C.H. Beck Verlag, Rn. 4 zu § 306 BGB; Schmidt, *AGB-Recht Kommentar zu den §§ 305-310 BGB und zum UKlaG*, Ulmer/Brandner/Hensen (Hrsg.), 12. Auflage 2016, Otto Schmidt Verlag, Rn. 4c zu § 306 BGB; Wolf, *AGB-Recht Kommentar*, Wolf/Lindacher/Pfeiffer (Hrsg.), 6. Auflage 2013, C.H. Beck Verlag, Rn. 7 zu RL Art. 6.

¹⁴⁷ Wolf, *AGB-Recht Kommentar*, Wolf/Lindacher/Pfeiffer (Hrsg.), 6. Auflage 2013, C.H. Beck Verlag, Rn. 7 zu RL Art. 6.; Heinrichs, „Das Gesetz zur Änderung des AGB-Gesetzes Umsetzung der EG-Richtlinie über mißbräuchliche Klauseln in Verbraucherverträgen durch den Bundesgesetzgeber“, (1996), *Neue Juristische Wochenschrift*, Heft 34, S. 2190-2197, S. 2195 f.; Schmidt, *AGB-Recht Kommentar zu den §§ 305-310 BGB und zum UKlaG*, Ulmer/Brandner/Hensen (Hrsg.), 12. Auflage 2016, Otto Schmidt Verlag, Rn. 4c zu § 306 BGB.

¹⁴⁸ Peterhänsel, *Nomos Kommentar Gesamtes Arbeitsrecht*, Boecken/Düwell/Diller/Hanau (Hrsg.), Nomos Verlag 2016, Rn. 12 zu § 306 BGB.

¹⁴⁹ Ibid.

¹⁵⁰ BGH, Urteil vom 13.12.2006 - VIII ZR 25/06 (OLG Köln); Schmidt, *Beck'scher Online-Kommentar BGB*, Bamberger/Roth (Hrsg.) 40. Edition 2016, C.H. Beck Verlag, Rn. 14 zu § 306 BGB.; Schmidt, *Vertragsfolgen der Nichteinbeziehung und Unwirksamkeit von Allgemeinen Geschäftsbedingungen*, (Deutscher Fachverlag, 1986), S. 136 f.; aA Graf v. Westphalen, „AGB-Recht im Jahr 2006“, (2007), *Neue Juristische Wochenschrift*, Heft 31, S. 2228-2236, S. 2230.

¹⁵¹ Basedow, *Münchener Kommentar zum BGB*, Säcker/Rixecker/Oetker/Limberg (Hrsg.), 7. Auflage 2016, C.H. Beck Verlag, Rn. 12 zu § 306 BGB; Schlosser, *Kommentar zum Bürgerlichen Gesetzbuch: Staudinger BGB - Buch 2: Recht der Schuldverhältnisse §§ 305-310; UKlaG (Recht der Allgemeinen Geschäftsbedingungen)*, Staudinger (Hrsg.), 15. Auflage 2013, De Gruyter Verlag, Rn. 28 zu § 306 BGB; anders noch Hager, *Gesetzes- und sittenkonforme Auslegung und Aufrechterhaltung von Rechtsgeschäften*, (C.H.Beck Verlag, 1983), S. 71.

¹⁵² Richtlinie 93/13/EG des Rates vom 5. April 1993 über mißbräuchliche Klauseln in Verbraucherverträgen, ABI Nr. L 095 vom 21/04/1993 S. 0029 - 0034

¹⁵³ Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016), S. 56-57.

Datenerhebung und –verarbeitung, die aufgrund von § 28 I Nr. 1, Nr. 2 BGB, Art. 6 I lit. b) DSGVO erlaubt ist von einer AGB-rechtlichen Unwirksamkeit nicht berührt bleiben.

Vor diesem Hintergrund haben wir gesehen, dass die Nummern 2, 4, 5 und 8 der HCA-Datenschutzerklärung sowohl aufgrund der §§ 305ff BGB sondern auch aufgrund mangelnder Erfüllung der datenschutzrechtlichen Voraussetzungen an die Einwilligung und *Geschäftszwecke* unwirksam. Die entsprechenden Datenerhebungen und –verarbeitung sind damit nicht gesetzlich erlaubt.

VI. Sonderproblem Drittbetroffenheit

Bei den Datenübertragungen im Smart Home kann es auch zur Erhebung und Verarbeitung von Daten Dritter (z.B. Bewegungsprofile von Wohnungsbesuchern) kommen. Soweit es sich um personenbezogene Daten handelt, ist das Recht dieser Dritten auf informationelle Selbstbestimmung aus Art. 2 I i.V.m. Art. 1 I GG betroffen. Teilnehmer und Nutzer eines Anschlusses sind gemeinschaftlich gegenüber über dem Mittler der Telekommunikation nach Art. 10 GG zu schützen; somit sollen auch die sie betreffenden Datenübertragungen selbst nach Außen vor dem Zugriff Dritter geschützt werden.¹⁵⁴ Dagegen erstreckt sich der Schutzbereich des Art. 13 GG nicht auf nur zufällig anwesende Personen wie Besucher.¹⁵⁵ Hierbei geht es nicht um die aktive Verarbeitung von Daten Dritter in der Cloud durch einen Verbraucher selbst (zum Beispiel durch das aktive Uploaden von Bildern oder Videos auf einem privaten Blog),¹⁵⁶ sondern um die passive Generierung von Daten durch bloße Anwesenheit in einem SmartHome.

Fraglich ist, ob und wie diese Daten Dritter geschützt werden können und müssen.

Vertragsrechtlich kommt ein Vertrag mit Schutzwirkung zugunsten Dritter in Betracht. Zu den Nebenpflichten in verschiedenen Vertragskonstellationen gehört die Einhaltung der Vorschriften des BDSG bei der Vertragsdurchführung.¹⁵⁷ Dies muss auch für die Bereitstellung von intelligenten Wohnsystemen gelten.

Beim von der Rechtsprechung entwickelten Vertrag mit Schutzwirkung zugunsten Dritter¹⁵⁸ ist der Grund für die Einbeziehung eines Dritten, dass diesem bei einer Schädigung, trotz

¹⁵⁴ Skimstins, *Smart Homes Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, (Nomos Verlag, 2016), S. 154-156.

¹⁵⁵ Ibid., S. 162.

¹⁵⁶ In diesem Fall wäre der Verbraucher selbst „verantwortliche Stelle“; Borges/Adler, „Datenschutz und Cloud Computing aus Verbrauchersicht“ in *Der Gläserne Verbraucher: Wird Datenschutz zum Verbraucherschutz-Beiträge zur Verbraucherforschung*, Bala/Müller (Hrsg.), (Band 1, 2014), S. 64.

¹⁵⁷ Z. B. Redeker, *Handbuch Multimedia-Recht Rechtsfragen des elektronischen Geschäftsverkehrs*, Hoeren/Sieber/Holznagel (Hrsg.), (C.H. Beck Verlag, 2015), Rn 244 in 42. Ergänzungslieferung, Teil 12 Vertragsrecht für Internetdienste sowie Karg, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 75 zu § 9 BDSG oder Panzer-Heemeier, *StichwortKommentar Arbeitsrecht*, Grobys/Panzer (Hrsg.), 2. Auflage, 8. Edition 2016, Nomos Verlag, Rn. 1-72 in Datenschutz, allgemein.

¹⁵⁸ Vgl. BGH, Urteil vom 14. 6. 2012 – IX ZR 145/11 (OLG Schleswig); BGH, Urteil vom 21.07. 2010 - XII ZR 189/08 (OLG Frankfurt a.M.); BGH, Urteil vom 12.01.2011 – VIII ZR 346/09 (LG Halle/Saale); BGH, Urteil vom 20.04.2004 - X ZR 250/02 (OLG Brandenburg); BGH, Urteil vom 02.07.1996 - X ZR 104/94 (Düsseldorf); Martiny, „Pflichtenorientierter Drittschutz beim Vertrag mit Schutzwirkung für

selber Gefahrenlage wie die des Vertragspartners, nur deliktische Ansprüche verbleiben, gegenüber welchen sich der Schädiger exkulpieren könnte sowie der Nicht-Existenz des vermuteten Verschulden i. S. d. § 280 Abs. 1 Satz 2 BGB im Deliktsrecht.¹⁵⁹ Um einen solchen Anspruch zu bejahen, muss die erkennbare Leistungsnähe des Dritten vorliegen, das erkennbare Schutzinteresse des Gläubigers sowie das Schutzbedürfnis des Dritten.¹⁶⁰

Das Tatbestandsmerkmal der Leistungsnähe ist erfüllt, wenn der Dritte bestimmungsgemäß mit der vertraglichen Hauptleistung in Berührung kommt und nach der Anlage des Vertrags den Leistungsgefahren in ähnlicher Weise ausgesetzt ist wie der Gläubiger selbst.¹⁶¹ Besucher sind der Datenerhebung bei Nutzung der verschiedenen Geräte einer Wohnung (z.B. Kühlschrank öffnen, Duschen, Nutzung der Toilettenspülung etc.) ebenso ausgesetzt wie der eigentliche Vertragspartner. Soweit entsprechende Daten personenbeziehbar gespeichert werden, besteht ein potenzielles Missbrauchsrisiko.¹⁶²

Fraglich ist also, ob Besucher-Daten, die von einem intelligenten Haussystem erfasst werden, überhaupt personenbeziehbar/personenbezogen sein können. Personenbezogene Daten sind grundsätzlich alle Informationen, die mit einer Person in Verbindung gebracht werden können.¹⁶³ Dies kann unmittelbar oder mittelbar geschehen.¹⁶⁴ Anders als der Vertragspartner (und ggf. seiner Mitbewohner wie Lebenspartner oder Familienangehörige) sind dem Dienstleister Daten wie Name und Wohnanschrift von einzelnen Besuchern jedoch nicht bekannt. Das Haussystem wäre somit in der Lage, Daten des Besuchs zwar zu erfassen, könnte diese jedoch nicht personenbeziehbar machen. Es wüsste aufgrund des Mehrgebrauchs, dass Gäste anwesend sind oder waren, jedoch nicht um welche Person es sich genau handelt.

Geht man allerdings davon aus, dass das Haussystem zur Identifikation im Stande wäre (z.B. Gesichtserkennung bei Klingeln an der Haustür und gleichzeitigem Abgleich mit der

Dritte - Eingrenzung uferloser Haftung“, (1996), *Juristenzeitschrift*, S. 19-25, S. 20; Kötz, *Europäisches Vertragsrecht*, (Mohr Siebeck Verlag, 1996), S. 381 ff.

¹⁵⁹ Gottwald, *Münchener Kommentar zum BGB*, Säcker/Rixecker/Oetker/Limberg (Hrsg.), 7. Auflage 2016, C.H. Beck Verlag, Rn. 164 ff. zu § 328 BGB § 328.

¹⁶⁰ S. zu den Voraussetzungen Zenner, „Der Vertrag mit Schutzwirkung zu Gunsten Dritter – Ein Institut im Lichte seiner Rechtsgrundlage“, (2009), *Neue Juristische Wochenschrift*, Heft 15, S. 1030-1034, S. 1031; die folgenden Ausführungen zur Schutzwirkung innerhalb familiärer Beziehungen gelten auch für nicht-eheliche Lebensgemeinschaften, Jagmann, *Kommentar zum Bürgerlichen Gesetzbuch: Staudinger BGB - Buch 2: Recht der Schuldverhältnisse §§ 328 - 345 (Vertrag zugunsten Dritter, Draufgabe, Vertragsstrafe)*, Suadinger (Hrsg.), 15. Auflage 2015, De Gruyter Verlag, Rn. 100 zu § 328 BGB.

¹⁶¹ Janoschek, *Beck'scher Online-Kommentar BGB*. Bamberger/Roth (Hrsg.) 40. Edition 2016, C.H. Beck Verlag, Rn. 51 zu § 328 BGB.

¹⁶² Skimstins, *Smart Homes Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, (Nomos Verlag, 2016), S. 300.

¹⁶³ Brühann, *Das Recht der Europäischen Union*, Grabitz/Hilf (Hrsg.), (C.H. Beck Verlag, 2009), Rn 6 zu Art. 2 Begriffsbestimmungen in A. EG-Verbraucher- und Datenschutzrecht (Art. 1 - Art. 34) in A 30. Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

¹⁶⁴ Brühann, *Das Recht der Europäischen Union*, Grabitz/Hilf (Hrsg.), (C.H. Beck Verlag, 2009), Rn 9 zu Art. 2 Begriffsbestimmungen in A. EG-Verbraucher- und Datenschutzrecht (Art. 1 - Art. 34) in A 30. Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Facebook-Freundesliste) müsste man prüfen, ob auch die anderen Tatbestandsmerkmale erfüllt sind.

Der Gläubiger müsste Interesse am Schutz des Dritten haben. Früher hat die Rechtsprechung diese Voraussetzung bejaht, wenn den Vertragsgläubiger eine Fürsorgepflicht gegenüber dem Dritten trifft, ob er also für dessen „Wohl und Wehe“ mitverantwortlich ist.¹⁶⁵ Als solche hat sie familien-, arbeits- und mietrechtliche Beziehungen angesehen. Jetzt ist erforderlich aber auch ausreichend, dass der Gläubiger an der Einbeziehung des Dritten ein besonderes Interesse hat und der Vertrag dahin ausgelegt werden kann, dass der Dritte in Anerkennung dieses Interesses in den vertraglichen Schutz einbezogen werden soll.¹⁶⁶ Das notwendige Interesse des Vertragspartners an dem Güterschutz zugunsten des Dritten richtet sich seiner Intensität nach ganz nach dem jeweiligen Schuldverhältnis, dem Vertragszweck und nach Treu und Glauben.¹⁶⁷ Je nach Besuch muss daher differenziert werden: Die beste Freundin, die jeden Tag zu Besuch kommt und mit welcher man ein familiäres Verhältnis hat, wird man ggf. dazu zählen können. Der Partner eines Bekannten, der als Begleiter bei einer Geburtstagsfeier beim Vertragspartner erscheint hingegen nicht.

Weitere Voraussetzung ist die Erkennbarkeit der Leistungsnähe und das Schutzinteresse des Gläubigers für den Schuldner. Der BGH erachtet es bei der Erkennbarkeit für ausreichend, dass der Vertragspartner aufgrund des Inhalts damit rechnen muss, dass weitere Dritte von dem Umgang mit persönlichen Informationen betroffen sein werden.¹⁶⁸ Der Dienstleister intelligenter Wohnsysteme wird ebenfalls davon ausgehen, dass regelmäßiger Besuch beim Vertragspartner erscheint.

Die Dritten sind auch schutzwürdig, da ihr Interesse nicht bereits durch eigene direkte vertragliche Ansprüche voll abgedeckt ist.¹⁶⁹ In Betracht kommen lediglich deliktische Ansprüche der Gäste. Bei einem Anspruch aus §§ 823 ff. BGB wird ein gesetzliches Schuldverhältnis begründet, jedoch kein vertragliches.

Kommt man also zu dem Ergebnis, dass Besuch in bestimmten Fällen unter dem Interesse des Gläubigers am Schutz des Dritten stehen, käme ein Anspruch nach §§ 280 Abs. 1, Abs. 3, 241 Abs. 2 i. V. m. Vertrag über das intelligente Wohnsystem in Betracht. Problematisch ist in diesem Zusammenhang jedoch, wie in anderen Fällen, die Berechnung des entstandenen Schadens. Dieser ist in jedem Fall immaterieller Natur. Die Schadenshöhe richtet sich wiederum danach, welche Werteinbuße der Besucher durch den

¹⁶⁵ BGH, Urteil vom 26.06.2001 - X ZR 231/99 (Frankfurt a.M.); BGH, Urteil vom 26.11.1968 - VI ZR 212/66 (Düsseldorf); BGH, Urteil vom 30. 9. 1969 - VI ZR 254/67 (Braunschweig) ; BGH, Urteil vom 12.07.1977 - VI ZR 136/76 (Stuttgart).

¹⁶⁶ Janoschek, *Beck'scher Online-Kommentar BGB*, Bamberger/Roth (Hrsg.) 40. Edition 2016, C.H. Beck Verlag, Rn. 52 zu § 328 BGB.

¹⁶⁷ BGH, Urteil vom 22.01.1968 - VIII ZR 195/65 (Hamm).

¹⁶⁸ BGH, Urteil vom 20.04.2004 - X ZR 250/02 (OLG Brandenburg).

¹⁶⁹ BGH, Urteil vom 18.02.2014 – VI ZR 383/12; BGH, Urteil vom 12.01.2011 - VIII ZR 346/09 (LG Halle/Saale); BGH, Urteil vom 22.07.2004 - IX ZR 132/03 (OLG Köln); BGH, Urteil vom 02.07.1996 - X ZR 104/94 (Düsseldorf)); BGH, Urteil vom 20.03.1995 - II ZR 205/94 (Düsseldorf) u. a.

Datenmissbrauch erlitten hat und damit nach der grundsätzlichen Frage, welchen Wert man Daten zumisst.

Aus datenschutzrechtlicher Sicht ist für Fälle, in denen personenbezogene Daten Dritter verwendet werden, das Einverständnis dieser erforderlich. Über § 28 BDSG, der den Zweck des Schuldverhältnisses in den Vordergrund stellt, wird jedoch auch der Kreis der jeweils verwendbaren Daten ausgeweitet. Daher richtet sich die Zulässigkeit und der Umfang von Erhebungen von Daten Dritter nach dem zugrundeliegenden rechtsgeschäftlichen Schuldverhältnis.¹⁷⁰ Das Einverständnis der Überweisungsempfänger braucht infolgedessen nicht eingeholt werden. Somit kann der Erlaubnistatbestand des § 28 BDSG hier indirekt eine rechtfertigende Wirkung haben.¹⁷¹ Die Einwilligung der Dritten ist nur dann unerlässlich, wenn die in Frage stehenden Daten über die für das jeweilige Vertragsverhältnis erforderlichen Informationen hinausgehen und die Grundlage für die Begründung eigenständiger Pflichten des Betroffenen darstellen.¹⁷²

Festzuhalten bleibt, dass die Rechtsposition Dritter im IoT nicht vollständig klar ist. Die Entscheidungen über die Anwendung eines Vertrages mit Schutzwirkung zugunsten Dritter sowie über die Anwendbarkeit des BDSG hängen maßgeblich davon ab, ob die Daten des Dritten personenbeziehbar sind. Dies ist eine technische Frage. Sollten die Daten personenbeziehbar sein, stellen sich eine Reihe praktischer Probleme, wie zum Beispiel die Machbarkeit der Einholung einer Einwilligung. Darüber hinaus stellt sich durch eine potentielle Anwendung des § 28 BDSG die Frage, inwiefern die sich ausbreitende Datenerhebung und –verarbeitung über „Geschäftszwecke“ gerechtfertigt sein kann oder sollte.

VII. Zusammenfassung der materiell-rechtlichen Probleme

Zusammenfassend lässt sich festhalten, dass der Datenschutz im IoT auf verschiedenen Ebenen eine große Rolle spielt. Dabei ergeben sich auch einige materiell-rechtliche Probleme.

Insbesondere stellen sich Fragen der Wirksamkeit von Einwilligungen gem. § 4 BDSG, Art. 6 I lit. a) DSGVO und der Aushöhlung des Einwilligungserfordernisses sowie des Grundsatzes der Datensparsamkeit durch eine sich ausbreitende Anwendung des § 28 BDSG, Art. 6 I lit. b) DSGVO. Eine etwaige Ausbreitung der Anwendung von § 28 BDSG in der Praxis sollte daher sorgfältig beobachtet werden. Wendehorst beobachtet schon jetzt einen „Paradigmenwechsel“ von einschränkenden Leistungsbeschreibungen im Vertragsrecht zu ausufernden Leistungsbeschreibungen im IoT, um möglichst viele Kundendaten erheben und nutzen zu können.¹⁷³ Dies ist eine ernstzunehmende Besorgnis, umso mehr, als dass die

¹⁷⁰ Simitis, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 63zu § 28 BDSG mit Beispielen.

¹⁷¹ Am Beispiel des vernetzten Fahrzeugs: So Roßnagel, „Fahrzeugdaten – wer darf über sie entscheiden?“, (2014), *Straßenverkehrsrecht*, Heft 8, S. 281-287, S. 281.

¹⁷² Simitis, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 64zu § 28 BDSG mit Beispielen.

¹⁷³ Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016), S. 51.

Zweckbestimmung im Rahmen des § 28 BDSG nur zur Selbstbindung nach Treu und Glauben führt und nachträgliche Zweckänderungen möglich sind. In Bezug auf Daten Dritter ist unklar, wie – sollten denn die erhobenen und verarbeiteten Daten personenbeziehbar sein und so das BDSG Anwendung finden – eine Einwilligung des Dritten in der Praxis eingeholt werden kann und von wem. Bezüglich der Legitimierung von Datenerhebungen und –verarbeitung aufgrund des § 28 BDSG ist zu fragen, inwiefern der in den Erklärungen angegebene Zweck tatsächlich auch ein Zweck ist, der zur Vertragsdurchführung notwendig ist. Im Beispiel der HCA haben wir festgestellt, dass dies nicht unbedingt der Fall ist.

Im Hinblick auf die meist formularmäßige Einwilligung in Datenerhebungen muss berücksichtigt werden, dass sich Verbraucher oft in einer strukturell unterlegenen Verhandlungsposition befinden und daher die Freiwilligkeit der Einwilligung in Frage gestellt werden kann. Zwar ist das Kopplungsverbot auch dahingehend zu verstehen, dass unterschwellige Drucksituationen vermieden werden sollen, aber dies ist nicht genug um die Freiwilligkeit der Einwilligung und die strukturellen Ungleichgewichte, die nicht durch die Kopplung von Einwilligung und Leistung entstehen, zu verhindern.

Die Kontrollierbarkeit von Datenschutzerklärungen nach AGB-Recht bei Vorlage der Voraussetzungen des § 305 I BGB ist grundsätzlich zu begrüßen. Die beispielhafte Überprüfung der HCA-Datenschutzerklärung im Lichte der §§ 307, 308 BGB bringt zu Tage, dass einige Klauseln unwirksam sein könnten, da sie den Verbrauchern einseitige Prüf- und Kontrollpflichten bzgl. Änderungen der Klauseln auferlegen und weil sie wegen mangelnder Aufklärung über die Weitergabe von Daten Dritter Verbraucher unangemessen benachteiligen.

E. Rechtsdurchsetzung

Die Möglichkeit der Rechtsdurchsetzung ist, zusammen mit dem Accountability Principle, ein grundlegendes Prinzip in den OECD Guidelines. Im IoT kommt es allerdings nicht nur zu materiell-rechtlichen Problemfällen. Auch die Rechtsdurchsetzung im internationalen Datenmarkt stellt Verbraucher vor Probleme, weil zum einen bestimmte Ansprüche nicht bestehen und zum anderen selbst bestehende Rechte vor faktische Hindernisse gestellt werden.

Im Folgenden werden die verschiedenen Rechtsdurchsetzungsmöglichkeiten und ihre Probleme dargestellt.

I. Nationaler Rechtsschutz

1. Individueller Rechtsschutz

a. Auskunftsansprüche, §§ 19, 34 BDSG, Art. 15 DSGVO

Auskunftsansprüche werden als grundlegend zur Effektuierung des Rechts auf informationelle Selbstbestimmung angesehen. Im BDSG ist ein formloses Auskunftsrecht gem. §§ 19, 34 verankert. Das Auskunftsrecht dient der Erfüllung der Kernforderungen des

Volkszählungsurteils, in welchem das BVerfG entschied, dass Bürger wissen sollen, „wer was wann und bei welcher Gelegenheit“ über sie weiß.¹⁷⁴

Das Auskunftsrecht gehört zu den unabdingbaren Rechten des Betroffenen.¹⁷⁵ Das Recht auf Auskunft versetzt den Betroffenen erst in die Lage, weitere Rechte bei unzulässiger Datenverarbeitung geltend zu machen. Es wird ergänzt durch das Benachrichtigungsrecht des Betroffenen gem. § 33 BDSG, wonach dieser vor der erstmaligen Erhebung und Übermittlung seiner personenbezogenen Daten grundsätzlich von der verantwortlichen Stelle zu benachrichtigen ist.

Für das Auskunftersuchen gem. § 19 BDSG muss weder ein berechtigtes oder rechtliches Interesse vorliegen oder sonst ein Anlass dargelegt werden.¹⁷⁶ Das Informationsinteresse muss von den Betroffenen auch, außer im Fall dass sich eine verantwortliche Stelle auf ihr Interesse der Wahrung des Geschäftsgeheimnisses beruft,¹⁷⁷ nicht begründet werden.¹⁷⁸ Der Auskunftsanspruch erstreckt sich sowohl auf für eigene Zwecke, auf geschäftsmäßig zum Zwecke der Übermittlung als auch auf nach § 30 BDSG gespeicherte Daten.¹⁷⁹ Durch den Auskunftsanspruch soll der Betroffene die Möglichkeit haben, Informationen über die Existenz oder das Fehlen eines des ihn betreffenden Datenbestands, dessen Zweckbestimmungen, die Datenkategorien und ggf. die Datenempfänger(kategorien), die Dateninhalte in verständlicher Form, deren Herkunft sowie ggf. über den logischen Aufbau automatisierter Datenverarbeitungen, zu erlangen.¹⁸⁰ Um effektiven Rechtsschutz zu gewährleisten richtet sich der Auskunftsanspruch nicht nur auf den gegenwärtigen Datenbestand bzw. die aktuellen Datenübermittlungen, sondern bezieht sich zur Gewährleistung eines effektiven Datenschutzes durch Berichtigungs- und sonstige Ansprüche zwingend auch auf die Vergangenheit.¹⁸¹

Ab Mai 2018 wird der Auskunftsanspruch einheitlich in der DSGVO geregelt. In Art. 15 DSGVO ist dieses Auskunftsrecht normiert. Dies ist jedoch umfassender als das bisher in §§ 19, 34 BDSG bzw. Art. 12 lit. a) DSRL geregelte, da der Betroffene auch Auskunft für die

¹⁷⁴ BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83 (Volkszählurteil).

¹⁷⁵ § 34 BDSG ist neben weiteren Rechten des Betroffenen gem. § 6 Absatz 1 BDSG nicht dispositiv.

¹⁷⁶ Dix, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 12 zu § 34 BDSG.; A.A. Hanloser, „EuGH: Umfang und Dauer des Auskunftsanspruchs über Datenempfänger“, (2009), *Datenschutzberater*, Heft 7-8, S. 15-17, der einen Auskunftsanspruch „ins Blaue“ ablehnt.

¹⁷⁷ Vgl. Dix, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 12 zu § 34, dann bedarf es einer Interessenabwägung zwischen dem Interesse der verantwortlichen Stelle und dem Betroffenen.

¹⁷⁸ Ibid. Dass der Betroffene nach § 34 Abs. 1 Satz 2 BDSG die personenbezogenen Daten, über die er Auskunft verlangt, näher bezeichnen soll, stellt lediglich eine Obliegenheit dar.

¹⁷⁹ Schmidt-Wudy, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 4 zu § 34 BDSG.

¹⁸⁰ Schneider, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 117 zu Völker- und unionsrechtliche Grundlagen.

¹⁸¹ Case C-553/07, Rotterdam v. Rijkeboer, EU:C:2009:293.

vom Verantwortlichen verarbeiteten personenbezogenen Daten erhalten kann, sich das Auskunftsrecht also nicht nur auf gespeicherte Daten beschränkt.¹⁸²

Die Durchsetzbarkeit dieses Rechts begegnet in der Praxis erheblichen Schwierigkeiten. Der von Maximilian Schrems gegründete Verein Europe v. Facebook hat auf gravierende Probleme hingewiesen. Zum Beispiel hat der Verein zutage gefördert, dass Auskunftersuchen gegenüber Facebook ins Leere laufen: Ein von Facebook eingerichtetes Download-Tool soll Auskunftersuchen beantworten, beinhaltet aber lediglich eine Kopie des Profils, aber keine Informationen über Daten, die Facebook darüber hinaus noch sammelt und weitergibt.¹⁸³

Problematisch ist weiterhin, dass viele Stellen eine Auskunft oftmals verweigern. Dies ist das Resultat einer Studie der Universitäten Hamburg und Siegen, welche bei der GI-Sicherheit 2016, 8. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI) vorgestellt wurde.¹⁸⁴ Außerdem gibt es enormen Zeitaufwand für die Betroffenen. In diesem Zusammenhang wurde im Jahr 2009 eine Petition¹⁸⁵ zur Änderung des § 34 BDSG gestartet. Im Einzelnen wollte der Verfasser, dass der Anspruch auf Auskunft aus §34 BDSG im Wege der einstweiligen Verfügung durchgesetzt werden kann, dass ein Nichtentsprechen des Auskunftersuchens als Ordnungswidrigkeit eingestuft wird, und dass die Aufsichtsbehörden das Recht erhalten, den Inhaber eines Bankkontos abzufragen, um den Täter eines Verstoßes gegen das BDSG festzustellen. Diese Petition hat zu damaliger Zeit das Quorum jedoch nicht erreicht, mit der Begründung, dass Verstöße gegen bestimmte Auskunftspflichten nach § 34 bußgeldbewehrt wurden und eine Sonderregelung für den Bereich des einstweiligen Rechtsschutzes aufgrund der Anwendungspraxis des BDSG nicht für erforderlich gehalten wurde.¹⁸⁶

b. Berichtigungsansprüche, §§ 20, 35 BDSG, Arts. 16, 17 DSGVO

Neben den Betroffenenrechten stehen dem Einzelnen Korrekturrechte nach § 35 BDSG zu. Durch diese Korrekturrechte auf Berichtigung, Widerspruch, Sperrung und Löschung kann die Verarbeitungspraxis beeinflusst werden. Die Ansprüche auf Berichtigung und Löschung werden als die zwei wichtigsten Ausprägungen des informationellen Selbstbestimmungsrechts angesehen.¹⁸⁷ Sie stellen Eingriffs- und Steuerungsbefugnisse¹⁸⁸

¹⁸²Schmidt-Wudy, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 3 zu Art. 15 DS-GVO.

¹⁸³http://europe-v-facebook.org/DE/Daten_verlangen_/daten_verlangen_.html (zuletzt abgerufen am 30.11.2016).

¹⁸⁴<https://arxiv.org/abs/1602.01804> (zuletzt abgerufen am 30.11.2016).

¹⁸⁵https://epetitionen.bundestag.de/petitionen/2009/09/12/Petition_7180.nc.html (zuletzt abgerufen am 30.12.2016).

¹⁸⁶Die Petition wurde vom Deutschen Bundestag am 17.06.2010 abschließend beraten.

¹⁸⁷Dix, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 2 zu § 35 BDSG; BVerfG, 15.12.1983 - 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83 (Volkszählurteil).

¹⁸⁸Dix, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 2 zu § 35 BDSG.

in Datenverarbeitungsprozesse dar und gehen damit über die Transparenzrechte wie den Auskunftsanspruch hinaus.¹⁸⁹

Die Voraussetzungen des Löschungsanspruchs ergeben sich aus § 35 Abs. 2 BDSG. Während § 35 Abs. 2 Satz 1 BDSG der verantwortlichen Stelle die Löschung von Daten erlaubt, wird gemäß § 35 Abs. 2 Satz 2 BDSG die verantwortliche Stelle zur Löschung von Daten verpflichtet. Danach besteht der Löschungsanspruch, wenn die Speicherung der personenbezogenen Daten unzulässig ist, [...] die Richtigkeit besonderer Arten personenbezogener Daten von der verantwortlichen Stelle nicht nachgewiesen werden kann, der Zweck der Verarbeitung erfüllt und eine Speicherung daher nicht mehr erforderlich ist oder bei zum Zwecke der Übermittlung gespeicherten Daten eine längere Speicherung nicht mehr erforderlich ist. Anstelle der Löschung kommt aufgrund bestimmter Umstände eine Sperrung der personenbezogenen Daten in Betracht (§ 35 III, IV, V BDSG) Dies ist der Fall, wenn dem gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigen würden, oder eine Löschung einen unverhältnismäßigen Aufwand bedeuten würde.

Nach Art. 17 Abs. 1 DSGVO hat die betroffene Person nunmehr das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der folgenden (über die Regelungen des BDSG hinausgehenden) Gründe zutrifft:

- Die Daten sind zur Zweckerreichung nicht mehr notwendig,
- der Betroffene hat seine Einwilligung widerrufen,
- die betroffene Person hat Widerspruch eingelegt,
- die personenbezogenen Daten wurden unrechtmäßig verarbeitet,
- eine Löschung zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder nach dem Recht der Mitgliedsstaaten erforderlich ist
- oder die personenbezogenen Daten in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 erhoben wurden.

Der EuGH hat in seinem Google-Urteil¹⁹⁰ mit Bezug auf den individuellen Löschungsanspruch entschieden, dass sich ein von einer Datenerhebung Betroffener direkt an – in diesem Fall – Suchmaschinenbetreiber wenden kann, um unter bestimmten Voraussetzungen die Entfernung von Links (Informationen) aus der Ergebnisliste zu löschen. Dieser Anspruch bestehe auch dann wenn eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten zum Zeitpunkt des Löschungsverlangens nicht mehr mit der Datenschutzrichtlinie – in diesem Fall Art. 6 Abs. 1 DSRL - vereinbar ist. Zu diesem Ergebnis kam der EuGH, da nach seiner Ansicht im Rahmen des Löschungsanspruch von Art. 12 lit. b) DSRL auch Art. 6 Abs. 1 DSRL beachtet werden muss, insbesondere in Bezug darauf, dass Daten nicht mehr dem ursprünglichen Zweck entsprechen. In der Interessenabwägung

¹⁸⁹ Ibid.; Meents, *BDSG und Datenschutzvorschriften des TKG und TMG Kommentar*, 2. Auflage 2013, Recht und Wirtschaft Verlag, Rn. 3 zu § 35 BDSG.

¹⁹⁰ Case C-131/12, Google Spain SL und Google Inc. v. Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, EU:C:2014:317

fürhte der EuGH aus, dass die wirtschaftlichen Interessen des Suchmaschinenbetreibers Google das Datenschutzinteresse des Betroffenen nicht überwiegen.

93 It follows from those requirements, laid down in Article 6(1) (c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.

94 Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.

In Abschnitt 3 der DSGVO sind weitere Korrekturrechte zusammengefasst. Es handelt sich dabei um das Recht auf Berichtigung, das Recht auf Löschung, das Recht auf Einschränkung der Verarbeitung, die Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung sowie das Recht auf Datenübertragbarkeit. Artikel 21 DSGVO sieht zudem ebenfalls ein Recht auf Widerspruch vor.

Art. 17 II DSGVO ergänzt den Berichtigungsanspruch aus Art. 16 DSGVO und den Lösungsanspruch gem. Art. 17 I DSGVO um das sog. „Recht auf Vergessenwerden“. Demnach sind Verantwortliche davon zu informieren, dass ein Betroffener die Löschung öffentlich gemachter personenbezogene Daten verlangt hat. Das Recht auf Vergessenwerden ist ein Lösungsanspruch mit mehreren Dimensionen.

Ebenso wie das Recht auf Auskunft ist jedoch auch die Umsetzung des Rechts auf Löschung in der Praxis schwer und mühselig. Im Internet beispielsweise ist es schwer für Verbraucher den verantwortlichen Webseitenbetreiber ausfindig zu machen und zur Verantwortung zu ziehen.¹⁹¹ Ein weiteres Problem stellen die Suchmaschinenbetreiber dar, da diese personenbezogene Daten noch nach Jahrzehnten auffindbar machen.¹⁹² Im

¹⁹¹ Vgl. Dix, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 8 zu § 35 BDSG; Gola/Klug/Körffner, *Bundesdatenschutzgesetz Kommentar*, Gola/Schomerus (Hrsg.), 12. Auflage 2015, C.H. Beck Verlag, Rn. 2a zu § 35 BDSG.

¹⁹² Dix, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 8 zu § 35 BDSG; Däubler, *Bundesdatenschutzgesetz Kompaktkommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage 2016, Bund Verlag, Rn. 2 zu § 35 BDSG.

Zusammenhang mit dem Google-Urteil des EuGH werden die Suchmaschinenbetreiber auch selbst vor Probleme gestellt. Sie haben auch dann eine Löschungspflicht, wenn Daten einmal rechtmäßig veröffentlicht wurden.

c. Schadensersatzansprüche

Normen, die Betroffenen Schadenersatz bei Datenschutzrechtsverletzungen zustehen, sind in verschiedenen Gesetzen zu finden, wie beispielsweise den Landesdatenschutzgesetzen, im BDSG, in den deliktischen Ansprüchen des BGB, im SDDSG, im SMG oder im AdVermiG. Als Voraussetzung sind allen die adäquat-kausale Verletzung des Datenschutzrechts und die Verursachung eines Schadens, gemein.

Zum Ausgleich materieller Schäden bei Verstößen gegen Datenschutzbestimmungen eröffnet § 7 BDSG natürlichen Personen einen eigenen deliktischen Anspruch.¹⁹³ Das Verschulden wird vermutet, es besteht aber eine Exkulpationsmöglichkeit für öffentliche sowie für nicht-öffentliche Stellen.¹⁹⁴ Zusätzlich zu § 7 BDSG enthält § 8 BDSG einen verschuldensunabhängigen Anspruch. Er trägt dem besonderen Gefahrenpotential der automatisierten Datenverarbeitung durch öffentliche Stellen Rechnung.¹⁹⁵ § 8 II BDSG sieht bei schweren Persönlichkeitsverletzungen einen Entschädigungsanspruch vor,¹⁹⁶ § 8 III BDSG begrenzt das Haftungsrisiko jedoch auf maximal 130.000 €. Die Regelung des § 7 BDSG entspricht weitestgehend Art. 23 DSRL, allerdings erfasst Art. 23 Abs. 1 DSRL auch Dritte und juristische Personen, sofern diese einen Schaden erlitten haben¹⁹⁷. Das bedeutet, dass im deutschen Recht insoweit die konkurrierenden Ansprüche greifen und die RL über § 7 BDSG hinaus umsetzen.¹⁹⁸ Umgekehrt verhält es sich bei der Verletzungshandlung, bei welcher § 7 BDSG weiter als die DSRL ist: § 7 BDSG erweitert das Objekt der Verletzungshandlung auf sämtliche Datenschutzbestimmungen, während nach Art. 23 DSRL nur Verstöße gegen die RL Schadensersatz auslösen.¹⁹⁹

Art. 82 DSGVO erweitert den Schadensersatzanspruch in zwei Bereichen. Im Gegensatz zu § 7 BDSG lässt sich aus Art. 82 DSGVO auch ein Direktanspruch gegen den Auftragsdatenverarbeiter ableiten. Im Fall des Verstoßes eines Verantwortlichen bzw. des Auftragsdatenverarbeiters wird der Pflichtverstoß vermutet. Dies stellt eine erhebliche Beweiserleichterung für die Betroffenen dar. Die Exkulpationsmöglichkeit für die Verantwortlichen bleibt jedoch bestehen. Ersetzt werden können sowohl materielle als auch immaterielle Schäden, wofür sich insbesondere die deutsche Delegation mit Stellungnahme v. 21.4.2015 (Nr. 8150/15 2012/0011 (COD)) eingesetzt hat.²⁰⁰ Es bedarf, wie nach der bisherigen Rechtslage, einer adäquat-kausalen Verletzung des Datenschutzrechtes und eines Schadens.

¹⁹³ Quaas, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 35-53 zu § 7 BDSG.

¹⁹⁴ Ibid., Rn. 37 zu § 7 BDSG.

¹⁹⁵ Ibid., Rn. 2-14, 37 zu § 8 BDSG.

¹⁹⁶ Ibid., Rn. 33-38 zu § 8 BDSG.

¹⁹⁷ Ibid., Rn. 7 zu § 7 BDSG.

¹⁹⁸ Ibid., Rn. 7 zu § 7 BDSG.

¹⁹⁹ Ibid., Rn. 7 zu § 7 BDSG.

²⁰⁰ Ibid., Rn. 8 zu § 7 BDSG.

Diesen Ansprüchen ist jedoch ein erhebliches praktisches Problem gemein: Der geforderte Kausalitätsnachweis ist schwierig bis unmöglich.²⁰¹ Hinzu kommt das Problem, dass der Nachweis eines (materiellen) Schadens bei Datenschutzverletzungen kaum gelingen wird.²⁰² Ersatz für immaterielle Schäden gewährt § 7 BDSG im Gegensatz zu § 8 II BDSG nicht.²⁰³

Eine höhere Relevanz haben vertragliche und deliktische Ansprüche des Verbrauchers für Datenschutzverstöße. Ein Schadenersatzanspruch kommt für Betroffene dann in Betracht, wenn beispielsweise datenkonformes Verhalten eine Hauptpflicht des Vertrages darstellt und diese verletzt wurde, oder aber durch Nebenpflichtverletzungen, was eher die Regel sein dürfte. § 823 Abs. 1 BGB i.V.m. Art. 2 I, Art. 1 I GG gibt Betroffenen einen Schadenersatzanspruch wegen Verletzung des Rechts auf informationelle Selbstbestimmung. Es ist darüber hinaus möglich, Schadenersatz für immaterielle Schäden zu erlangen.²⁰⁴ Daneben sind auch Fallkonstellationen denkbar, in denen ein Anspruch aus §§ 831, 824 oder 826 BGB einschlägig ist.

Im Rahmen des § 823 BGB i.V.m. § 7 BDSG kann der Betroffene, alternativ zur Geltendmachung eines tatsächlichen Schadens, auch einen abstrakten Wertausgleich nach der Lizenzanalogie verlangen oder wahlweise den von der verantwortlichen Stelle durch die unzulässige Datenverarbeitung erzielten Gewinn heraus verlangen - dann ist die dreifache Schadensberechnung wie im Immaterialgüterrecht möglich.²⁰⁵ Dies umfasst Fälle, in denen dem Betroffenen durch eine unzulässige oder unrichtige Datenverarbeitung kein tatsächlicher Schaden entstanden ist, aber sich die verantwortliche Stelle gerade den materiellen Wert personenbezogener Daten unzulässigerweise zunutze gemacht hat, z.B. wenn ein Adresshändler personenbezogene Daten verkauft, ohne sich auf eine Einwilligung oder den Erlaubnistatbestand des § 29 BDSG stützen zu können.²⁰⁶ Ebenso kann der Betroffene gegenüber einer Auskunftfein einen Anspruch auf Herausgabe des Gewinns geltend machen, den jene durch die entgeltliche Übermittlung von Kreditauskünften und Credit Scores zu seiner Person erzielt hat. Die auf vorsätzlichem Rechtsbruch beruhende Verfolgung kommerzieller Interessen wird in der Rechtsprechung als Zwangskommerzialisierung des Persönlichkeitsrechts des Betroffenen bezeichnet.²⁰⁷

²⁰¹ Conrad, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 152 zu § 34 Recht des Datenschutzes.

²⁰² Ibid., Rn. 153 zu § 34 Recht des Datenschutzes.

²⁰³ Gola/Klug/Körffer, *Kommentar zum Bundesdatenschutzgesetz*, Gola/Schomerus (Hrsg.) 12. Auflage 2015, C.H. Beck Verlag, Rn. 19 zu § 7 BDSG; Däubler, *Bundesdatenschutzgesetz Kompaktkommentar zum BDSG*, Däubler/Klebe/Wedde/Weichert (Hrsg.), 5. Auflage 2016, Bund Verlag, Rn. 19 zu § 7 BDSG.

²⁰⁴ Conrad, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 154 zu § 34 Recht des Datenschutzes.

²⁰⁵ Buchner, *Informationelle Selbstbestimmung im Privatrecht*, (Mohr Siebeck Verlag, 2006), S. 303 f; Buchner, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 156 zu § 29 BDSG.

²⁰⁶ Buchner, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 155 zu § 29 BDSG.

²⁰⁷ Dazu Marwitz, „Zwangskommerzialisierung vermögenswerter immaterieller Rechte“, (2003), *Zeitschrift für Medien und Kommunikationsrecht*, Heft 5, S. 405 409, S. 405f.

2. Kollektiver Rechtsschutz: Verbraucherzentralen & Marktwächter

a. Verbandsklagebefugnis

Durch § 2 I Nr. 11 UKlaG wurde die Klagebefugnis der Verbraucherverbände bei Datenschutzverstößen über das AGB-Recht und das UWG hinaus ausgedehnt. Damit soll die Lücke geschlossen werden, welche zuvor dadurch entstand, dass Verbraucherverbände nicht auch bei anderweitigen Verstößen, insbesondere bei einer Datenerhebung zu Nicht-Werbezwecken und ohne in Klauseln vorformulierten Einwilligungen, anspruchsberechtigt waren. Gerade die bei der individuellen und behördlichen Rechtsdurchsetzung auftretenden Defizite sollen so kompensiert werden.²⁰⁸

Die Reform des UKlaG bringt also einige Klarstellungen, z.B. hinsichtlich des Charakters des Datenschutzrechts als Verbraucherschutzrecht und zur expliziten Einführung des Beseitigungsanspruchs im gesamten § 2 UKlaG. Da das Datenschutzrecht lauterkeitsrechtlich nur rudimentär erschlossen ist, könnte sich die Erweiterung der Verbandsklagekompetenz auf datenschutzrechtliche Gesetze in der Praxis durchaus bemerkbar machen. Denn die Aufzählung der kommerziellen Zwecke der Datenerhebung, -verarbeitung oder -nutzung, die in den Anwendungsbereich der Norm fallen, ist beinahe umfassend: Werbung, Adresshandel sowie Markt- und Meinungsforschung sind ebenso wie die Erstellung von Persönlichkeits- und Nutzungsprofilen (Scoring gem. § 28b BDSG) und sonstigem Datenhandel erfasst. Auch Verstöße gegen die DSGVO fallen in den Anwendungsbereich der Verbandsklage. Zwar sieht Kapitel VI DSGVO eher eine Überwachung der Anwendung ihrer Vorschriften durch unabhängige Aufsichtsbehörden vor. Zugleich erlaubt Art. 58 V DSGVO den Mitgliedstaaten ausdrücklich, bestimmten Organisationen Klagebefugnis zur Rechtsdurchsetzung zu verleihen.²⁰⁹

Ob sie die befürchteten „Massenabmahnungen“ provoziert, wird die Zukunft zeigen. Sollte dies eintreten, so wäre außerdem das materielle Datenschutzrecht zu ordnen und zu bereinigen. So könnten die materiell-rechtlichen Formulierungen klarer gestaltet werden, um für mehr Rechtssicherheit zu sorgen. Gerade um die zu erwartenden Unklarheiten zu beseitigen, ist die Rechtsdurchsetzung und Rechtsfortbildung mit Hilfe der Verbandsklage notwendig.²¹⁰

Während der Vorstand des VZBV Müller die Reform des UKlaG positiv bewertet, da individuellen Klagen i.d.R. aufwendig und teuer seien und Verbraucher daher häufig die gerichtliche Auseinandersetzung vermeiden wollen,²¹¹ hält die amtierende Bundesdatenschutzbeauftragte Voßhoff die Erweiterung der Verbandsklagebefugnis für

²⁰⁸ Ritter/Schwichtenberg, „Die Reform des UKlaG zur Eliminierung des datenschutzrechtlichen Vollzugsdefizits – neuer Weg, neue Chancen?“, (2016), *Verbraucher und Recht*, Heft 3, S. 95-102, S.97.

²⁰⁹ Halfmeier, „Die neue Datenschutzverbandsklage“, (2016), *Neue Juristische Wochenschrift*, Heft 16, S. 1126-1129, S. 1129.

²¹⁰ Halfmeier, „Die neue Datenschutzverbandsklage“, (2016), *Neue Juristische Wochenschrift*, Heft 16, S. 1126-1129, S. 1129.

²¹¹ <<http://www.vzbv.de/pressemitteilung/erweitertes-verbandsklagerecht-datenschutzverstoesse-werden-sich-nicht-mehr-lohnen>> (zuletzt abgerufen am 30.11.2016).

Verbraucherzentralen für nicht notwendig.²¹² Das Datenschutzrecht sei konzeptionell kein Verbraucherschutzrecht, da von diesem nicht die wirtschaftliche Handlungs- und Entscheidungsfreiheit von Verbrauchern, sondern die informationelle Handlungs- und Entscheidungsfreiheit in Ausübung des (Grund-)Rechts auf informationelle Selbstbestimmung geschützt wird. Die Auskunfts-, Einsichts- und Prüfungsrechte sowie Anordnungs- und Untersagungsbefugnisse der Aufsichtsbehörden gegenüber den datenverarbeitenden Stellen seien ausreichend und die Parallelstruktur zivil- und verwaltungsrechtlicher Rechtsdurchsetzung daher nachteilhaft. Sie befürchtet, dass der gesetzliche vorgesehene Beratungsauftrag der Aufsichtsbehörden aus § 38 I 2 BDSG geschwächt werde, wenn Vereinbarungen, die aus Sicht der Aufsichtsbehörden ein ausreichendes Datenschutzniveau gewährleisten, durch Abmahnungen und Verbandsklagen im Nachhinein in Frage gestellt würden.

Eine solche Sichtweise fußt jedoch auf dem Verständnis einer strikten Trennung zwischen verwaltungs- und zivilrechtlichem Rechtsweg, der zum einen eine aufgegebene Rechtsprechung und herrschende Meinung widerspiegelt und zum anderen auch im Ausland so nicht existiert. Die Trennung wurde in der früheren Rechtsprechung und h.M. mit Verweis auf die unterschiedlichen Schutzgüter des Daten- und Persönlichkeitsrechts vertreten; in der Diskussion ging es um den Unterschied zwischen datenschutzrechtlichen Vorschriften auf der einen und Marktverhaltensvorschriften auf der anderen Seite.²¹³ Inzwischen ist jedoch sowohl in der Rechtsprechung als auch der h.M. eine Abkehr von dieser strikten Trennung zu beobachten. In Großbritannien können die Aufsichtsbehörden (Watchdog) ein formalisiertes Beschwerdeverfahren in Anspruch nehmen, wenn die Interessen der Verbraucher in einem Markt systematisch beeinträchtigt werden. Die angerufene Regulierungsbehörde ist dann verpflichtet, innerhalb von 90 Tagen zu dem Sachverhalt Stellung zu nehmen und darzulegen, welche Maßnahmen sie ergreifen wird. Daneben besteht für die Watchdogs die Möglichkeit der Stellungnahme gegenüber Ministerien, der EU-Kommission und gegenüber Aufsichtsbehörden.²¹⁴

Eine berechtigtere Kritik liegt eher in dem Argument, dass eine effektive Rechtsdurchsetzung trotz der UKlaG-Reform an den begrenzten Ressourcen der Verbraucherverbände, dem unkoordinierten Nebeneinander von Datenschutzbehörden und Verbraucherverbänden, dem langwierigen Vollstreckungsverfahren und der inkonsequenten Ausgestaltung der Befugnisse

²¹² Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 25. *Tätigkeitsbericht zum Datenschutz 2013 – 2014*, S. 114 f.
<https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/25TB_13_14.pdf;jsessionid=047ADA6C12D5BF27DE04AAB7DF1ADB96.1_cid319?_blob=publicationFile&v=10> (zuletzt abgerufen am 30.11.16).

²¹³ S. dazu Übersicht in Robak, „Neue Abmahnrisiken im Datenschutzrecht“, (2016), *Gewerblicher Rechtsschutz und Urheberrecht*, Praxis im Immaterialgüter und Wettbewerbsrecht, Heft 7, S. 139-141, S. 139.

²¹⁴ S. „2 I. Das britische Modell“, <http://www.vzbv.de/sites/default/files/mediapics/consumer_watchdogs_20_juni_2007.pdf> (zuletzt abgerufen am 30.11.2016).

scheitern könne – das allgemein beklagte Vollzugsdefizit im Datenschutzrecht, es wird wohl auch in naher Zukunft bestehen bleiben.²¹⁵

Ein weiteres Manko der Reform bestehe darin, dass sie den Beseitigungsanspruch, der neu in § 2 I UKlaG aufgenommen wurde, nicht ausdrücklich auch auf § 1 UKlaG erstreckt. Gerade durch rechtswidrige AGB werden häufig Störungszustände geschaffen, die mit einem bloßen Unterlassungsurteil nicht beseitigt werden können. Es entspreche dem Grundmodell des § 1004 BGB, dass eine rechtswidrige Handlung nicht nur für die Zukunft verboten, sondern auch ihre eingetretenen Folgen beseitigt werden können.²¹⁶ Daher ist im Sinne einer einheitlichen Interpretation von einem Beseitigungsanspruch auch im Rahmen des § 1 UKlaG auszugehen. Eine entsprechende Klarstellung durch den Gesetzgeber wäre demzufolge geboten.

b. Stärkung des kollektiven Rechtsschutzes durch Marktwächter?

Die 2015 eingerichteten Marktwächter präsentieren sich auf ihrer Website als das neue Frühwarnsystem der Verbraucherzentralen. Mit ihrer Hilfe sollen die Verbraucherzentrale Bundesverband und die Verbraucherzentralen Erkenntnisse über die tatsächliche Lage von Verbrauchern im Finanzmarkt und in der digitalen Welt sammeln. Verbraucherschützer sollen mit deren Mithilfe Probleme rechtzeitig erkennen²¹⁷ Für den Marktwächter Digitale Welt wurden fünf Schwerpunktverbraucherzentralen ausgewählt, die jeweils ein Handlungsfeld des digitalen Marktes näher untersuchen: Bayern (Digitale Dienstleistungen), Brandenburg (Digitaler Wareneinkauf), Nordrhein-Westfalen (Nutzergenerierte Inhalte), Rheinland Pfalz (Digitale Güter) und Schleswig-Holstein (Telekommunikationsdienstleistungen). Die zentrale Koordinationsstelle liegt auch hier beim vzbv. Für den Finanzmarkt ist schwerpunktmäßig die Verbraucherzentrale Baden-Württemberg zuständig.

Die Datenschutzaufsichtsbehörden sind im Beirat des Marktwächters Digitale Welt durch die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg vertreten. Die Marktwächter sollen die Aufsichts- und Regulierungsbehörden in ihrer Arbeit unterstützen.²¹⁸ Die Datenerhebung für die Marktbeobachtung findet auf Grundlage der Verbraucherberatung in allen 16 Verbraucherzentralen statt. Der Finanzmarkt und die digitalen Märkte sollen systematisch beobachtet werden, es sollen Verbraucherprobleme erfasst und identifiziert werden, daneben sollen Politik, Behörden und Verbraucher regelmäßig informiert werden. Die Marktbeobachtung durch die Marktwächter basiert auf einem vier-Säulen-System.²¹⁹

²¹⁵ Ritter/Schwichtenberg, „Die Reform des UKlaG zur Eliminierung des datenschutzrechtlichen Vollzugsdefizits – neuer Weg, neue Chancen?“, (2016), *Verbraucher und Recht*, Heft 3, S. 95-102, S. 102.

²¹⁶ Halfmeier, „Die neue Datenschutzverbandsklage“, (2016), *Neue Juristische Wochenschrift*, Heft 16, S. 1126-1129, S. 1129.

²¹⁷ <<http://www.marktwaechter.de/>> (zuletzt abgerufen am 30.11.2016).

²¹⁸ Dieser Abschnitt basiert auf <<http://www.vzbv.de/pressemitteilung/finanzmarktwaechter-und-marktwaechter-digitale-welt-starten-und-bauen>> (zuletzt abgerufen am 30.11.2016).

²¹⁹ Dieser Absatz basiert auf den Präsentationsfolien der Pressekonferenz vom 25.08.2016 – Erste Bilanz über die Arbeit der Marktwächter Digitale Welt und Finanzen

- Im Frühwarnnetzwerk sollen besonders auffällige Fälle aus den Beratungsgesprächen den VZen gemeldet werden
- In der Vorgangserfassung ist sodann die quantitative Erfassung der Fälle aus den Verbraucherzentralen zu verstehen.
- Sonderuntersuchungen sollen zur Vertiefung der Erkenntnisse für ausgewählte Themen durchgeführt werden.
- Das Online-Portal soll sodann eine Möglichkeit des direkten Austausches mit Verbraucher darstellen. Es soll ein interaktives Portal sein, welches zum Beispiel durch ein Beschwerdepostfach Verbrauchervarnungen, Verbraucheraufrufe oder Verbraucherinformationen aus den Sonderuntersuchungen aufbereitet.

Die von den Marktwächtern hervorgebrachten Erkenntnisse sollen dem vzbv und den Verbraucherzentralen für die kollektive Rechtsdurchsetzung dienen.

Die bisherigen Tätigkeiten mit Stand 09/2016 sind laut Angabe des Vorstands der vzbv Klaus Müller, die Folgenden:²²⁰

- Ungefähr 7000 Meldungen
- 6 Warnungen an Öffentlichkeit
- 7 Untersuchungsberichte
- 25 Gespräche mit Behörden etc.
- 12 Abmahnverfahren wovon 5 erfolgreich waren

Im politischen Diskurs wird die bisherige Arbeit der Marktwächter als Erfolg bewertet. Ulrich Kelber, der Parlamentarische Staatssekretär im BMJV äußerte sich bei der Marktwächter-Presskonferenz vom 25.08.2016 positiv:

*Die Verbraucherzentralen bringen hier ihr Wissen ein, das bei den Marktwächtern zusammen getragen und systematisch ausgewertet wird. So funktioniert eine wirkungsvolle, realitätsnahe und gut verzahnte Verbraucherschutzpolitik.*²²¹

Die bisherige Praxis wird jedoch auch kritisiert, insbesondere von Industrie- und Handelsvertretern. Nach Aussage von de Vries²²² soll ein Handlungsschwerpunkt auf dem Führen von Dialogen liegen, bei welchen Verbraucher, Anbieter und Behörden, Politiker und

²²⁰ Klaus Müller, Vorstand des Verbraucherzentrale Bundesverband auf der Veranstaltung „Marktwächter, Digitalagentur & Co.: Sind neue Strukturen in der Verbraucherpolitik notwendig? Erkennen-Informieren-Handeln-eine Zwischenbilanz: Wie unterstützt die Marktwächterarbeit Verbraucherschutz?“ vom 22.09.2016.

²²¹ <http://www.marktwaechter.de/pressmeldung/marktwaechterarbeit-staerkt-verbraucherschutz>; auch Justizminister Heiko Maas äußerte sich noch im Jahr 2015 positiv: „[...]Es ist daher besonders wichtig darauf zu achten, dass Verbraucherrechte und Datenschutz von den Unternehmen beachtet werden. Die Marktwächter übernehmen hierfür eine wesentliche ‘Sensorfunktion’, um frühzeitig Probleme am Markt erkennen zu können. Denn: Rechtzeitige Informationen sind notwendig, damit die Nutzer oder die Politik entsprechend reagieren können.“ (Heiko Maas am 02.09.2015 http://www.bmjbv.de/SharedDocs/Artikel/DE/2015/09022015_vz-Rheinland-Pfalz.html)

²²² Björn de Vries, Projektleiter Marktwächter Finanzen, Verbraucherzentrale Bundesverband e. V. auf der Veranstaltung „Marktwächter, Digitalagentur & Co.: Sind neue Strukturen in der Verbraucherpolitik notwendig?“ vom 22.09.2016 zum Programmpunkt „Finanzmarkt unter der Lupe: Der Marktwächter Finanzen fahndet nach strukturellen Problemen.“

Experten die Zielgruppe darstellen. Langer²²³ sieht jedoch in der Umsetzung dieser Dialoge ein Problem in der Herangehensweise, da diese erst nach einer Untersuchung stattfinden. Von der Deutschen Kreditwirtschaft wird darüber hinaus auch mehr Neutralität gefordert: „Würde [der Marktwächter] nur als Sprachrohr von Verbraucherorganisationen wahrgenommen, könne er seine ordnungspolitische Aufgabe nicht erfüllen.“²²⁴ Die Kreditwirtschaft fordert, dass vor einer Veröffentlichung alle relevanten Interessengruppen angehört werden müssen. Ein weiterer Negativpunkt stellt für Langer die Behauptung „95 % aller Anlageprodukte sind nicht bedarfsgerecht“ der Marktwächter dar. Seiner Ansicht nach hat es sich dabei um eine reißerische Behauptung gehandelt, da im Übrigen nur 362 Angebote untersucht wurden. Wenn man lediglich die Beschwerden betrachtet kann das Ergebnis nicht repräsentativ sein.

Auf die Frage, inwieweit die Erkenntnisse der Marktwächter wissenschaftlich fundiert seien, entgegnete Klaus Müller im Ausschussbericht vom 22.06.2016, dass die Verbraucherzentralen diesen Anspruch nicht erheben würden „Wir sind parteiisch, nämlich für die Verbraucher.“ Uwe Wewel,²²⁵ langjähriger zuständige Abteilungsleiter im BMF für Investmentfonds bezeichnet zudem die Vorgehensweise des Finanzmarktwächters, weiterhin KAGB-Produkte dem grauen Kapitalmarkt zuzurechnen, als "unzulässig": *"Damit missachtet er die Entscheidung des Gesetzgebers und es muss das 'quasi amtliche Siegel' der Förderung durch die Bundesregierung hinterfragt werden."*

In Bezug auf die Arbeit der Marktwächter und angesichts der starken Kritik im Verhältnis zu den bisherigen Ergebnissen und der Höhe der Fördermittel (5,6 Mio € pro Jahr durch das BMJV bis Ende 2017) stellen sich also einige Fragen: Kann ein Wächterkonzept überhaupt von anderen Institutionen als dem Staat effektiv wahrgenommen werden? Was ist der Mehrwert der Marktwächter, wenn es sich bei ihnen nicht um eine staatliche Institution mit hoheitlichen Befugnissen handelt, sondern um eine Art zwischengeschaltete Instanz der Informationsbündelung? Warum haben die Marktwächter keine Befugnisse wie die oft als Vorbild genannten Watchdogs aus Großbritannien?²²⁶ Die Marktwächter kümmern sich nur um nationale Angelegenheiten – kann das ein Zukunftsmodell mit europäischer Perspektive sein?

Fest steht, dass empirische Untersuchungen, die Aufschluss über etwaigen Handlungsbedarf oder weitere Kompetenzen für die Marktwächter geben könnten, noch fehlen. Um die Aktivität der Marktwächter zukunftsweisend beurteilen zu können, müssten also weitere Untersuchungen angestrengt werden.

²²³ Dr. Olaf Langer, Chefsyndikus und Leiter der Abteilung Recht, Steuern und Verbraucherpolitik des Deutschen Sparkasse- und Giroverbandes e.V. auf der Veranstaltung „Marktwächter, Digitalagentur & Co.: Sind neue Strukturen in der Verbraucherpolitik notwendig?“ vom 22.09.2016.

²²⁴ <<http://www.die-bank.de/news/sinnvoller-ansatz-mit-verbesserungspotenzial-8118/>> (zuletzt abgerufen am 30.11.2016).

²²⁵ <<http://www.cash-online.de/recht-steuern/2016/finanzwaechter-oder-nachtwaechter/326871/2>> (zuletzt abgerufen am 30.11.2016).

²²⁶ Vgl. S. 28 <http://kerstin-tack.de/imperia/md/content/bezirkhannover/kerstintack/2013/dokumentation_marktwaechter_nov_12.pdf> (zuletzt abgerufen am 30.11.2016).

3. Behördlicher Rechtsschutz

Jedem steht das Recht zu, sich bei Verdacht auf eine Rechtsverletzung, in Bezug auf Erhebung, Verarbeitung oder Nutzung seiner persönlichen Daten, an eine Aufsichtsbehörde (Landes- und Bundesdatenschutzbehörden) zu wenden, § 38 BDSG und Arts. 77 ff DSGVO. Dienststelle ist der BfDi.²²⁷ Den Aufsichtsbehörden stehen zur Wahrnehmung der Rechte des Betroffenen Auskunfts- und Kontrollbefugnisse zu.²²⁸ Das Beschwerderecht stellt damit eine mittelbare Möglichkeit der Rechtsdurchsetzung für den Einzelnen dar. Das Ziel der Regelungen ist, eine Rechtsschutzmöglichkeit für Betroffene zu schaffen, die sich wirtschaftlich unterlegen fühlen, oder denen es aus anderen Gründen nicht sinnvoll erscheint, selbst seine Ansprüche geltend zu machen.²²⁹

a. System

Fühlt sich der Einzelne wirtschaftlich unterlegen, oder erscheint es einem Betroffenen nicht sinnvoll selbst seine Ansprüche geltend zu machen, kann er sich an die Datenschutzaufsichtsbehörden der Länder und des Bundes wenden.²³⁰ Jedem steht das Recht zu, sich bei Verdacht auf eine Rechtsverletzung, in Bezug auf Erhebung, Verarbeitung oder Nutzung seiner persönlichen Daten, an eine Aufsichtsbehörde zu wenden. Den Aufsichtsbehörden stehen zur Wahrnehmung der Rechte des Betroffenen Auskunfts- und Kontrollbefugnisse zu.²³¹ Das Beschwerderecht ist eine mittelbare Möglichkeit der Rechtsdurchsetzung für den Einzelnen.

Das Beschwerderecht des Einzelnen bei einer Datenschutzaufsichtsbehörde, egal ob diese privatrechtlich ist oder sich gegen eine öffentliche Stelle wendet²³², ist in der DSGVO weiterhin verankert. Geregelt wird das Beschwerderecht in Artikel 77. In Artikel 78 DSGVO hat der Betroffene zudem die Möglichkeit, einen wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde geltend zu machen.

Auf nationaler Ebene sind folgende Institutionen für die Beschwerden zuständig:

²²⁷ Der BfDi verzeichnete für die Jahre 2013/14 rund 371 Beschwerden und Fragen der Bürgerinnen und Bürger pro Monat rund um den Datenschutz, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 25. Tätigkeitsbericht zum Datenschutz 2013 – 2014, S. 232.

²²⁸ Brink, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 4 zu § 38 BDSG.

²²⁹ S. 2 <https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/Standpunkte/140815-BvD-Stellungnahme_zur_Ank%C3%BCndigung_des_UKlaG.pdf> (zuletzt aufgerufen am 30.11.2016).

²³⁰ Ibid.

²³¹ Brink, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 4 zu § 38 BDSG.

²³² Vgl. (EU-Datenschutzgrundverordnung:

Ergebnisse der Verhandlungen („Trilogie“) und die 10 wichtigsten Punkte - Federführender Ausschuss des Europäischen Parlaments: Bürgerliche Freiheiten, Justiz und Inneres (LIBE), EP-Verhandlungsführer („Berichterstatte“): Jan Philipp Albrecht, MdEP, Grüne / Europäische Freie Allianz, S. 1,

<https://www.janalbrecht.eu/fileadmin/material/Dokumente/20151217_Datenschutzreform_10_wichtige_Punkte_DE.pdf> (zuletzt abgerufen am 30.11.16):

Die Datenschutzgrundverordnung wird für den gesamten privaten und öffentlichen Bereich gelten. Ausgenommen ist lediglich der Bereich der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten sowie der Strafvollstreckung. Hier wird künftig die gleichzeitig verhandelte Richtlinie für den Datenschutz im Polizei- und Justizbereich gelten.

- Die Bundesdatenschutzbeauftragte für den Bereich der Bundesverwaltung (§ 24 BDSG)²³³,
- die jeweiligen Landesdatenschutzbeauftragten für den Datenschutz beziehungsweise die Aufsichtsbehörden nach § 38 BDSG (in den Ländern wurden die Zuständigkeiten konsolidiert, so dass dort die Landesdatenschutzbeauftragten sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich zuständig sind. Es sind also fast alle Aufsichtsbehörden für die Privatwirtschaft bei den entsprechenden Landesdatenschutzbeauftragten angesiedelt. Eine Ausnahme gilt für den Freistaat Bayern: Für den Bereich Privatwirtschaft ist hier das Bayerische Landesamt für die Datenschutzaufsicht zuständig)²³⁴

Auf Bundesebene ist das BDSG für öffentliche Stellen des Bundes sowie für Unternehmen einschlägig. Auf Landesebene regeln die Landesdatenschutzgesetze die Bestimmungen für Landes- und Kommunalbehörden. Kontrolliert werden die öffentlichen Stellen des Bundes und die Telekommunikations- sowie Postdienstleistungen von der Bundesaufsichtsbehörde für Datenschutz unter der Leitung des Bundesbeauftragten für Datenschutz und Informationsfreiheit. Die Aufsichtsbehörden der Bundesländer und deren Landesbeauftragten für Datenschutz kontrollieren die Landesbehörden.

Die Aufsicht über private Unternehmen liegt bei den Aufsichtsbehörden für den nicht-öffentlichen Bereich. Durch die bundesgesetzliche Regelung des § 38 BDSG wird näher bestimmt, wie die landeseigene Verwaltung als Aufsichtsbehörde privatwirtschaftliche Unternehmen und Stellen auf dem Feld des Datenschutzes kontrolliert.²³⁵ Die oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich ist der sogenannte Düsseldorfer Kreis.²³⁶ Es handelt sich dabei um eine informelle Vereinigung der obersten Aufsichtsbehörden. Die Beschlüsse und Stellungnahmen des Düsseldorfer Kreises und der Konferenz der Datenschutzbeauftragten von Bund und Ländern sind für die Aufsichtsbehörden zwar nicht bindend, nehmen aber eine wichtige Rolle bei der Bewertung konkreter Verfahren im Rahmen der Kontrolltätigkeit der Datenschutzbehörden ein.²³⁷

Die Kontrolle durch die zuständigen Aufsichtsbehörden erfolgt anlass- und verdachtslos aufgrund eigenen Entschlusses zu stichprobenartiger oder systematischer Untersuchung der Datenschutzkonformität des Verhaltens verantwortlicher Stellen, oder nach Hinweisen Betroffener, Dritter oder anderer staatlicher Behörden.²³⁸ Durch das Beschwerderecht des Einzelnen erhalten die Aufsichtsbehörden zusätzlich wichtige Impulse und Informationen, die

²³³ Brandt, *Corporate Compliance Handbuch der Haftungsvermeidung im Unternehmen*, Hauschka/Moosmayer/Lösler (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 176 zu § 29 Datenschutz.

²³⁴ Ibid., Rn. 176 zu § 29 Datenschutz.

²³⁵ Gola/Klug/Körffner, *Bundesdatenschutzgesetz Kommentar*, Gola/Schomerus (Hrsg.), 12. Auflage 2015, C.H. Beck Verlag, Rn. 1 zu § 38 BDSG.

²³⁶ Conrad, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn. 249 zu § 33 Compliance IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung.

²³⁷ Ibid., Rn. 251 zu § 33 Compliance IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung.

²³⁸ Brink, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 3 zu § 38 BDSG.

für die effektive Wahrnehmung ihrer Rechtsdurchsetzungsmöglichkeiten unerlässlich sind.²³⁹ Auch der betriebliche Datenschutzbeauftragte kann im Fall des § 4d Abs. 6 BDSG ebenfalls verpflichtet sein, sich an die Aufsichtsbehörden zu wenden.²⁴⁰

Gemäß § 40 VwVfG steht die Kontrolltätigkeit der Aufsichtsbehörden in deren Ermessen. Zu den Tätigkeiten gehören mithin Beratungstätigkeiten, Kontrolltätigkeiten, Vorortkontrollen und in Ausnahmefällen eine Pflicht zum Einschreiten. Daneben trifft die Aufsichtsbehörde eine Beratungs- und Unterstützerpflicht gegenüber betrieblichen Datenschutzbeauftragten und der verantwortlichen Stelle insgesamt. Neben diesen Anordnungs- und Untersagungsbefugnissen haben die Aufsichtsbehörden bei materiellen Rechtsverstößen bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten die Möglichkeit, die in Rede stehende Praktik zu Untersagen oder die Beseitigung anzuordnen.²⁴¹

Mangels spezialgesetzlicher Regelungen im BDSG, welches die „zuständige Aufsichtsbehörde“ nur an mehreren Stellen erwähnt, ohne selbst die Zuständigkeit zu regeln, finden die Verwaltungsverfahrensgesetze der Länder Anwendung.²⁴² Für die Zuständigkeit gilt § 3 Abs. 1 Nr. 2 VwVfG. Für die örtliche Zuständigkeit maßgeblich ist somit der Sitz der Betriebsstätte der verantwortlichen Stelle beziehungsweise der Ort der datenschutzrechtlich relevanten Tätigkeitsausübung.²⁴³ Zuständigkeitsfragen ergeben sich grundsätzlich nur für die Länder untereinander, da es auf sachlicher Ebene keine Überschneidungen mit den Datenschutzaufsichtsbehörden der Länder gibt.²⁴⁴

In bestimmten Konstellationen sind Mehrfach- und Parallelzuständigkeiten²⁴⁵ nicht ausgeschlossen, z.B. wenn das Unternehmen mehrere Zweigstellen oder Betriebe in verschiedenen Ländern hat. In solchen Fällen ist grundsätzlich diejenige Aufsichtsbehörde zuständig, in deren Zuständigkeitsbereich der Hauptsitz des Unternehmens liegt.²⁴⁶ Es bedarf jedoch der Abstimmung und gegenseitiger Unterstützung der Behörden im Wege der Amtshilfe.²⁴⁷ Ein Tätigwerden der für eine Zweigstelle zuständigen Aufsichtsbehörde ist nicht ausgeschlossen.²⁴⁸

Ob sich aus diesem Zuständigkeitsproblem weitere Rechtsdurchsetzungsprobleme ergeben, ist umstritten. Auf der einen Seite erscheint es fraglich, ob der permanente

²³⁹ Schneider, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 142 in Völker- und unionsrechtliche Grundlagen.

²⁴⁰ Meltzian, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 60 in § 4d BDSG.

²⁴¹ Gola/Klug/Körffer, *Bundesdatenschutzgesetz Kommentar*, Gola/Schomerus (Hrsg.), 12. Auflage 2015, C.H. Beck Verlag, Rn. 25 zu § 38 BDSG.

²⁴² Kranig, „Zuständigkeit der Datenschutzaufsichtsbehörden - Feststellung des Status quo mit Ausblick auf die DS-GVO“, (2013), *Zeitschrift für Datenschutz*, Heft 11, S. 550-557, S. 551-552.

²⁴³ Brink, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 89 zu § 38 BDSG.

²⁴⁴ Kranig, „Zuständigkeit der Datenschutzaufsichtsbehörden - Feststellung des Status quo mit Ausblick auf die DS-GVO“, (2013), *Zeitschrift für Datenschutz*, Heft 11, S. 550-557, S. 551.

²⁴⁵ Ibid., S. 552.

²⁴⁶ Brink, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 89 zu § 38 BDSG.

²⁴⁷ Ibid.

²⁴⁸ Ibid.

Koordinationsbedarf bei mehreren zuständigen Aufsichtsbehörden die Effektivität nicht zum Erliegen bringt.²⁴⁹ Rechtsklarheit könnte auf verschiedenem Wege erreicht werden. So wird vorgeschlagen, dass eine Art Generalklausel, wie sie im Polizeirecht zu finden ist, Abhilfe schaffen könnte indem sie die Auffangzuständigkeit im Streitfall sicherstellt. Auch wäre eine spezifische Regelung der Zuständigkeit der Datenschutzaufsichtsbehörden wegen Art. 83, 84 Abs. 1 Satz 2 GG nicht ausgeschlossen.²⁵⁰ Auf der anderen Seite, gibt es, so Kranig, im Ergebnis bei Fragen der Zuständigkeit keine einhergehenden Rechtsverluste.²⁵¹ Bei der Weiterleitung von Eingaben einer unzuständigen, an die zuständige Aufsichtsbehörde, handelt es sich um einen routinemäßigen Vorgang, der zeitnah und problemfrei erledigt werden könne.²⁵²

b. Maßnahmen - Übersicht

Wird der Verstoß gegen deutsches Datenschutzrecht durch ein Unternehmen von einer deutschen Datenschutzbehörde im Sinne des § 38 Abs. 1 BDSG festgestellt, hat sie mehrere Möglichkeiten darauf zu reagieren: Sie kann eine Anordnungs- oder Untersagungsverfügung gem. § 38 V BDSG erlassen oder Sanktionen verhängen.

Im Unterlassungsverfahren hat die Behörde die Möglichkeit gegenüber dem Unternehmen, nach vorheriger Anhörung, per Verwaltungsakt anzuordnen, den Verstoß zu unterlassen. Leistet die verantwortliche Stelle der Verfügung nicht Folge, kommt es zu einem abgestuften Verfahren.²⁵³ Die Beseitigung wird erneut unter Fristsetzung und unter Zuhilfenahme einer Zwangsgeldfestsetzung angeordnet. Wenn auch diese Maßnahme erfolglos bleibt, hat die Aufsichtsbehörde die Möglichkeit, die in Rede stehende Praktik des Unternehmens zu untersagen (§ 38 Abs. 5 Satz 2 BDSG). Bringen diese Maßnahmen nicht den gewünschten Erfolg, kann die Behörde, bei schwerwiegenden Verstößen oder Mängeln, eine Untersagungsverfügung in Bezug auf das mangelbehaftete Datenverarbeitungsverfahren treffen. Das Merkmal „schwerwiegend“ ist in der Regel dann erfüllt, wenn die betroffene Datenverarbeitung der Vorabkontrolle nach § 4 d Abs. 5 BDSG unterliegt.²⁵⁴

Daneben hat die Aufsichtsbehörde das Recht, Bußgelder zu verhängen und die Strafverfolgungsbehörden einzuschalten: Ihr ist gemäß § 44 II 2 BDSG ein Strafantragsrecht eingeräumt.²⁵⁵ §§ 43, 44 BDSG normieren die Sanktionen bei datenschutzrechtlichen Verstößen. Sind die Ordnungswidrigkeitstatbestände des § 43 I, II BDSG erfüllt, sieht § 43 III BDSG eine Geldbuße vor. Wenn im Falle des § 43 II BDSG zusätzlich ein vorsätzlicher

²⁴⁹Kranig, „Zuständigkeit der Datenschutzaufsichtsbehörden - Feststellung des Status quo mit Ausblick auf die DS-GVO“, (2013), *Zeitschrift für Datenschutz*, Heft 11, S. 550-557, S. 556.

²⁵⁰*Ibid.*, S. 557.

²⁵¹*Ibid.*, S. 557.

²⁵²*Ibid.*, S. 557.

²⁵³Vgl. Brink, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 76 zu § 38 BDSG sowie Gola/Klug/Körffner, *Bundesdatenschutzgesetz Kommentar*, Gola/Schomerus (Hrsg.), 12. Auflage 2015, C.H. Beck Verlag, Rn. 26 zu § 38 BDSG.

²⁵⁴Vgl. Brink, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 78 zu § 38 BDSG sowie Petri, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 73 zu § 38 BDSG.

²⁵⁵Gola/Schulz, *Nomos Kommentar Gesamtes Arbeitsrecht*, Boecken/Düwell/Diller/Hanau (Hrsg.), Nomos Verlag 2016, Rn. 11 zu § 38 BDSG.

Verstoß gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht vorliegt, ist der Straftatbestand des § 44 BDSG erfüllt.

Die im BDSG vorgesehenen Sanktionsmöglichkeiten lassen sich systematisch in einer Tabelle zusammenfassen:

Tabelle 2: Sanktionsmöglichkeiten des BDSG (eigene Darstellung)

Norm im BDSG	Typ	Tatbestandsvoraussetzungen	Rechtsfolge
§ 43 Abs. 1	Ordnungswidrigkeit	Vorsätzliche oder fahrlässige Verletzung einer in § 43 Abs. 1 Nr. 1–11 BDSG -genannten Verfahrensvorschrift	Geldbuße bis zu 50 000 € (§ 43 Abs. 3, 1. Alt BDSG)
§ 43 Abs. 2	Ordnungswidrigkeit	Vorsätzliche oder fahrlässige Verletzung einer in § 43 Abs. 2 Nr. 1–7 BDSG -genannten materiellen Schutzvorschrift	Geldbuße bis zu 300 000 € (§ 43 Abs. 3, 2. Alt BDSG)
§ 44 Abs. 1	Straftat	Vorsätzliche Begehung einer Handlung nach § 43 Abs. 2 BDSG – gegen Entgelt oder – mit Bereicherungs- oder – Schädigungsabsicht	Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe (erfordert gemäß § 44 Abs. 2 BDSG einen Strafantrag)

Neben den genannten Vorschriften aus dem BDSG finden sich auch im StGB Sanktionsvorschriften, die bei Verletzung von Datenschutzrechtlichen Vorschriften einschlägig sind, beziehungsweise solche, die zumindest auch das Recht auf informationelle Selbstbestimmung schützen. Hierzu gehören insbesondere die §§ 202, 202a, 203 und 206 StGB, sowie ggf. §§ 263, 263 a, 268-270 und § 303a StGB.

Auch im TMG finden sich Sanktionsvorschriften. § 16 TMG erfasst Ordnungswidrigkeiten, die bei Zuwiderhandlung mit Bußgeld geahndet werden können. § 16 I TMG betrifft getarnte kommerzielle Nachrichten. Tatbestandsvoraussetzung ist der dolus directus ersten Grades. § 16 II TMG lässt demgegenüber Vorsatz sowie Fahrlässigkeit zu. § 16 II Nr. 1 hat den Verstoß gegen Informationspflichten aus § 5 I, die nur für geschäftsmäßige Telemedien gelten, zum Inhalt. Nr. 2 beinhaltet den Verstoß gegen datenschutzrechtliche Informationspflichten. In Nr. 3 geht es um die Verletzung der Sicherungspflichten aus § 13 Abs. 4 Nr. 1 – 4 oder Nr. 5. Abs. 2 Nr. 5 fasst verschiedene Pflichtverstöße bei der Datenverarbeitung zusammen und Nr. 5 verbietet die Zusammenführung, von Telemedien unter Verwendung von Pseudonymen zulässigerweise erstellte Nutzungsprofile, mit Daten über den Träger des Pseudonyms. Hauptsanktion ist das Bußgeld gem. § 65 OWiG.

Wie auch das BDSG sieht die DSGVO in Art. 58 verschiedene Anordnungen zur Beendigung von datenschutzrechtlichen Verstößen vor.

Eines der Hauptanliegen der DSGVO ist die eben erwähnte Einführung „starker Sanktionen“ bei Datenschutzverstößen, die „wehtun sollen“.²⁵⁶ Den deutschen Datenschutzbehörden stehen als „Aufsichtsbehörde“ i. S. d. Art. 5 Abs. 19 DSGVO somit zahlreiche Sanktionsmöglichkeiten bei Datenschutzverstößen zur Verfügung: Im Erwägungsgrund 119 der DSGVO ist vorgesehen, dass die Mitgliedstaaten strafrechtliche Sanktionen für die Verletzung der DSGVO festlegen können. Die Aufsichtsbehörden können Bußgelder nach der DSGVO sowohl gegen Unternehmen als auch gegen handelnde Personen verhängen.

Die in Art. 79 DSGVO normierten Tatbestände reichen deutlich weiter als die bisherigen Bußgeldtatbestände nach § 43 BDSG. Art. 58 Abs. 2 lit i) DSGVO sieht vor, dass Bußgelder gemäß Art. 83 DSGVO verhängt werden können. Aufgeführte Verstöße können mit einem Bußgeld von bis zu 10 Millionen Euro oder im Fall eines Unternehmens 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden. Die DSGVO sieht keine konkrete Zahl als Höchstgrenze vor. Die Verstöße können zu Geldbußen von bis zu € 20 Mio. oder im Fall eines Unternehmens sogar bis zu 4 % des Jahresumsatzes führen.²⁵⁷ Welche konkreten Voraussetzungen erfüllt sein müssen, damit ein Bußgeld verhängt werden kann, bestimmt die DSGVO nicht. Die Aufsichtsbehörde hat jedoch sicherzustellen, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Erwägungsgrund 120 DSGVO verweist zudem auf Art. 101 und Art. 102 AEUV. Damit bezieht sich die DSGVO bei der Berechnung von Bußgeldern auf den kartellrechtlichen Unternehmensbegriff. Über die Anwendung des kartellrechtlichen Unternehmensbegriffs ist jedoch eine Diskussion entbrannt (dazu unten).

Im Gegensatz zur DSGVO ist im BDSG die verantwortliche Stelle nach §3 Abs. 7 BDSG der zentrale Begriff bei der Bußgeldberechnung. Verantwortliche Stelle ist danach jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Werden personenbezogene Daten durch Unternehmen verarbeitet, wird dieses Unternehmen als eigenständige verantwortliche Stelle angesehen.²⁵⁸ Bei Unternehmensgruppen gilt, dass nicht der Konzern als solcher, sondern jede einzelne Konzerngesellschaft für sich verantwortliche Stelle ist.²⁵⁹

c. Probleme

Bußgeldfestsetzung

Zwar finden sich verschiedene Sanktionsvorschriften für Datenschutzrechtsverstöße. Fraglich erscheint jedoch deren Effektivität. Bei den Bußgeldern gilt zwar § 43 Abs. 3 Satz 2

²⁵⁶ S. 2.

<http://www.janalbrecht.eu/fileadmin/material/Dokumente/Datenschutzreform_Stand_der_Dinge_10_Punkte_110615.pdf> (zuletzt abgerufen am 30.11.2016).

²⁵⁷ Faust/Spittka/Wybitul, „Milliardenbußgelder nach der DS-GVO? - Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz“, (2016), *Zeitschrift für Datenschutz*, Heft 3, S. 120-125, S. 123.

²⁵⁸ Dammann, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 223 zu § 3 BDSG in Faust/Spittka/Wybitul, „Milliardenbußgelder nach der DS-GVO? - Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz“, (2016), *Zeitschrift für Datenschutz*, Heft 3, S. 120-125, S. 122.

²⁵⁹ Ibid.

BDSG, wonach das Bußgeld so festgesetzt werden muss, dass es den wirtschaftlichen Vorteil, der sich für den Täter aus der Pflichtverletzung ergibt, übersteigt.²⁶⁰ Allerdings wird in der Praxis der Bußgeldrahmen von den Behörden noch nicht ausgeschöpft. Zum Beispiel wurde bereits ein Bußgeld von lediglich 150,00 EUR gegen ein Unternehmen verhängt, das dem Auskunftersuchen eines Betroffenen nicht entsprach.²⁶¹ Die Gesamthöhe der Geldbußen für die Jahre 2014 und 2015 einer deutschen Landesdatenschutzbehörde betrug knapp 13.000,00 EUR.²⁶² Durch die Festsetzung zu niedriger oder durch das Absehen der Festsetzung von Bußgeldern geht allerdings der Abschreckungseffekt von Bußgeldern verloren.²⁶³ Der Vorteil, den manch großes Unternehmen durch datenschutzrechtswidrige Praktiken erlangt, kann daher höher sein als der Verlust, den es durch ein etwaiges Bußgeld riskiert.²⁶⁴ Dieser Eindruck wird auch dadurch bestärkt, dass nicht jeder Datenschutzverstoß letztendlich zur Festsetzung eines Bußgeldes durch die Aufsichtsbehörde führt.²⁶⁵ Bußgeldverfahren wegen Verstößen gegen datenschutzrechtliche Bestimmungen wurden in den letzten Jahren nur sehr selten eingeleitet und mündeten noch seltener in gerichtlichen Verfahren.²⁶⁶ Im Endeffekt stellt der Erlass von Bußgeldbescheiden sogar eine Ausnahme dar.²⁶⁷

Ob sich diese Praxis unter Anwendung der DSGVO weiter fortsetzt bleibt abzuwarten. Die DSGVO nimmt in Erwägungsgrund 150 für die Berechnung der Bußgelder Bezug auf den kartellrechtlichen Unternehmensbegriff nach Art. 101 und 102 AEUV. Dies bedeutet, dass oftmals ein höherer Bußgeldrahmen angewandt werden könnte. Nach dem kartellrechtlichen Unternehmensbegriff wird jede wirtschaftlich tätige Einheit, unabhängig von ihrer Rechtsform und der Art der Finanzierung, als ein Unternehmen angesehen, auch wenn sie aus mehreren Unternehmen besteht.²⁶⁸ Sinn der Figur der wirtschaftlichen Einheit ist es, das Vorliegen nur eines einzigen Unternehmens zum Zeitpunkt des Wettbewerbsverstoßes zu

²⁶⁰ Nink, *Recht der elektronischen Medien Kommentar*, Spindler/Schuster (Hrsg.), (C.H. Beck Verlag, 2015), Rn. 17 zu § 43 BDSG.

²⁶¹ S. 394

<https://www.tlfdi.de/imperia/md/content/datenschutz/taetigkeitsberichte/2_tigkeitsbericht.pdf> (zuletzt abgerufen am 30.11.2016).

²⁶² Ibid.

²⁶³ Holländer *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 71 zu § 43 BDSG.

²⁶⁴ Vgl. Bundesregierung, BT-Drucksache 16/12011 *Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften* (Drucksache 16/12011 18.02.2009), S. 36.

²⁶⁵ Holländer *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 75 zu § 43 BDSG.

²⁶⁶ Ehmann, *Kommentar zum Bundesdatenschutzgesetz*, Simitis (Hrsg.), 8. Auflage 2014, Nomos Verlag, Rn. 21 zu § 43 BDSG.

²⁶⁷ Ibid., Rn. 80 zu § 43 BDSG. Eine Ausnahme von dieser Beobachtung gab es allerdings im Nachspiel von mehreren Datenschutzskandalen im Jahr 2008, als die Aufsichtsbehörden erstmals Bußgelder in sechstelliger Höhe oder höher verhängten, s. a. Holländer *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2016, C.H. Beck Verlag, Rn. 74 zu § 43 BDSG.

²⁶⁸ St. Rspr., s. etwa Case C-41/90, Klaus Höfner und Fritz Elser v. Macrotron GmbH, EU:C:1991:161; Case C-205/03 P – FENIN v. Kommission, EU:C:2006:453; dazu auch: Weiß, *EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar*, Calliess/Ruffert (Hrsg.), 5. Auflage 2016, C.H. Beck Verlag, Rn. 33 zu Art. 101 AEUV.

begründen.²⁶⁹ Die Zurechnung innerhalb einer Unternehmensgruppe erfolgt somit von unten nach oben.²⁷⁰ In Bezug auf datenschutzrechtlich relevante Verletzungshandlungen im Rahmen der DSGVO würde dies eine Mithaftung der Muttergesellschaft für Datenschutzverstöße der Tochtergesellschaft bedeuten. Außerdem wäre dann der Höchstbetrag des Bußgelds nicht 4% des Umsatzes der rechtswidrig handelnden Gesellschaft, sondern des Umsatzes der wirtschaftlichen Einheit.²⁷¹ Dies betrifft wiederum den gesamten globalen gruppenweiten Umsatz des Konzerns.²⁷²

In der Literatur gibt es Kritik an der Anwendung des kartellrechtlichen Unternehmensbegriffs im Datenschutzrecht. Eine solche sei systemwidrig: Nach Faust, Spittka und Wybitull stehe das kartellrechtliche Verständnis des Unternehmens als wirtschaftliche Einheit unabhängig vom Rechtssubjekt nicht nur im Widerspruch zum System der Sanktionen für Datenschutzverstöße nach bislang geltendem Recht, sondern passe auch nicht in die materiell-rechtliche Systematik der DSGVO.²⁷³ Ihrer Ansicht nach werden auch in der DSGVO Konzerne oder andere Unternehmensgruppen gerade nicht als „datenschutzrechtliche Einheit“ angesehen. Problematisiert wird in diesem Zusammenhang auch, dass sich die Definition des Unternehmensbegriffs lediglich im Erwägungsgrund und nicht in der DSGVO selbst befindet. Erwägungsgründe dürften jedoch keine Bestimmungen mit normativem Gehalt enthalten und werden im Gegensatz zum verfügbaren Teil so formuliert, dass ihre Unverbindlichkeit deutlich werde.²⁷⁴

Dem lässt sich jedoch entgegenhalten, dass Erwägungsgründe durchaus als Auslegungshilfe herangezogen werden können und als solche anerkannt sind. Im Übrigen könnte die Heranziehung des Konzernumsatzes als Berechnungsmaßstab die bisher niedrige Abschreckungswirkung von Bußgeldern verbessern. Damit könnte die Rechtsdurchsetzung im Datenschutzrecht effektiver gestaltet werden.

Mangelnde Ausstattung

Die mangelnde Einleitung von Bußgeldverfahren durch die Datenschutzbehörde könnte symptomatisch für ein weiteres Problem sein. Die Tätigkeitsberichte der Landesdatenschutzbehörden machen auf ein Kapazitätsproblem aufmerksam.

Die monierte Unterausstattung der Landesdatenschutzbehörden ist insbesondere für die Kontrolle der IT-Branche problematisch. Im Zusammenhang mit der Untersuchung von

²⁶⁹ Case 170/83 Hydrotherm, Gerätebau GmbH v. Firma Compact del Dott. Ing. Mario Andreoli & C. Sas., EU:C:1984:271; Case C-501/11 Schindler Holding u.a. v. Kommission, EU:C:2013:522, Rn. 104; Case T-11/89, Shell International Chemical Company Ltd v. Commission of the European Communities, EU:T:1992:33; Dass die wirtschaftliche Einheit später, zum Zeitpunkt der Kommissionsentscheidung, nicht mehr vorliegt, ist unschädlich, Case T-517/09, Alstom v European Commission, EU:T:2014:999.

²⁷⁰ Faust/Spittka/Wybitull, „Milliardenbußgelder nach der DS-GVO? - Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz“, (2016), *Zeitschrift für Datenschutz*, Heft 3, S. 120-125, S. 121.

²⁷¹ Ibid., S. 124.

²⁷² Ibid., S. 123.

²⁷³ Dieser Absatz basiert auf ibid., S. 120 f.

²⁷⁴ S. 22, <<http://eur-lex.europa.eu/content/techleg/KB0213228DEN.pdf>> (zuletzt abgerufen am 30.11.2016).

Apps²⁷⁵ beispielsweise, wurden im Jahr 2014 11.000 Webauftritte in Baden-Württemberg ansässiger Unternehmen mit einer selbst entwickelten Prüfplattform untersucht. Solche Kontrollen binden erhebliche personelle und finanzielle Kapazitäten, „denn förmliche Abmahnschreiben oder datenschutzrechtliche Verfügungen an tausende von Unternehmen können nicht ohne weiteres aus der sprichwörtlichen Portokasse gezahlt werden.“²⁷⁶ Ein weiteres mit Kapazitätsgründen begründbares Beispiel aus Europa bildet die irische Datenschutzbehörde, die nach Auskunft des Vereins Europe v. Facebook nach dem Verfahren *Schrems gegen Facebook* aufgehört hat, Beschwerden mit Einzelfallentscheidung zu bearbeiten und stattdessen eine Standard E-Mail-Antwort eingeführt, weswegen der Verein Verbraucher dazu aufruft, gegen die irische Behörde bei der Europäischen Kommission Beschwerde einzulegen.²⁷⁷

Boykottierung

Außerdem sind Behörden mit allgemeinen praktischen Umsetzungsproblemen konfrontiert. Im Zuge von Abmahnungen gegen Unternehmen aufgrund Facebook-Fanpages ist die Behörde direkt mit Facebook in Kontakt gewesen. Thilo Weichert, Leiter des ULD bis zum Jahr 2015 beschrieb in einem Interview²⁷⁸ eine Vermeidungsstrategie des Unternehmens folgendermaßen:

„Im Rahmen der Zuständigkeit verweist Facebook auf Irland, wo der europäische Hauptsitz ist, oder auf die USA, wo es kein valides Datenschutzrecht gibt. Weitere Taktik ist die Verweigerung von Fakten. Wenn man Informationen will bedarf es folgend aufwändiger Webanalysen. Die interne Datenverarbeitung verweigert zudem Auskünfte. Um die Aufsichtsbehörden weiterhin lahmzulegen werden die personell unterbesetzten Behörden mit Hinhaltetaktik und irrelevanten Fragestellungen beschäftigt, z. B. marginalen Änderungen von Nutzungsbestimmungen. Kommt es zu rechtlichen Auseinandersetzungen spielt der Konzern auf Zeit und im Falle von Gerichtsbeschlüssen werden diese ignoriert.“

II. Internationale Rechtsdurchsetzung

1. Europäische Ebene

Mit der Datenschutzrichtlinie 95/46/EG²⁷⁹ und der Verordnung wurde das Datenschutzrecht in der EU harmonisiert und ein Rechtsrahmen für die Gewährleistung eines gleichwertigen Schutzes geschaffen.²⁸⁰ Was die Rechtsdurchsetzung angeht, sind die meisten Regelungen

²⁷⁵ Dieser Absatz basiert auf S.30, <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/01/32_TB_Internet.pdf>

(zuletzt abgerufen am 30.11.2016).

²⁷⁷ <http://europa-v-facebook.org/DE/Daten_verlangen/Beschwerde_einreichen/beschwerde_einreichen.html> (zuletzt abgerufen am 30.11.2016).

²⁷⁸ <<https://futurezone.at/netzpolitik/facebooks-geschaeftsmodell-ist-illegal/24.583.706>> (zuletzt abgerufen am 30.11.2016).

²⁷⁹ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23/11/1995, S. 31 –50.

²⁸⁰ Grapentin, *Handbuch IT- und Datenschutzrecht*, Auer-Reinsdorff/Conrad (Hrsg.), (C.H. Beck Verlag, 2016), Rn.1 zu § 35 Grenzüberschreitende Datenverarbeitung.

mit der Festschreibung von Zuständigkeiten befasst. Werden personenbezogene Daten im Rahmen der Tätigkeit einer Niederlassung verarbeitet, dann ist gemäß Art. 4 EU-DSRL grundsätzlich das nationale Datenschutzrecht des Mitgliedsstaates anwendbar, in dessen Geltungsgebiet sich die Niederlassung befindet. Wenn es mehrere Niederlassungen gibt, ist für deren Tätigkeiten das Recht des EU-Mitgliedsstaates maßgeblich, in dem die datenverarbeitende Niederlassung jeweils belegen ist. Gemäß Art. 28 der RL 95/45/EG wurden alle Mitgliedsstaaten zudem verpflichtet, eine oder mehrere unabhängige Datenschutzkontrollstellen einzurichten.²⁸¹

Auf Grundlage der Art. 41 ff Datenschutz-VO Nr. 45/2001²⁸² wurde der Europäische Datenschutzbeauftragte als Kontrollinstanz bestimmt.²⁸³ Die Zuständigkeit des Europäischen Datenschutzbeauftragten liegt in der Überwachung und Durchsetzung der Anwendung der Verordnungsbestimmungen und aller anderen Rechtsakte der Gemeinschaft zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten durch ein Organ oder eine Einrichtung der Gemeinschaft.²⁸⁴ Die Aufsicht beruht größtenteils auf individuellen Meldungen über Verarbeitungen personenbezogener Daten durch ein Unternehmen oder eine europäische Einrichtung.²⁸⁵ Bei einer zulässigen Beschwerde führt der Europäische Datenschutzbeauftragte eine Untersuchung durch. Die Untersuchungsergebnisse werden dem Beschwerdeführer übermittelt und etwaige erforderlichen Maßnahmen ergriffen. Neben Stellungnahmen zu Verwaltungsmaßnahmen der europäischen Organe und Einrichtungen kann der Europäische Datenschutzbeauftragte auch auf eigene Initiative Untersuchungen einleiten.

Die DSGVO regelt in den Arts. 51 ff. die Arbeit der Aufsichtsbehörden. In der Begründung für die allgemeine Zuständigkeit im Hoheitsgebiet des eigenen Mitgliedstaats, wenn ein für die Verarbeitung Verantwortlicher oder ein Auftragsdatenverarbeiter Niederlassungen in mehreren Mitgliedstaaten hat, wird angeführt, dass „eine einheitliche Rechtsanwendung (Prinzip einer zentralen Anlaufstelle für den Datenschutz)“ gewährleistet werden soll. Damit sollen Mehrfachzuständigkeiten vermieden werden (One-Stop-Shop-Prinzip). In der Praxis bedeutet das, dass für ein Unternehmen, welches seinen Hauptsitz im Geltungsbereich der DSGVO hat, die Aufsichtsbehörde des Landes zuständig ist, in dem das Unternehmen seinen Hauptsitz hat. Diese Aufsichtsbehörde ist gegebenenfalls nach dem Recht des Mitgliedsstaates landesintern zu bestimmen. Bei Unternehmen, die ihren Hauptsitz außerhalb des Geltungsbereichs der DSGVO haben ist der Ort der Hauptniederlassung im Geltungsbereich der Verordnung maßgebend.

Abgesehen von Zuständigkeitsregelungen, soll die DSGVO außerdem die Vereinheitlichung der Datenschutzregelungen der EU Mitgliedstaaten bewirken. Ob dies tatsächlich der Fall ist,

²⁸¹ Hatje, *EU-Kommentar*, Schwarze/Becker/Hatje/Schoo (Hrsg.), 3. Auflage 2012, Nomos Verlag, Rn. 9 zu Art. 16 AEUV.

²⁸² VO (EG) Nr. 45/2001 v. 18.12.2000, ABl. 2001 Nr. L 8/1, 12.1.2001.

²⁸³ Hatje, *EU-Kommentar*, Schwarze/Becker/Hatje/Schoo (Hrsg.), 3. Auflage 2012, Nomos Verlag, Rn. 9 zu Art. 16 AEUV.

²⁸⁴ Ibid., Rn. 9 zu Art. 16 AEUV.

²⁸⁵ <<https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/Supervision>> (zuletzt abgerufen am 30.11.16).

ist fraglich. An über 60 Stellen befinden sich in der DSGVO sog. Öffnungsklauseln, die es nationalen Gesetzgebern erlauben, Konkretisierungen in bestimmten Bereichen vorzunehmen. Zum Beispiel können die Mitgliedstaaten zusätzliche Bedingungen und Einschränkungen für automatisierte Entscheidungen wie Profiling aufstellen, Art. 22 II lit. b) DSGVO. Eine allgemeine Öffnungsklausel befindet sich außerdem in Art. 23 DSGVO, der – unter der Beachtung der Grundrechte und Grundfreiheiten - ausdrücklich Beschränkungen der Rechte auf Auskunft, Information, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch auf Mitgliedstaatenebene erlaubt.

Die Durchsetzung von Verbraucherrechten allgemein wird in der EU von der CPC-Verordnung 2006/2004²⁸⁶ geregelt. Das mit der CPC-Verordnung 2006/2004 errichtete europäische Behördennetzwerk „Consumer Protection Cooperation“ wird aktiv, wenn Interessen einer Vielzahl von Verbrauchern eines Mitgliedstaates der EU durch ein Unternehmen eines anderen verletzt oder gefährdet ist. Dies umfasst keine Schadenersatzansprüche o.ä.; vielmehr geht es um die Beseitigung von Störungszuständen für eine Vielzahl von Verbrauchern in einem Mitgliedsstaat. In Deutschland erfolgt die Koordinierung durch das Bundesministerium der Justiz und für Verbraucherschutz, welches außerdem Anliegen an das Luftfahrt-Bundesamt, die Bundesanstalt für Finanzdienstleistungsaufsicht, das Eisenbahn-Bundesamt und verschiedene Landesbehörden, der Verbraucherzentrale Bundesverband e.V. und die Zentrale zur Bekämpfung unlauteren Wettbewerbs e.V. weiterleiten kann.²⁸⁷

Im Rahmen des CPC-Netzwerks führten beispielsweise die Europäische Kommission gemeinsam mit nationalen Verbraucherschutzverbänden in den Jahren 2013 und 2014 Verhandlungen mit Apple, Google und der Interactive Software Federation of Europe , um die Irreführung von Verbrauchern durch sog. In-App-Käufe zu verhindern, im Zuge derer die Unternehmen zusicherten, die Worte „gratis“/„kostenlos“ nicht mehr für solche Apps zu verwenden.²⁸⁸ Solch Vorgehen zeigt, dass grenzüberschreitende Fälle in der EU durch direkte Verhandlungen mit den betroffenen Unternehmen durchaus gelöst werden können.

Trotz Erfolgen wie diesem, ist das CPC-Netzwerk auch von Defiziten geprägt. Die europäische Kommission hat im Rahmen der Digitalmarktstrategie²⁸⁹ eine Verbesserung der zugrundeliegenden CPC-Verordnung 2006/2004 angestrengt, um die unzureichende gegenseitige Unterstützung, mangelnde Compliance, die mangelnden Maßnahmen zur Begegnung von weitreichenden Verletzungshandlungen in der EU, insbesondere auf dem Markt für digitale Güter, sowie die oftmals schwierige Ermittlung von Verstößen und

²⁸⁶ Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates vom 27. Oktober 2004 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden („Verordnung über die Zusammenarbeit im Verbraucherschutz“), OJ L 364, 9.12.2004, S. 1–11.

²⁸⁷ Dazu <http://www.bmfv.de/DE/Verbraucherportal/Verbraucherinformation/CPC/CPC_node.html> (zuletzt abgerufen am 30.11.2016).

²⁸⁸ Dazu <http://ec.europa.eu/justice/newsroom/consumer-marketing/news/141222_en.htm> (zuletzt abgerufen am 30.11.2016).

²⁸⁹ <http://europa.eu/rapid/press-release_IP-15-4919_de.htm> (zuletzt abgerufen am 30.11.2016).

unzureichender Priorisierung von Durchsetzungsvorgehen zu verbessern.²⁹⁰ Der Vorschlag für eine neue Verordnung beinhaltet u.a.:

- Ein Update von Definitionen, um beispielsweise auch bereits abgeschlossene Handlungen zu erfassen, die jedoch noch weitergehende Verletzungseffekte haben;
- Minimalkompetenzen für die zuständigen Behörden;
- Die Errichtung eines ‘Amtshilfemechanismus’ für Anträge auf Information oder die Anwendung von Durchsetzungsmaßnahmen;
- Besondere Vorschriften für die Abhilfe von verbreiteten Rechtsverletzungen, wie z.B. Schwellenwerte für die Anzahl der betroffenen Mitgliedstaaten und betroffene Bevölkerung, die festlegen wann mutmaßliche Rechtsverletzungen EU-weiten Charakter haben;
- Gemeinsame prozessuale Vorschriften für koordinierte Maßnahmen;
- Ein neues Überwachungssystem, das das gegenwärtige Alert-System mit weiteren Informationsmechanismen kombiniert.

Die regelmäßigen Überprüfungen der Kommission sind zu begrüßen. Ob diese vorgeschlagenen Neuerungen durch den legislativen Prozess so angenommen werden bzw. ob sie tatsächlich zu einer Verbesserung für den Verbraucherrechtsschutz führen, bleibt abzuwarten.²⁹¹

2. Internationale Ebene

Im Internet der Dinge ist es angesichts der international tätigen Unternehmen, die IoT-Geräte herstellen, oft der Fall, dass sich die datenverarbeitende Stelle nicht im EU-Inland befindet. Dann sind sowohl formelle Zuständigkeiten, als auch die Existenz datenschutzrechtlicher Regelungen abzuklären.

a. Schutzbereich europäischer Vorschriften

Es ist beispielsweise schwierig für Verbraucher, Anspruchsgegner im internationalen Waren- und Dienstleistungsverkehr zu identifizieren und in Haftung zu nehmen. Wie im bereits erwähnten Samsung-Urteil des LG Frankfurt deutlich wurde, kann sich der konkrete Anspruchsgegner eines Verbrauchers auch im Ausland befinden, wobei es für den Verbraucher unklar ist, welche Stelle verantwortlich für die jeweilige Datenerhebung und –verarbeitung ist. Das LG entschied, dass die südkoreanische Muttergesellschaft Samsung verantwortlich sei. Damit war ein Teil der Ansprüche gegen den falschen Anspruchsgegner (Samsung Deutschland) gerichtet und musste abgewiesen werden.

Dass die Abklärung von Zuständigkeiten schwierig ist, zeigen noch andere Urteile in der Rechtsprechung. Es sei auf einen Fall vor dem KG Berlin²⁹² verwiesen, welches in einem Verfahren gegen Facebook die amerikanische Konzernmutter als datenschutzrechtlich

²⁹⁰ S. 3 – 5, <<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0165>> (zuletzt abgerufen am 30.11.2016).

²⁹¹ Eine erste Stellungnahme des VZBV sieht sowohl positive Entwicklungen, wirft aber auch neue Fragen auf, <http://www.vzbv.de/sites/default/files/stellungnahme_vzbv_cpc.pdf> (zuletzt abgerufen am 30.11.2016).

²⁹² KG, Urteil vom 24.01.2014 - 5 U 42/12 (LG Berlin) (nicht rechtskräftig).

verantwortliche Stelle und die Anwendbarkeit des BDSG (§ 1 Abs. 5 Satz 2) bejahte, während das Oberverwaltungsgericht Schleswig (Beschluss vom 22.04.2014, Az. 4 MB 11/13) in einem Verfahren des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein gegen Facebook die Anwendbarkeit des BDSG mit dem Argument verneinte, die irische Konzerntochter sei die datenschutzrechtlich verantwortliche Stelle, weshalb irisches Datenschutzrecht anzuwenden sei (§ 1 Abs. 5 Satz 1 BDSG). In einem weiteren Fall erklärte das LG Berlin²⁹³ allein unter Anwendung der Rom-I-Verordnung deutsches AGB-Recht - und somit auch das BDSG - auf die Datenschutzrichtlinie des IT-Anbieters Apple für anwendbar, und zwar unabhängig von § 1 Absatz 5 BDSG, der die Anwendbarkeit des BDSG davon abhängig macht, ob die Datenverarbeitung durch eine Niederlassung in einem Drittland wie den USA (dann BDSG) oder in einem Mitgliedstaat der EU wie Irland (dann irisches Datenschutzrecht) erfolgt.

In dem Versuch, den Anwendungsbereich der europäischen Vorschriften möglichst weit zu gestalten, hat der EuGH im Google-Urteil entschieden, dass wenn personenbezogene Daten im Rahmen der Tätigkeit einer Niederlassung in der EU (Spanien) verarbeitet werden und ein Suchmaschinenbetreiber aus den USA in Spanien für die Vermarktung und den Verkauf von Werbeflächen eine Niederlassung einrichtet, deren Tätigkeit sich an die Einwohner Spaniens richtet. Nach dem EuGH gilt das auch dann, wenn die datenverarbeitende Tätigkeit selbst nicht von der spanischen Niederlassung ausgeführt wird.²⁹⁴ Damit unterfalle die Tätigkeit der Datenverarbeitung europäischen Regeln.

In diesem Sinne ist die DSGVO gem. ihres Artikels 3 auf die Verarbeitung personenbezogener Daten anwendbar, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragsdatenverarbeiters in der EU erfolgt, und zwar unabhängig davon, ob die Verarbeitung selbst in der EU stattfindet. Die DSGVO findet ferner Anwendung, wenn die Datenverarbeitung in einem Zusammenhang mit einem Waren- oder Dienstleistungsangebot oder dem Verhalten einer betroffenen Person in der EU steht und wenn der Verantwortliche aufgrund von völkerrechtlichen Vorschriften dem Recht eines EU-Mitgliedstaates unterliegt.

b. Datenschutzniveau

Werden Daten in Drittstaaten übermittelt, bedarf es besonderer Schutzvorkehrungen, um das im europäischen Binnenmarkt harmonisierte Datenschutzniveau nicht zu umgehen.²⁹⁵ Der Grundsatz manifestiert Art. 25 Abs. 1 RL 95/46/EG wonach personenbezogene Daten in Staaten außerhalb der Europäischen Union übermittelt werden dürfen, wenn sie ein angemessenes Schutzniveau gewährleisten. Ob das Schutzniveau eines Drittstaates angemessen ist, beurteilt die Kommission (Art. 25 Abs. 6 RL 95/46/EG). Daneben besteht für die Mitgliedsstaaten die Möglichkeit, dass personenbezogene Daten unter den Voraussetzungen des Art. 26 Abs. 1 RL 95/46/EG in bestimmten Einzelfällen an Drittstaaten

²⁹³ LG Berlin, Urteil vom 30.04.2013 – 15 O 92/12.

²⁹⁴ Case C-131/12, Google Spain SL/Google Inc. v. Agencia Española de Protección de Datos/Maria Costeja González, EU:C:2014:317.

²⁹⁵ Ähnl. Gola/Klug/Körffer, *Kommentar zum Bundesdatenschutzgesetz*, Gola/Schomerus (Hrsg.) 12. Auflage 2015, C.H. Beck Verlag, Rn. 20 zu § 4 b BDSG.

übermittelt werden dürfen, obwohl diese kein angemessenes Schutzniveau gewährleisten.²⁹⁶ Dies ist insbesondere dann möglich,

- Wenn eine Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses erfolgt, Art. 45 DSGVO.
- wenn die betroffene Person eingewilligt hat, sofern die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und der für die Verarbeitung verantwortlichen Stelle erforderlich ist, sowie zur Wahrung eines wichtigen öffentlichen Interesses oder eines lebenswichtigen Interesses der betroffenen Person, s. Art 49 DSGVO.²⁹⁷
- wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre bietet, Art. 46 DSGVO.²⁹⁸ Die hierfür wichtigsten Maßnahmen sind zum einen vertragliche Vereinbarungen zwischen dem für die Verarbeitung Verantwortlichen und dem Empfänger der Daten im Drittstaat, zum anderen verbindliche unternehmensinterne Datenschutzregelungen (Binding Corporate Rules).

c. Safe-Harbor

Gem. §§ 4b II 2, 4c I BDSG, Arts. 25 und 26 EU-DSRL und Art. 45 DSGVO kommt es also darauf an, ob in dem Land, in welches die Daten übertragen werden, ein angemessenes Datenschutzniveau gegeben ist. In dieser Hinsicht hatte die Europäische Kommission mit den USA die sogenannten Safe-Harbor-Prinzipien vereinbart.²⁹⁹

1. Informationspflicht: Die Unternehmen müssen die Betroffenen darüber informieren, welche Daten sie für welche Zwecke erheben und welche Rechte die Betroffenen haben.
2. Wahlmöglichkeit: Die Unternehmen müssen den Betroffenen die Möglichkeit geben, der Weitergabe ihrer Daten an Dritte oder der Nutzung für andere Zwecke zu widersprechen.
3. Weitergabe: Wenn ein Unternehmen Daten an Dritte weitergibt, muss es die Betroffenen darüber und die unter 2. aufgeführte Wahlmöglichkeit informieren.
4. Zugangsrecht: Die Betroffenen müssen die Möglichkeit haben, die über sie gespeicherten Daten einzusehen und sie ggfs. berichtigen, ergänzen oder löschen können.

²⁹⁶ Holznagel/Dietze, *Europarecht – Handbuch für die deutsche Rechtspraxis*, Schulze/Zuleeg/Kadelbach (Hrsg.), (Nomos Verlag, 2015), Rn. 21 zu § 37 Europäischer Datenschutz.

²⁹⁷ Als Auslegungshilfe vgl

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_de.pdf> (zuletzt abgerufen am 30.11.2016); zu den einzelnen Ausnahmetatbeständen vgl Ehmann/Helfrich, *EG-Datenschutzrichtlinie Kurzkomentar*, Ehmann/Helfrich (Hrsg.), Otto Schmidt Verlag 1999, Rn. 6ff zu Art. 26 [EU-DSRL]; Holznagel/Dietze, *Europarecht – Handbuch für die deutsche Rechtspraxis*, Schulze/Zuleeg/Kadelbach (Hrsg.), (Nomos Verlag, 2015), Rn. 21 zu § 37 Europäischer Datenschutz.

²⁹⁸ Holznagel/Dietze, *Europarecht – Handbuch für die deutsche Rechtspraxis*, Schulze/Zuleeg/Kadelbach (Hrsg.), (Nomos Verlag, 2015), Rn. 22 zu § 37 Europäischer Datenschutz.

²⁹⁹ Grundsätze des „sicheren Hafens“ zum Datenschutz, Verkündungsblatt ausgewertet bis 15.09.2016

[E 2000/520/EG] Anhang I: Text gilt seit 01.07.2002

5. Sicherheit: Die Unternehmen müssen angemessene Sicherheitsvorkehrungen treffen, um die Daten vor unbefugtem Zugang oder vor Zerstörung und Missbrauch zu schützen.
6. Datenintegrität: Die Unternehmen müssen sicherstellen, dass die von ihnen erhobenen Daten korrekt, vollständig und zweckdienlich sind.
7. Durchsetzung: Die dem Safe Harbor beigetretenen Unternehmen verpflichten sich zudem, Streitschlichtungsmechanismen beizutreten.

Der EuGH hat in seiner Safe-Harbor-Entscheidung am 6. Oktober 2015 diese Prinzipien jedoch für ungültig erklärt.³⁰⁰ Hintergrund des Urteils ist das Aufsehen erregende Verfahren von Maximilian Schrems gegen den Data Protection Commissioner, in welchem ersterer bei der Irischen Datenschutzbehörde Beschwerde wegen der Datenerhebung und –verarbeitung bei Facebook eingelegt hatte. Die von ihm an Facebook gelieferten Daten werden von der irischen Tochtergesellschaft von Facebook ganz oder teilweise an Server, die sich in den USA befinden, übermittelt und dort verarbeitet. Vor dem Hintergrund der Enthüllungen von Edward Snowden bezweifelt Schrems die Angemessenheit des Schutzniveaus für Daten in den U.S.A. Der irische High Court legte dem EuGH die Vorabentscheidung vor, ob die zugrundeliegende Entscheidung der Europäischen Kommission³⁰¹ für die irische Behörde präjudiziell in dem Sinne sei, dass die Angemessenheit des Schutzniveaus nicht von ihr geprüft werden kann.

Der EuGH stellte fest, dass die Existenz einer Entscheidung der Kommission, in der festgestellt wird, dass ein Drittland ein angemessenes Schutzniveau für übermittelte personenbezogene Daten gewährleistet, die Befugnisse, über die die nationalen Datenschutzbehörden aufgrund der Charta der Grundrechte der Europäischen Union und der Richtlinie verfügen, weder beseitigen noch auch nur beschränken kann. Daher seien nationale Datenschutzbehörden im Rahmen einer Beschwerde verpflichtet, in völliger Unabhängigkeit zu prüfen, ob bei der Übermittlung der Daten einer Person in ein Drittland die in der Richtlinie aufgestellten Anforderungen gewahrt werden. Darüber hinaus erklärte der EuGH die Entscheidung der Kommission für ungültig, dass sie dem Verhältnismäßigkeitsgrundsatz nicht entspreche, da sie Behörden gestatte, generell auf den Inhalt elektronischer Kommunikation zuzugreifen und damit das Grundrecht auf Achtung des Privatlebens verletze. Da kein Rechtsbehelf des betroffenen Bürgers vorgesehen war, sei auch das Grundrecht auf wirksamen gerichtlichen Rechtsschutz ebenfalls verletzt.

d. Der Nachfolger: Privacy Shield

Anfang 2016 gab die Europäische Kommission bekannt, sie habe sich mit der amerikanischen Regierung auf eine Nachfolgeregelung zum Safe-Harbor-Agreement geeinigt: Das sog. Privacy-Shield. Am 12.07.2016 verabschiedete die Kommission offiziell die endgültige Fassung des EU-US Privacy Shield als Angemessenheitsentscheidung nach

³⁰⁰ Case C-362/14, Maximilian Schrems v. Data Protection Officer, EU:C:2015:650.

³⁰¹ Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen häufig gestellten Fragen (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABI L 215/7, 25.8.2000.

Art. 25 IV der Datenschutzrichtlinie (Richtlinie 95/46/EG).³⁰² Paragraphen 19 bis 20 der sog. Implementierungsentscheidung Privacy Shield (IE-PS) beinhalten die Grundsätze für die Übermittlung von personenbezogenen Daten in Drittländer: Notice, Choice, Accountability, Security, Data Integrity, Purpose Limitation, Access, Recourse, Enforcement, and Liability. Die Grundsätze und Regelungen des Privacy Shield sind auf alle Datensubjekte anwendbar, deren personenbezogene Daten aus der EU zu teilnehmenden Unternehmen und Organisationen in den U.S.A. übermittelt werden.

Im Rahmen des Privacy Shield können sich Unternehmen seit dem 01.08.2016 in die „Privacy Shield List“ eintragen. Die Prinzipien der Teilnahme sind in Annex II des „EU-U.S.: Privacy Shield Framework Principles issued by the U.S. Department of Commerce“ enthalten. Für die Eintragung ist, wie nach dem alten Safe Harbor, die Selbstzertifizierung des US-Datenempfängers gegenüber dem US-Department of Commerce erforderlich, die im Rahmen einer Re-Zertifizierung jährlich zu wiederholen ist. Die Teilnahme am Privacy Shield ist freiwillig; Regelbefolgung bei Teilnahme dagegen obligatorisch.³⁰³ Damit ist die Teilnahme am Privacy Shield eine Maßnahme der Selbstregulierung.

Trotz der positiven Entwicklungen von Safe Harbour zum Privacy Shield, wie zum Beispiel der Existenz von Regelungen zu Zwecken der nationalen Sicherheit und Rechtsdurchsetzung (zum Beispiel im Hinblick auf die Auseinandersetzung mit den Rechtsschutzmöglichkeiten in den U.S.A., s. Paragraphen 91 ff. des IE-PS), ist fraglich, ob die IE-PS eine Maßnahme darstellt, die datenschutzrechtlich ein „angemessenes Datenschutzniveau“ i.S.d. § 4b II BDSG, Art 44 DSGVO bietet. Zu kritisieren sind insbesondere die zahlreichen Ausnahmen, der Mangel an vergleichbaren Datenschutzgrundsätzen, sowie fehlende Möglichkeiten des Rechtsschutzes für Betroffene.

Weitreichende Ausnahmen

So bestehen einige sehr weitreichende Ausnahmen für die Pflicht der Regelbefolgung. Nr. 5 des Annexes 2 IE-PS erwähnt als solche Ausnahmen:

- (a) to the extent necessary to meet national security, public interest, or law enforcement requirements;
- (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or
- (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable

³⁰² Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, Brussels, 12.7.2016, C(2016) 4176 final.

³⁰³ Annex 2 Nr. 2 EU-U.S.: Privacy Shield Framework Principles issued by the U.S. Department of Commerce.

contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

Die Ausnahmen legen einen äußerst breiten Spielraum für Non-Compliance aus. Insbesondere im Zusammenhang mit den Ausnahmen für öffentliche Sicherheit, öffentliches Interesse oder Rechtsdurchsetzung (lit. a) sowie für abweichendes nationales Recht (lit. c) ist fraglich, ob die Bedenken gegen den Safe-Harbour-Vorgänger nicht weiterhin Bestand haben. Es ist im Rahmen dieser Ausnahmen Behörden beispielsweise gestattet, auf Kommunikation von Bürgern und deren Daten zurückzugreifen. So kann die NSA Kommunikationen von Individuen außerhalb von den U.S.A. sammeln, wenn eine *verständige Auffassung* besteht, dass das in Frage stehende Kommunikationsmittel benutzt wird, um ausländische Sicherheitsinformationen (beispielsweise auch bzgl. „hostile cyber activities“) weiterzugeben.³⁰⁴ Diese Ausnahme ist weitreichend und unklar definiert. Ein angemessenes, vergleichbares Datenschutzniveau kann daher angezweifelt werden.

Fehlende Datenschutzgrundsätze

Diese Einschätzung bestätigt sich auch im Hinblick auf andere Regelungen des Privacy Shield. Im EU Datenschutzrecht grundlegende Prinzipien finden sich nicht in den Prinzipien des Privacy Shield wieder. Zum Beispiel ist das Gebot der Datensparsamkeit aus Art. 6 I lit. C DSGVO im Privacy Shield nicht ausdrücklich enthalten –Paragraph 89 IE-PS erlaubt sogar ausdrücklich „bulk collection“ von Daten als Ausnahme von „targeted collection“, wobei begleitende Datenminimierungsmaßnahmen getroffen werden sollen, ohne dies zu spezifizieren. Außerdem gibt es in der IE-PS kein ausdrückliches Verbot der ausschließlich automatisierten Entscheidung wie in Art. 22 DSGVO. Um die Relevanz und genaue Anwendung dieser u.a. Grundsätze, wie Zweckbindung, klarzustellen, drängt die Art 29 Data Protection Working Party auf eine Klarstellung.³⁰⁵

Unzureichender Rechtsschutz

Weitere Kritik kann gegenüber der Möglichkeiten des Rechtsschutzes für Betroffene geäußert werden. Wenn sich Betroffene gegen die Datensammlung und –verarbeitung im Bereich der Überwachung wehren wollen, stehen ihnen die folgenden Optionen zur Verfügung (Paragraphen 111 ff IE-PS):

- Monetärer Schadensersatz gem. FISA (Foreign Intelligence Surveillance Act) gegen die U.S.A. im Falle von unrechtmäßiger und wissentlicher Nutzung oder Zugänglichmachung; monetärer Schadensersatz gegen U.S. Bedienstete; Klage auf Unrechtmäßigkeit der Überwachung mit dem Ziel die Informationen nicht

³⁰⁴ Dazu Paragraph 109 IE-PS.

³⁰⁵ S.3, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> (zuletzt abgerufen am 30.11.2016).

herauszugeben, wenn diese Informationen in gerichtlichen oder behördlichen Prozessen verwandt werden sollen (112)

- Entschädigung für unrechtmäßigen, vorsätzlichen und schädigenden Zugriff auf oder Nutzung von personenbezogenen Daten durch Regierungsangestellte (113)
- Zugang zu behördlichen Akten gem. FOIA (Freedom of Information Act); allerdings können die Sicherheitsbehörden den Zugang zu den Akten aufgrund zahlreicher Ausnahmen verweigern (114)

Darüber hinaus richten die U.S.A. für den Bereich der öffentlichen Überwachung einen Ombudsmann Mechanismus ein (Privacy Shield Ombudsman, PSO, Annex III IE-PS.). Der unabhängige Ombudsmann soll sicherstellen, dass individuelle Beschwerden untersucht werden und der Betroffene unabhängige Einschätzungen über die Einhaltung von U.S.-Recht erhält (116, 117). Der Ombudsman erhält auch Beschwerden, die in der jeweiligen nationalen Sprache abgefasst und über die Aufsichtsbehörden der EU-Staaten an den Ombudsmann adressiert werden (119).

Für den Bereich der Datenschutzverletzungen durch am Privacy Shield teilnehmende Unternehmen beschränkt sich der individuelle Rechtsschutz des Privacy Shields auf Schlichtung gem. Annex I lit. B) des Annex 2 IE-PS. In diesem Rahmen können Individuen ihre Rechte im Hinblick auf Datentransfers gegenüber dem erhebenden oder verarbeitenden Unternehmen (Paragraph 43 IE-PS), welches entsprechenden Beschwerdeprozesse und -mechanismen zur Verfügung stellen muss, dem Privacy Shield Panel als Schlichtungsstelle (45 IE-PS), der nationalen Datenschutzbehörde (Paragraph 48 IE-PS), oder dem Department of Commerce (52 IE-PS), geltend machen. Das Privacy Shield Panel darf im Rahmen der Schlichtung individuell nur nicht-monetären Rechtsschutz gewähren, also z.B. Zugang, Korrektur oder Löschung personenbezogener Daten. Schadens- oder Kostenersatz sind ausdrücklich ausgeschlossen. Die Teilnahme von Datenschutzbehörden an der individuellen Schlichtung ist Annex I lit. G) Nr. 4 des Annex 2 ausdrücklich ausgeschlossen; diese dürfen lediglich auf Wunsch des Betroffenen bei der Verfassung der anfänglichen Notiz der Beschwerde, die das Schlichtungsverfahren auslöst, teilnehmen. Gerichtsstand für die Überprüfung der Entscheidungen des Privacy Shield Panels liegt bei den U.S.-amerikanischen Bezirksgerichten, in deren Bezirk der primäre Geschäftssitz des am Privacy Shield teilnehmenden Unternehmens liegt, Annex I lit. E) des Annex 2.

Damit haben Betroffene nur eingeschränkte Möglichkeiten des Rechtsschutzes. Die Rechtsschutzmöglichkeiten im öffentlichen Bereich der Überwachung durch Sicherheitsbehörden sind von zahlreichen Ausnahmen geprägt. Im privaten Bereich ist der Betroffene nur auf die Schlichtung durch das Privacy Shield Panel verwiesen, dessen Entscheidungen nur bei U.S.-Gerichten angegriffen werden können.

III. Beispiel: HCA und Rechtsschutz

Die Rechtsdurchsetzungsmöglichkeiten für Verbraucher lassen sich anhand der HCA wie folgt darstellen.

Der Verbraucher und Nutzer der HCA haben die Auskunftsansprüche gem. §§ 19, 34 BDSG, Art. 15 DSGVO gegen die verantwortliche Stelle. Verantwortliche Stelle ist laut Satz 1 der Datenschutzerklärung HCA die Home Connect GmbH mit Sitz in München. Die Home Connect GmbH muss damit den Betroffenen von der erstmaligen Erhebung und Übermittlung seiner Daten benachrichtigen und außerdem Auskunftersuchen gem. §§ 19, 34 BDSG, Art. 15 DSGVO annehmen. Für den Fall, dass die Daten unrichtig sind, kann der App-Nutzer bei Erfüllung der Voraussetzungen aus §§ 20, 35 BDSG, Arts. 16, 17 DSGVO die Berichtigung, Löschung oder Sperrung der Daten verlangen. Dies ist auch dann möglich, wenn die Datenerhebung nicht mehr dem ursprünglichen Zweck dienen, wenn also die erhobenen Daten nicht mehr der Eingruppierung in Punkt 2 der HCA-Datenschutzerklärung entsprechen, also wenn beispielsweise Benutzerstammdaten nicht mehr der Bereitstellung der Funktionalitäten der App sowie der über die App angebotenen Dienste dienen, sondern für die Verbesserung der Benutzerfreundlichkeit der App oder des weitergehenden Produkt- und Dienstleistungsangebots. Ob dieser Wegfall des ursprünglichen Zweckes jedoch für den Verbraucher ohne weiteres nachvollziehbar ist, ist fraglich.

Im Falle einer Verletzung der datenschutzrechtlichen Vorschriften, kann der Verbraucher gem. § 7 BDSG Schadensersatz von der verantwortlichen Stelle, also der Home Connect App verlangen. Gem. Art. 82 II S. 2 DSGVO hat der Verbraucher auch einen Anspruch auf Schadensersatz gegen mögliche Stellen, die seine Daten im Auftrag der Home Connect GmbH verarbeiten. Allerdings ist aus der Datenschutzerklärung selbst nicht ersichtlich, wer diese Auftragsdatenverarbeiter sind. Sofern die Home Connect GmbH auf Nachfrage die Identität dieser nicht preisgibt, könnte der Verbraucher versuchen, über die zuständige Aufsichtsbehörde wie die Landesdatenschutzbehörde Auskunft zu bekommen, da die Home Connect GmbH an diese gem. §§ 4d, 4e Nr. 2 BDSG die mit der Leitung der Datenverarbeitung beauftragten Personen meldet. Abgesehen von dem u.U. nicht unerheblichen Aufwand, der damit verbunden ist, dürfte dem Verbraucher der Nachweis eines Schadens und der Kausalität schwer fallen.

Auf nationaler Ebene könnte der Verbraucher eine Prüfung der Datenschutzerklärung als AGB anstrengen. Sollte sich herausstellen, dass diese unzulässig ist (siehe oben), macht sich der Verwender dem Verbraucher gegenüber aus c. i. c. (§§ 280 Abs. 1, 241 Abs. 2, 311 Abs. 2) schadensersatzpflichtig.³⁰⁶ Für das Individualverfahren gilt jedoch, dass nach § 305 c Abs. 2 BGB Auslegungszweifel zu Lasten des Verwenders gehen. Das bedeutet, dass einer objektiv mehrdeutige Klausel diejenige Bedeutung zugemessen wird, die im Ergebnis für den anderen Teil, typischerweise den Kunden, am günstigsten ist,³⁰⁷ die sogenannte kundengünstigste Auslegung.

³⁰⁶ BGH, Urteil vom 28.05.1984 - III ZR 63/83 (Karlsruhe); BGH, Urteil vom 12.11.1986 - VIII ZR 280/85 (Köln); BGH, Urteil vom 08.10.1987 - VII ZR 358/86 (Düsseldorf); BGH, Urteil vom 14.06.1994 - XI ZR 210/93 (Stuttgart) in Wurmnest, *Münchener Kommentar zum BGB*, Sackner/Rixecker/Oetker/Limberg (Hrsg.), 7. Auflage 2016, C.H. Beck Verlag, Rn. 8 zu § 309 BGB.

³⁰⁷ Basedow, *Münchener Kommentar zum BGB*, Sackner/Rixecker/Oetker/Limberg (Hrsg.), 7. Auflage 2016, C.H. Beck Verlag, Rn. 34 zu § 305 c BGB

Für den Verbandsprozess gemäß §§ 1, 3 UKlaG ist hingegen anerkannt, dass unklare AGB im kundenfeindlichsten Sinne auszulegen sind,³⁰⁸ d.h. dass bei mehreren Auslegungsmöglichkeiten einer Klausel von der Alternative auszugehen ist, die am ehesten ein Klauselverbot gemäß §§ 307–309 rechtfertigt.³⁰⁹ Grund für diese Handhabe ist, dass nur so der Zweck der Verbandsklage und zwar die Sanierung des Rechtsverkehrs von unangemessenen Vertragsklauseln, erreicht werden kann.³¹⁰ Vorformulierte Vertragsbedingungen dürfen den Verbandsprozess nicht unter Berufung auf die kundenfreundlichste Auslegung unbehelligt überstehen.³¹¹ Dies erleichtert die Durchsetzung des Anspruchs im Zweifel erheblich. Zudem würde die Verbandsklage eine vorbeugende Klauselkontrolle von Datenschutzerklärungen ermöglichen.³¹² Für die Erfolgsaussichten bedeutet dies, dass die der Verbandsklage der des Individualverfahrens deutlich überwiegen; und auch, dass die Ergebnisse des Individual- und des Verbandsklageverfahrens bei dem selben Sachverhalt differieren können.³¹³ Eine mögliche Divergenz ließe sich aber vermeiden, wenn für das Individualverfahren und das Verbandsklageverfahren eine identische Auslegungsregel gelten würde.³¹⁴

Der Verbraucher könnte also zur Durchsetzung seiner Ansprüche sowie zur vorbeugenden Kontrolle die Verbraucherverbände gem. § 1 UKlaG einbeziehen.³¹⁵ Das Verfahren richtet sich nach den §§ 5 ff UKlaG. Eine Schadensersatzpflicht wird allerdings grundsätzlich nicht begründet,³¹⁶ es sei denn diese ergibt sich aus *culpa in contrahendo*.³¹⁷ Würden sich Unternehmen jedoch auch mit Schadensersatzklagen bei nach §§ 305 ff. unwirksamen Datenschutzerklärungen konfrontiert sehen, würde dies die Abschreckungswirkung erheblich verstärken.

In Betracht käme auch eine einstweilige Verfügung nach allgemeinen Regeln. Die Vollstreckung aus einem Unterlassungsurteil erfolgt gem. § 890 ZPO durch Verhängung von Ordnungsgeld oder -haft. Ein Widerruf wird als unvertretbare Handlung gem. § 888 ZPO durch Zwangsgeld oder -haft durchgesetzt. Um ein gerichtliches Verfahren zu vermeiden wird der Anspruch in der Praxis in aller Regel zunächst durch eine vorprozessuale

³⁰⁸ BGH, Urteil vom 05.04.1984 - III ZR 2/83 (Stuttgart); BGH, Urteil vom 19.09.1985 - III ZR 213/83 (Hamburg); BGH, Urteil vom 12.01.1994 - VIII ZR 165/92 (Düsseldorf); BGH, Urteil vom 10.05.1994 - XI ZR 65/93 (Düsseldorf); BGH, Urteil vom 19.05.2005 - III ZR 437/04 (LG Mönchengladbach); BGH, Urteil vom 23.01.2003 - III ZR 54/02 (Köln); OLG Brandenburg, Urteil vom 12.05.2004 - 7 U 165/03; s.a. Micklitz, *Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen*, Rauscher/Krüger (Hrsg.), 4. Auflage 2013, C.H. Beck Verlag Rn. 17 zu § 1 UKlaG.

³⁰⁹ Basedow, *Münchener Kommentar zum BGB*, Säcker/Rixecker/Oetker/Limberg (Hrsg.), 7. Auflage 2016, C.H. Beck Verlag, Rn. 34 zu § 305 c BGB.

³¹⁰ Ibid.

³¹¹ Ibid.

³¹² Micklitz, *Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen*, Rauscher/Krüger (Hrsg.), 4. Auflage 2013, C.H. Beck Verlag Rn. 7 zu § 1 UKlaG.

³¹³ Ibid., Rn. 18 zu § 1 UKlaG.

³¹⁴ Ibid., Rn. 18 zu § 1 UKlaG.

³¹⁵ Absatz vgl. Walker, *Unterlassungsklagengesetz Nomos Kommentar*, Walker (Hrsg.), Nomos Verlag 2016, Rn. 16-17 zu § 1 UKlaG.

³¹⁶ Micklitz, *Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen*, Rauscher/Krüger (Hrsg.), 4. Auflage 2013, C.H. Beck Verlag Rn. 4 zu § 1 UKlaG.

³¹⁷ BGH, Urteil vom 11.06.2010 - V ZR 85/09 (OLG Düsseldorf); BGH, Urteil vom 27.05.2009 - VIII ZR 302/07 (LG Frankfurt a.M.); BGH, Urteil vom 28.05.1984 - III ZR 63/83 (Karlsruhe).

Abmahnung mit der Aufforderung zur Abgabe einer strafbewehrten Unterlassungserklärung geltend gemacht.³¹⁸ Eine vorherige Abmahnung seitens des klageberechtigten Verbandes macht in diesem Fall Sinn, da der Verbraucher andernfalls bei sofortiger Anerkennung des Beklagten gem. § 93 ZPO die Kosten tragen muss, weil dieser ohne Abmahnung in der Regel keine Veranlassung zur Klageerhebung gegeben hat.³¹⁹

Vorerst bleibt bei der nationalen Rechtsdurchsetzung als „Sanktion“ die normale Zwangsvollstreckung nach einem erstrittenen Unterlassungs- bzw. Widerrufstitel.³²⁰ Das wäre nach derzeitiger Rechtslage dann auch das Durchsetzungsmittel der Verbände, wenn man die AGB-Kontrolle von Datenschutzerklärungen zuließe und diese sich dann im Einzelfall als unwirksam herausstellen.

Für die internationale Rechtsdurchsetzung sind die Punkte 4 und 5 der HCA Datenschutzerklärung relevant. Punkt 4 der Datenschutzerklärung legt fest, dass eine Weitergabe der Daten ins Ausland möglich ist. Es ist nicht klar, in welches Ausland diese Weitergabe erfolgt. Lediglich für App-Nutzungsdaten wird in Punkt 5 der Datenschutzerklärung erwähnt, dass diese an einen Server von Adobe in den USA übertragen und dort gespeichert werden.

Adobe nimmt an dem Zertifizierungsprozess über das Privacy Shield teil.³²¹ Dies bedeutet, dass die Weitergabe der App-Nutzungsdaten über das Privacy Shield prima facie legitimiert ist. Für etwaige Beschwerden über die Datenverarbeitung durch Adobe steht den betroffenen App-Nutzern der Weg der Schlichtung durch das Privacy Shield Panel offen. Eine entsprechende Notiz muss an das Privacy Shield Panel gesandt werden. Nur in diesem Moment dürfen nationale Datenschutzbehörden involviert sein. Sollte der Betroffene mit der Entscheidung des Privacy Shield Panels nicht einverstanden sein und diese gerichtlich überprüfen lassen wollen, kann er dies nur von U.S. Bezirksgerichten tun. Der damit verbundene Aufwand stellt ein erhebliches Hindernis für die Rechtsdurchsetzung dar.

IV. Zusammenfassung der Probleme im Rechtsschutz

Die Rechtsdurchsetzung in transnationalen Fällen von Datenschutzverletzungen ist, wie die auf nationaler Ebene, von Problemen geprägt.

Verschiedene Ansprüche und Rechtsdurchsetzungsmöglichkeiten haben spezifische juristische und praktische Probleme. Zum Beispiel ist für Schadensersatzansprüche der erforderliche Kausalitätsnachweis sowie der Nachweis eines Schadens so gut wie unmöglich. Auskunft- und Berichtigungsansprüche treffen auf praktische Hindernisse, wie z.B. Nichtbearbeitung oder unterschiedliche Bearbeitung durch die verantwortlichen Stellen oder die Schwierigkeit für Verbraucher, die verantwortliche Stelle ausfindig zu machen,

³¹⁸ Ausf. Wolf, *AGB-Recht Kommentar*, Wolf/Lindacher/Pfeiffer (Hrsg.), 6. Auflage 2013, C.H. Beck Verlag, Rn. 9 ff zu § 5 UKlaG.

³¹⁹ Walker, *Unterlassungsklagengesetz Nomos Kommentar*, Walker (Hrsg.), Nomos Verlag 2016 Rn. 17 zu § 1 UKlaG.

³²⁰ Micklitz, *Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen*, Rauscher/Krüger (Hrsg.), 4. Auflage 2013, C.H. Beck Verlag, Rn. 4 zu § 1 UKlaG.

³²¹ s. <<http://www.adobe.com/de/privacy/eudatatransfers.html>> (zuletzt abgerufen am 30.11.2016).

insbesondere im internationalen Kontext. Es mag nach juristischer Analyse der entsprechenden Vorschriften klar sein, welche Stelle verantwortlich i.S.d. BDSG ist; eine solche fundierte Analyse ist Verbrauchern jedoch kaum abzuverlangen.

Abgesehen von den spezifischen Problemen in der Rechtsdurchsetzung bestimmter Ansprüche, gibt es allgemeine Probleme, die die Wirksamkeit der Durchsetzung von Datenschutzregeln durch individuelle Verbraucher hemmt. Zunächst einmal sind gerichtliche Verfahren für Verbraucher teuer und aufwendig; oftmals wird deswegen von einer Rechtsdurchsetzung auf der individuellen Ebene abgesehen.³²² Außerdem ist für Verbraucher oft nicht ersichtlich, welche Rechte sie überhaupt haben oder gegen wen sie diese durchsetzen können. Das IT-Sicherheitsunternehmen Symantec hat in seinem State of Privacy Report 2015³²³ Teilnehmer aus Spanien, Deutschland, Frankreich, Niederlande, Italien, Dänemark und dem Vereinten Königreich zu Datenschutzproblemen befragt. Von den 7000 Befragten hatten insgesamt 60 % bereits Probleme mit möglichen Datenschutzrechtsverstößen. Die Studie fand heraus, dass bei den Teilnehmern allgemeine Verwirrung herrschte, wie in einem solchen Fall vorzugehen ist und wie man Hilfe bekommt. 69 % der deutschen Befragten würden ihre Daten auch gerne besser schützen, wissen aber nicht wie. Gleichzeitig haben 62 % der befragten deutschen Teilnehmer Sorge, dass ihre Daten nicht ausreichend geschützt sind. Aber nur 23 % von ihnen lesen die Datenschutzerklärungen. Zudem vertrauen nur 9 % der Deutschen darauf, dass ihre Daten bei Social Media-Anbietern ausreichend geschützt werden.

Im kollektiven Rechtsschutz sind die Rechtsdurchsetzungsmöglichkeiten durch Verbände mit der Ausweitung des § 1 UKlaG zwar verbessert worden. Allerdings leidet eine effektive Rechtsdurchsetzung an den begrenzten Ressourcen und der Unterausstattung der Verbraucherverbände und Aufsichtsbehörden, einem noch unkoordinierten Nebeneinander von Datenschutzbehörden und Verbraucherverbänden, sowie der zu niedrigen Berechnung und seltenen Verhängung von Bußgeldern, denen dadurch kaum Abschreckungswirkung zukommt. Der tatsächliche Mehrwert für die Rechtsdurchsetzung durch die Marktwächter als eine Art Zwischeninstanz ist bisher unklar.

Im transnationalen Bereich der Rechtsdurchsetzung gibt es im Grunde drei Hauptprobleme: Zuständigkeit, prozessuale Durchführung und materielles Datenschutzniveau in anderen Staaten. Auf europäischer Ebene gibt es einige Anstrengungen, insbesondere Zuständigkeiten und Prozesse auf einheitliche Regelungen zu stellen. Gleichwohl hat auch die Europäische Kommission erkannt, dass neben mangelnder Unterstützung der nationalen Behörden untereinander und Compliance der Unternehmen auch die Ermittlung von Verstößen schwierig ist und der Rechtsrahmen für bereits beendete, aber in ihren Effekten noch nachwirkende Rechtsverstöße noch fehlt. Davon abgesehen werden viele praktische

³²² So Klaus Müller in seiner Reaktion auf die UKlaG-Reform (dazu unten):

<<http://www.vzbv.de/pressemitteilung/erweitertes-verbandsklagerecht-datenschutzverstoesse-werden-sich-nicht-mehr-lohnen>> (zuletzt abgerufen am 30.11.16).

³²³ <<http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf>> (zuletzt abgerufen am 30.11.16).

Probleme beobachtet, wie der Facebook-Fall deutlich macht. Auskunftsverweigerung und Boykottierung von Ersuchen erschweren die Rechtsdurchsetzung erheblich.

Obschon Art. 3 DSGVO versucht, möglichst viele Aktivitäten in ihren Regelungsbereich zu bringen (ganz im Sinne des Google-Urteils des EuGH), gibt es noch immer unklare Verhältnisse in Bezug auf Zuständigkeitsregelungen. Oftmals ist für Verbraucher nicht ohne weiteres ersichtlich, wer die für die Datenverarbeitung verantwortliche Stelle ist.

Auf internationaler Ebene geht es insbesondere darum, sicherzustellen, dass Daten, die ins Ausland außerhalb der EU übermittelt werden, ähnlich wie nach europäischen Standards geschützt werden. Hier ist das Privacy Shield zwischen der EU und den U.S.A., auch wenn es die Defizite des für ungültig erklärten Safe-Harbor-Abkommens ändern sollte, durchaus auch in die Kritik geraten. Es gewährleistet aufgrund der zahlreichen Ausnahmen kein angemessenes Schutzniveau, womit gleichzeitig die Vermutung des angemessenen Datenschutzniveaus bei freiwilliger Teilnahme an Zertifizierung ins Leere läuft. Betroffene haben nur mangelnde Rechtsschutzmöglichkeiten vor U.S.-Gerichten. Schwer wiegt außerdem, dass Datenschutzbehörden u.a. kollektive Träger von der Teilnahme an Schlichtungsmechanismen ausgeschlossen sind.

F. Lösungsansätze: Datenschutz durch Recht und Technik

Dieses Papier basiert auf der Annahme, dass Maßnahmen von Recht und Technik ineinander verzahnt, die Herausforderungen des Datenschutzes im IoT verbessern können. Im letzten Teil dieses Papiers werden entsprechende Lösungsansätze und eventuelle Diskussionen um deren Effektivität dargestellt.

I. Rechtsänderungen

1. Vertragsrecht & AGB-Kontrolle

Die offensichtlichste Möglichkeit, Probleme des Datenschutzes im IoT zu lösen, ist die Änderung vertragsrechtlicher Vorschriften. In den Verträgen, die Verbraucher mit digitalen Dienstleistern im IoT abschließen, definieren sie die Basis für den Umgang mit ihren personenbezogenen Daten im IoT.

Wendehorst schlägt beispielsweise die Einführung von entsprechenden Tatbeständen in §§ 308, 309 BGB vor.³²⁴ Eine formularmäßige Einwilligung in Datennutzungen im IoT soll daher nur möglich sein, wenn es sich um personenbezogene Daten handelt, die durch die Nutzung einer erworbenen Sache oder Dienstleistung generiert werden. Außerdem soll durch ein Klauselverbot gem. § 309 BGB sichergestellt werden, dass die Einwilligungsvoraussetzungen nicht durch extensive Beschreibung von Geschäftszwecken ausgehöhlt werden.

³²⁴ Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016), S. 84-87.

Außerdem könnten Unternehmen künftig gezwungen sein, sich bei einer Datenverarbeitung oder -verwendung für eigene berechtigte Interessen i.S.d. § 28 BDSG gegenüber Verbraucher- oder Wirtschaftsverbänden für die dazu (nicht) durchgeführte Abwägung mit den Betroffeneninteressen zu rechtfertigen.³²⁵

Viele sprechen sich darüber hinaus für einen deliktischen Tatbestand aus, der als Schutzgesetz über § 823 II BGB zur Haftung für die eigenmächtige Verwertung personenbezogener Daten führt.³²⁶ Alternativ wird vorgeschlagen, de lege ferenda einen eigenen Tatbestand ähnlich den §§ 824, 825 BGB oder parallel zu § 812 I 1 Alt 2 und § 687 II BGB bei rechtsgrundloser bzw. eigenmächtiger Verwertung fremder Daten einzuführen.³²⁷

2. Drittbetroffenheit

Was das Sonderproblem der Drittbetroffenheit angeht, sollte eine rechtliche Einwilligungslösung gefunden werden. Am Beispiel des Smart Meter wurde beispielsweise vorgeschlagen, dass das starke Gebot des BVerfG durch hohe Anforderung an die Nutzung feingranularer Metering-Daten durch eine Zustimmungspflicht des Dritten, wie z.B.: Ehepartnern, umgesetzt werden soll.³²⁸ Dies soll durch eine Zustimmungspflicht Dritter, deren Daten regelmäßig miterhoben werden (z.B. Partner), erreicht werden.

3. Rechtsdurchsetzung

Die oben beschriebenen Probleme der Rechtsdurchsetzung müssten abgesehen von einer besseren Ausstattung der Datenschutzbehörden und Verbraucherverbände mit weiteren Kompetenzen einhergehen. Dazu gehören auch Mechanismen, die die Behörden zur Ausschöpfung ihres Ermessensspielraums in Bezug auf die Festsetzung und Höhe von Bußgeldern anhalten. Der finanzielle Rahmen von Bußgeldern sollte erhöht werden, um genügend Abschreckungswirkung zu erzeugen.

Um zu gewährleisten, dass die Aufsichts- und Regulierungsbehörden durch die Bereitstellung von Erkenntnissen des Marktwächters unterstützt werden, sollen die Marktwächter institutionell besser mit den Aufsichtsbehörden verzahnt werden.³²⁹ In diesem Zusammenhang fordert die Partei Die Grünen ein formelles Anrufungsrecht gegenüber der BaFin und anderen Aufsichtsbehörden. Bisher ist diese Benachrichtigung anders als beispielsweise beim betrieblichen Datenschutzbeauftragten keine gesetzliche normierte Pflicht. Auf das Gutachten des Sachverständigenrates 2016 „Verbraucherrecht 2.0“ und die Ausführungen zur Digitalagentur wird verwiesen.

³²⁵ Robak, „Neue Abmahnrisiken im Datenschutzrecht“, (2016), *Gewerblicher Rechtsschutz und Urheberrecht-Praxis im Immaterialgüter und Wettbewerbsrecht*, Heft 7, S. 139-141, S. 141.

³²⁶

<http://static1.1.sqspcdn.com/static/f/1376130/26847040/1455040340113/Faust+Digitale+Wirtschaft+-+Analoges+Recht+Gutachten+fur+den+71.+DJT.PDF?token=73St8IVwwV4tYnJQSVMQJmH3F8c%3D> (zuletzt abgerufen am 30.11.2016)

³²⁷ Wendehorst, „Die Digitalisierung und das BGB“, (2016), *Neue Juristische Wochenschrift*, Heft 36, S. 2609-2613, S. 2613.

³²⁸ http://oliver-krischer.eu/fileadmin/user_upload/gruene_btf_krischer/fotos/3_Greveler.pdf (zuletzt abgerufen am 30.11.2016).

³²⁹ <https://www.gruene-bundestag.de/presse/pressemitteilungen/2016/august/marktwaechter-gute-bilanz-mit-luft-nach-oben-25-08-2016.html> (zuletzt abgerufen am 30.11.2016).

Das größte Problem der Rechtsdurchsetzung im Datenschutz im IoT ist nach Ansicht der Verfasserinnen jedoch die internationale Gewährleistung eines hohen Schutzniveaus. Wir haben gesehen, dass die Übermittlung von Daten ins EU-Ausland mit rechtlichen Problemen überhäuft ist. Nunmehr ist auch schon das unlängst vereinbarte Privacy Shield kritisiert worden. Dies bringt nicht unerhebliche Rechtsunsicherheit sowohl für Unternehmen als auch Verbraucher mit sich.

Wegen der möglichen rechtlichen Konsequenzen einer Überprüfung des Privacy Shield durch den EuGH, ist eine Alternativlösung für internationale Datentransfers vorgeschlagen worden. Im Nachgang des Safe-Harbor-Urteils des EuGH sind viele Unternehmen, Facebook inbegriffen, für ihre internationalen Datentransfers auf eine Art Standardvertrag umgestiegen.³³⁰

Das Netzwerk Datenschutzexpertise hat einen solchen „Export-Import-Standardvertrag“ ausgearbeitet, der langfristig Rechtssicherheit versprechen soll.³³¹ Anlass, einen konkreten Formulierungsvorschlag auszuarbeiten, war nach Aussage von Weichert und Schuler die Tatsache, dass viele Unternehmen nach Kippen des „Safe-Harbor“-Abkommens beim Netzwerk Datenschutzexpertise anfragten, wie deren abstrakt formulierte Anforderungen an den vorgeschlagenen Export-Import-Vertrag zur Datenübertragung ins Drittausland ohne angemessenes Schutzniveau, konkret umgesetzt werden können. Der vom Netzwerk Datenschutzexpertise konkret ausgearbeitete Vorschlag baut auf den von der EU-Kommission anerkannten Standardvertragsklauseln auf. Diese wurden so weiterentwickelt, dass sie mit der EuGH-Rechtsprechung im Einklang stehen und genügen zudem sämtlichen künftig geltenden Regelungen der DSGVO.

Der „Export-Import-Standardvertrag“ zielt auf eine praktikable und unbürokratische Regelung ab, welche davon ausgeht, dass es – wie in den USA mit dem Patriot Act oder dem Foreign Intelligence Surveillance Act – mit europäischem Datenschutz kollidierende Vorschriften und Praktiken geben kann bzw. gibt. In Bezug auf den Inhalt des Vorschlags, unterscheidet dieser nicht zwischen Verträgen zur Datenübermittlung und zur Auftragsdatenverarbeitung (anders Standardvertragsklauseln der EU-Kommission). Der Standardvertrag enthält unveränderbare Bestandteile sowie veränderbare Angaben in den Anhängen, welche eine zentrale Bedeutung einnehmen, da die in den Anhängen enthaltenen Angaben bestimmt und rechtskonform sein müssen und mit der Realität in Einklang stehen. Durch eine „Notice-and-take-down“-Lösung, also der Kombination einer Informationspflicht des Datenimporteurs und einer Suspendierungspflicht des weiteren Datentransfers durch den Exporteur, wird versucht, das durch die grundrechtswidrigen Rahmenbedingungen bei der Datenverarbeitung im Empfängerstaat entstehende Defizit zu kompensieren.

³³⁰ <<https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu/>> (zuletzt abgerufen am 30.11.2016).

³³¹ Dieser Abschnitt basiert auf Schuler/Weichert, „Ein „Export-Import-Standardvertrag“ für den Drittauslands-Datentransfer“, (2016), *Datenschutz und Datensicherheit*, Heft 6, S. 386-390, S. 386-390.

Allerdings ist auch der Standardvertrag wiederum Gegenstand juristischer Prüfung. Max Schrems hat bei der irischen Datenschutzbehörde eine Beschwerde eingereicht, woraufhin die Behörde entschieden hat, eine Vorabentscheidungsverfahren beim EuGH einzuleiten.³³² Rechtssicherheit ist daher noch immer nicht in Sicht.

II. Datenschutz durch Technik

Wir haben gesehen, dass die momentane Rechtslage mit Problemen zu kämpfen hat, die die Gefahren für die Privatsphären durch PITs nicht neutralisiert. Im Folgenden wird diskutiert, inwiefern eine Normierung von Regelungen für die Technikgestaltung dazu beitragen kann, dass die Privatsphäre der Verbraucher besser geschützt ist, als bisher der Fall. Die Grundannahme für diese Diskussion ist, dass die Gefahren die von PITs für die Privatsphäre ausgehen, mit sog. Privacy-Enhancing-Technologies (PETs) entgegnet werden kann. So soll den Gefahren für die Privatsphäre durch technische Eingriffe entgegen gesetzt werden.

Besondere Bedeutung kommt PETs zum Schutz der Privatsphäre in transnationalen Umgebungen mit Cloud-Computing, globalen Datenflüssen und online Social Networks zu, weil technische Lösungen die Uniformität nationaler Rechtsordnungen in Bezug auf ihre Datenschutzregeln befördern können.³³³ Mit ihrer Relevanz für Cloud-Dienste und transnationale Datenflüsse, haben diese technischen Lösungen auch eine direkte Relevanz für das IoT und das Smart Home. Die Diskussionen im Teil F. sind nicht als abschließend zu verstehen. Eine Tabelle im Anhang

1. Konzeptionelle Grundlagen: Code as Law – Law as Code - PETs

Unter dem Einfluss von der Ethik des „Einbaus“ von Werten in technische Prozesse, basiert Regulierung durch Technik auf der Annahme, dass menschliche Werte, Normen und moralische Grundsätze Gegenständen und Prozessen verliehen und damit die Kommunikations- und Informationstechnik interpretiert werden können.³³⁴ Als Ausfluss aus dem generellen Value Sensitive Design (VSD) werden die sozialen und ethischen Verantwortlichkeiten von Wissenschaftlern, Investoren, Ingenieuren und Designern hervorgehoben, wenn diese Techniken erforschen, erfinden, konstruieren oder designen und damit eine „normative Technik“ kreieren.³³⁵ Einen solchen Ansatz der ethischen Technikgestaltung gibt es bereits im Umweltschutz in der Designpraxis des „Green by design“, wonach Produkte so designt werden, dass sie einen möglichst niedrigen umweltschädigen Effekt oder sog. Carbon Footprint haben.

Dieser Ansatz beruht auf Lessigs bahnbrechender Arbeit über die Architektur von Computer Code und seinen Fähigkeiten, menschliches Verhalten zu regulieren („Code as Law“ or „Law as Code“),³³⁶ ein Verständnis, das von vielen Autoren übernommen wurde. So sieht zum

³³² <http://www.europe-v-facebook.org/PA_MCs.pdf> (zuletzt abgerufen am 30.11.2016).

³³³ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 296; auch Hornung.

³³⁴ Dazu Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 260ff.

³³⁵ Dazu *ibid.*, S. 261.

³³⁶ Lessig, *Code and other laws of cyberspace Version 2.0*, (2. Auflage 2006, Basic Books Verlag),

Beispiel Spindler³³⁷ in seinem Gutachten im Auftrag des Sachverständigenrates einen wesentlichen Vorteil der Codierung von Recht in dem Selbstvollzug der technisch implementierten Norm; prominentes Beispiel dafür ist ein Mechanismus in der digitalen Kopie eines digitalen Inhaltes, der den digitalen Inhalt nach Ablauf der Leihzeit unbrauchbar macht.³³⁸ Durch diesen direkten Selbstvollzug wird Regulierung durch Technik allgemein hin als effizient betrachtet, weil Regeln mechanisch-konsistent angewandt werden.³³⁹

Im Sinne eines normativen Datenschutzes durch Technik zeigt Reidenberg,³⁴⁰ dass ein *lex informativa* Technik und technische Protokolle zur Regulierung von Datenschutz und Privatsphäre bereits einsetzt. Borking hat den Begriff Privacy-Enhancing Technologies (PETs) geprägt, unter dem er ein kohärentes System von Informations- und Kommunikationstechniken versteht, das die Privatsphäre durch die Eliminierung oder Reduktion bzw. Verhinderung von unnötiger oder unerwünschter Verarbeitung von personenbezogenen Daten schützt, ohne die Funktionalität des Systems zu verlieren.³⁴¹

2. Rechtliche Grundlagen: DSGVO und ePrivacy-Richtlinie

Technischer Privatsphärenschutz ist nach einiger Diskussion in der Fachwelt inzwischen in rechtlichen Vorgaben reflektiert und entsprechende Tools als eine grundlegende Voraussetzung für Privatsphärenschutz akzeptiert. Schon in der ePrivacy-Richtlinie³⁴² 2002/58/EG ist in Erwägungsgrund 46 die Notwendigkeit von Maßnahmen beschrieben,

„mit denen die Hersteller bestimmter Arten von Geräten, die für elektronische Kommunikationsdienste benutzt werden, verpflichtet werden, in ihren Produkten von vornherein Sicherheitsfunktionen vorzusehen, die den Schutz personenbezogener Daten und der Privatsphäre des Nutzers und Teilnehmers gewährleisten.“

Die ePrivacy Richtlinie 2002/58 wird im Moment überarbeitet. Eine neue Richtlinie soll gemeinsam mit der DSGVO 2018 in Kraft treten. Ein Kommissionspapier wird für Ende 2016 erwartet.³⁴³

³³⁷ Spindler, *Regulierung durch Technik*, Gutachten im Auftrag des Sachverständigenrates für Verbraucherfragen 2016.

³³⁸ Das sog. Digital Rights Management (DRM), welches Urheberrechte durchsetzt oder ausdehnt.

³³⁹ Z.B. Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 295-296; Yeung zeigt dagegen, dass höher Effizienz wegen unvermeidbaren technischen Versagens und unpräziser Standards nur schwer erreicht wird, s. Yeung, „Towards an Understanding of Regulation by Design, Regulating technologies“ in *Regulating technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Brownsword & Yeung (Hrsg.), (Hart, 2008), S. 79-107, S. 89ff.

³⁴⁰ Reidenberg, „Lex Informatica: The Formulation of Information Policy Rules through Technology“, (1997), *Texas Law Review*, S. 553-593; Reidenberg, *Privacy protection and the interdependence of law, technology and self-regulation*, Vortrag zum 20. Geburtstag des C. R. I. D., <<http://reidenberg.home.sprynet.com>> (zuletzt abgerufen am 30.11.2016).

³⁴¹ Z.B. Borking, *Laws, PETs and Other Technologies for Privacy Protection*.

³⁴² Richtlinie 2002/58/EG des europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201/37, 31.7.2002.

³⁴³ Die Konsultationen sind bereits abgeschlossen. <<https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive>> (zuletzt abgerufen am 30.11.2016).

In der DSGVO ist technischer Privatsphärenschutz nunmehr in Art 25 I, II und in Erwägungsgrund 78 festgeschrieben. Art. 25 DSGVO besagt:

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — , die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.“

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Erwägungsgrund 78 DSGVO normiert, dass es „zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen“ erforderlich ist,

„dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.“

Bemerkenswert ist, dass der ursprüngliche Kommissionsentwurf über den Inhalt der DSGVO hinaus ging: Gem. Art 23 III des Kommissionsvorschlages zur DSGVO sollte die Kommission ermächtigt werden, delegierte Rechtsakte im Hinblick auf die Implementierung von Privacy by Design zu erlassen, insbesondere was die Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen für ganze Sektoren und bestimmte

Erzeugnisse und Dienstleistungen betrifft.³⁴⁴ Diese Vorgaben sind in dem gegenwärtigen Wortlaut des Art. 25 DSGVO verwässert. Die Implementierung liegt in den Händen des „Verantwortlichen“ und ist nicht nur der Berücksichtigung des Stands der Technik unterworfen, sondern auch der Kosten, den Umständen der Datenverarbeitung und der Wahrscheinlichkeit und Schwere der Risiken für den Betroffenen. Art. 25 I DSGVO reflektiert eine durchaus gebotene Interessenabwägung, bietet aber gleichzeitig Exkulpationsmöglichkeiten für die Verantwortliche im Hinblick auf die Zumutbarkeit von technischen Maßnahmen auf dem „Stand der Technik“.

Jedenfalls sind die breit diskutierten Begriffe von Privacy by Design und Privacy by Default als Begriffe im Datenschutz etabliert.

3. Privacy by Design

Privacy by Design umfasst sowohl technische als auch organisatorische Lösungen. Diese werden im Folgenden, nach einem Abriss der Grundsätze von privacy by Design, dargestellt.

a. Grundsätze

Der kanadische Information and Privacy Officer ist ebenso wie das Unabhängige Landeszentrum für Datenschutz (UDL) in Schleswig-Holstein an der Spitze von Policy-Bestrebungen, Privacy by Design –Vorgaben für das Recht operabel zu machen.³⁴⁵

Die kanadische Behörde hat sieben Grundsätze für Privacy by Design aufgestellt.³⁴⁶

1. Proactive not Reactive; Preventative not Remedial

The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the Default Setting

We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

³⁴⁴ Brüssel, den 25.1.2012,

Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig.

³⁴⁵ <<https://www.datenschutzbeauftragter-online.de/datenschutz-ideengeschichte-privacy-by-design-teil-1/9929/>> (zuletzt abgerufen am 30.11.2016).

³⁴⁶ <<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>> (zuletzt abgerufen am 30.11.2016).

3. Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality — Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.

5. End-to-End Security — Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. Visibility and Transparency — Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy — Keep it User-Centric

Above all, Privacy by Design requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Auch der European Data Protection Officer erkennt an, dass Privacy by Design einen inhärenten Teil europäischer technischer Entwicklungen darstellen muss³⁴⁷ und auch in der Industrie setzt sich die Erkenntnis durch, dass Privatsphärenschutz auch einem Unternehmen zuträglich sein kann.³⁴⁸

³⁴⁷ European Data Protection Supervisor, *The EDPS and EU Research and Technological Development Policy paper*, (Brussels, 2008), S. 2
<https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf> (zuletzt abgerufen am 30.11.2016).

³⁴⁸ Z.B. <http://www8.hp.com/us/en/pdf/hp_fy11_gcr_privacy_tcm_245_1357687.pdf> (zuletzt abgerufen am 30.11.2016); für weitere Informationen s.

b. Parameter von Privacy by Design

Es gibt unterschiedliche technische Ansätze, wie Privacy by Design –Modelle umgesetzt werden können. Generell reichen die Möglichkeiten einer technischen Umsetzung von Privacy by Design von der Benutzung von Privatsphärenfiltern, eingebetteten Verschlüsselungstechniken, oder Algorithmen, die bestimmte personenbezogene Daten in anonymisierte Daten umwandeln oder Software, die bestimmte Funktionen nur aktiviert, wenn es Anhaltspunkte für die Notwendigkeit gibt.³⁴⁹

Beim nationalen IT-Gipfel in Saarbrücken hat die Plattform „Verbraucherschutz in der digitalen Welt“ ein Thesenpapier zu „Privacy by Design“ beschlossen, in dem es das Konzept aufgrund von Gesprächen in Fokusgruppen mit Unternehmen mit Thesen untermauert. In diesen Thesen wird deutlich, dass Privacy by Design verschiedene Komponenten umfasst.

Tabelle 3 – Prinzipien von Privacy by Design³⁵⁰

Prinzip	Umsetzung durch
Verfügbarkeit	• Maßnahmen der Redundanz • Fallback/Backup/Reparaturstrategien • Recht auf Datenportabilität (Art. 20 DSGVO)
Integrität	• Kontinuierliche Integritätsprüfung • Hashwert-Checks zum Erkennen von anormalen Veränderungen • Manipulationsgesichertes Logging
Vertraulichkeit	• Abschottungsmaßnahmen • Verschlüsselung (z.B. Ende-zu-Ende; Transport; Storage Privacy) • Anonymisierung & Pseudonymisierung (Klarnamenproblematik) • Nachvollziehbarkeit • Rollenbasiert beschränkte Zugriffsrechte • Sichere Anmeldeverfahren
Transparenz	• Planung, Nachvollziehbarkeit, Überprüfung, Bewertung • methodisches Projektmanagement • Dokumentation der IT-Infrastruktur • Dokumentation von Rollen und Rechtemanagement • Unterrichtung / Unterrichtungspflicht der Betroffenen • Information abgestimmt auf Benutzerhorizont (Detailgrad wählbar?) • Kontaktstelle für Auskunft
Datensparsamkeit und -vermeidung	• „attributbasierende Berechtigungsnachweise“ (ermöglicht pseudonyme Nutzung plattformübergreifend) • Strikte Umsetzung des Grundsatzes „Verbot mit Erlaubnisvorbehalt“; im Zweifel stets ausdrückliche Einwilligung des Nutzers erbitten

<http://www.informationweek.com/software/enterprise-applications/big-data-protecting-privacy-is-good-for-business/a/d-id/1320367> (zuletzt abgerufen am 30.11.2016).

³⁴⁹ Im Hinblick auf Body Scanners, menschliche Chipimplantate und CCTV-Kameras: Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 268ff.

³⁵⁰ <https://www.bmjbv.de/SharedDocs/Downloads/DE/Artikel/11162016_IT_Gipfel_Thesenpapier.pdf?__blob=publicationFile&v=1> (zuletzt abgerufen am 30.11.2016).

Nichtverkettbarkeit	• Maßnahmen, die die Zweckentfremdung erschweren • Löschung von Daten nach Funktionserfüllung • technische Vorkehrungen zur Einhaltung des Zweckbindungsgrundsatzes • Datenminimierung • Datenschutzfreundliche Voreinstellungen (privacy by default) • Verzicht auf Metadatenerhebung • feingranulare statt pauschale Einwilligungen • Maßnahmen, die die unnötige/nachträgliche Zusammenführung von Daten erschweren • Aufteilung auf getrennte Datenbanken • Getrennte Speicherung von identifizierenden Daten • Verwendung mehrerer Pseudonyme
Intervenierbarkeit	• Nutzbarkeit/Verständlichkeit von Konfigurationsoptionen und Beschwerdemanagement • Anwenderkontrolle über Daten zum Zweck des einzelfallbezogenen Datenzugriffs (einsehbar, änderbar, korrigierbar, sperrbar, löschar) • Recht auf Vergessenwerden (Art. 17 DS-GVO) • Überprüfung/Überprüfbarkeit automatisierter (Einzel-) Entscheidungen

In dieser Aufstellung wird deutlich, dass Privacy by Design ein holistisches Konzept ist, das viele Ausprägungen hat. Das Prinzip der Verfügbarkeit von Daten ist beispielsweise vornehmlich wettbewerbspolitisch und –rechtlich relevant; das Recht auf Datenportabilität soll die Möglichkeit für Verbraucher herstellen, ihre Daten von einem Dienstleister zum anderen zu „bringen“. Das Prinzip der Integrität befasst sich mit IT-Sicherheitsmaßnahmen.

Im Folgenden (unter F.II.4) soll es um die Prinzipien von Privacy by Design gehen, die vorrangig dem Privatsphärenschutz dienen. Dies sind die Prinzipien der Vertraulichkeit, Datensparsamkeit und der Nichtverkettbarkeit. Das Prinzip der Transparenz und das Prinzip der Intervenierbarkeit dienen, mit ihrer Ausrichtung auf die Rechtsdurchsetzung, ebenfalls dem Privatsphärenschutz. Dabei geht es insbesondere um die Rolle von Technik und technische Möglichkeiten, die Gefahren für die Privatsphäre, die von PITs ausgehen, mit der Hilfe von PETs einzudämmen.

c. Diskussion

Ein Vorteil eines gesetzlich verankerten Privacy by Design wäre der direkte Effekt auf die Hersteller. Da Strategien eines indirekten Einflusses auf Hersteller privatsphärenfreundliche Technik zu entwickeln, z.B. durch Druck von Seiten der Datennutzer oder der Kunden, als ineffizient erwiesen haben,³⁵¹ wäre eine direkte Regulierung der Anreize und Pflichten für Hersteller eine Möglichkeit direkt auf den Design-Prozess Einfluss zu nehmen und damit effektiver zu sein und auch mit technischem Fortschritt mitzuhalten. Das Ambient Agors Projekt der Fraunhofer Gesellschaft stellt in diesem Sinne fest: „privacy enhancement is better obtained by actively constructing a system exactly tailored to specific goals than by trying to defend ex-post a poor design against misuse or attacks.“³⁵² Dies soll außerdem kostensparend für Unternehmen sein, wenn Privacy by Design von vornherein in IT-Systeme

³⁵¹ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 4.

³⁵² S. 3 < <http://eprints.lse.ac.uk/33125/>> (zuletzt abgerufen am 30.11.2016).

integriert wird, anstelle von regulativen Reaktionen, die die nachträgliche Einbettung von technischen Maßnahmen erfordert.³⁵³

Kritikpunkte bzw. noch anzugehende Herausforderungen für die Umsetzung von Privacy by Design – Modellen, die im Folgenden besprochen werden, sind breit gefächert und umfassen Probleme von Adressaten, Innovationsfeindlichkeit, Verfassungswidrigkeit und Methodik.

Klitou zeigt, dass das Hauptproblem in existierenden Datenschutzrechtssystemen darin besteht, dass diese hauptsächlich auf die Datenbanken und Dienstleister anwendbar sind, die jedoch die PITs nicht herstellen.³⁵⁴ Außerdem bezieht sich der Umfang von Privacy by Design – Modellen wie er im europäischen und deutschen Rechtsrahmen erläutert ist, hauptsächlich auf Datensicherheit und nicht auf große, umfassende Strategien.³⁵⁵ In der DSGVO, zum Beispiel, sind die Adressaten der Pflichten die „Verantwortlichen“ i.S.d. Art. 4 Nr. 7 DSGVO, also solche Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Vereinbarung von personenbezogenen Daten entscheiden. Damit ist nicht der Produkthersteller eines Geräts oder einer für eine Dienstleistung benutzter oder in ein Produkt integrierte Software gemeint. Daher können die Vorteile von Privacy by Design nur dann entfalten, wenn klar ist, dass Privacy by Design zur Verpflichtung für die Hersteller wird.

Es gibt weitere Bedenken gegen Privacy by Design-Modelle, dass sie innovationsfeindlich sein könnten und Innovationen in technischen Entwicklungen hemmen. Allerdings verkennt eine solche Sichtweise, dass Privacy by Design nur sicherstellen soll, dass Privatsphäreneinstellungen bereits auf der ersten Entwicklungsstufe des Life-Cycles des Produkts eingebaut werden, anstelle eines nachträglichen Einbaus; so ist Privacy by Design kein Innovationshemmnis, sondern lediglich ein Antrieb zu gesteuerter technischer Entwicklung.³⁵⁶ Dieser Lifetime-Ansatzpunkt stellt sicher, dass Privatsphäreneinstellungen stärker, einfach und daher umsatzfähiger sind, und darüber hinaus schwerer zu umgehen und voll in das Produktsystem und seine Kernfunktion integriert sind (s. Grundsatz 3 der sieben Grundsätze des Privacy by Design).

In Kritik zu „Law as Code“ im Allgemeinen und Lessig's Arbeit im Konkreten bringt Schwartz vor, dass Privatschutzkontrolle den Effekt haben kann, dass Informationspraktiken verschleiert werden und dass somit nachteilige Entscheidungen für Individuen und die Gesellschaft getroffen werden.³⁵⁷ Verfassungsrechtliche Bedenken äußert Koops, der den Mangel parlamentarischer Kontrolle hervorhebt. Diesen verfassungsrechtlichen Bedenken muss entsprochen werden und Koops bietet einen Katalog von Kriterien an, den er auf

³⁵³ <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/> (zuletzt abgerufen am 30.11.2016).

³⁵⁴ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 256.

³⁵⁵ Ibid., S. 274.

³⁵⁶ So ibid., S. 264.

³⁵⁷ Schwartz, „Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices“, (2000), *Wisconsin Law Review*, S. 743-788, S. 760.

Grundlage der existierenden Literatur zur normativen Bewertung von technischen Lösungen entwickelt hat.³⁵⁸

Es wird außerdem zu Bedenken gegeben, dass in die Software eines „smarten“ Systems eine Definition von durchschnittlichem Verhalten aufgenommen wird, was zu Profilierung und Diskriminierung führen kann, wenn die subjektiven Vorstellungen derjenigen, die das System konfigurieren, in die Programmierung des Systems mit einfließen.³⁵⁹ In diesem Sinne kann es zu Verletzungen des allgemeinen Persönlichkeitsrechts kommen, wenn Personen versuchen, nicht durch abweichende Verhaltensweisen aufzufallen.³⁶⁰ Dies soll allerdings verhindert werden können, wenn selbstlernende Algorithmen verwendet werden.³⁶¹

Weiterhin muss methodisch in Betracht gezogen werden, dass es aufgrund der technischen Komplexität keine einheitliche, anerkannte Methode gibt, um rechtliche Normen in technische Befehle umzusetzen.³⁶² Ein anerkanntes Problem ist zum Beispiel die Flexibilität von menschlichen Interpretationen und dem Verstehen von natürlicher Sprache und dagegen die Starre von Maschinensprachen.³⁶³ Grimmelmann kritisiert daher Lessig's Ansatzpunkt von „code is law“ da Computer Software, die im Gegensatz zu menschlichen Entscheidungsmechanismen potentiell intransparent, unmöglich zu ignorieren und anfällig für plötzliches technisches Versagen sei, nicht mit physischer Architektur gleichgesetzt werden könne.³⁶⁴ Darüber hinaus wird eine Regulierung durch Technik wohl nur in Bereichen zu legitimieren sein, in denen Einigkeit über bestimmte Interpretationen oder Anwendungen herrscht.³⁶⁵

Diese methodischen Kritikpunkte müssen berücksichtigt werden, können allerdings teilweise widerlegt werden. Im Hinblick auf die Flexibilität von menschlichen Entscheidungen gegenüber maschinengesteuerten Entscheidungen besteht überwiegend Einigkeit darüber, dass eine Codierung von rechtlichen Normen jedenfalls dann möglich ist, wenn in einer Rechtsnorm eine klare Ja-Nein-Entscheidung, ähnlich wie einer technisch-binären 0-1-Entscheidung, implementiert ist und so eine eindeutige Entscheidung und Auflösung der

³⁵⁸ Kopps, „Criteria for Normative Technology – An essay on the acceptability of ‚code as law‘ in light of democratic and constitutional values“, in *TILT Law & Technology Working Paper Series 2007*, (Tilburg University, 2007), weitere Diskussion der verfassungsrechtlichen Dimension von Regulierung durch Technik: Kopps, *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes*, Brownsword & Yeung (Hrsg.), (Hart Pub Verlag, 2008), S. 157ff; Brownsword, *So what does the world need now?, Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes*, Brownsword & Yeung (Hrsg.), (Hart Pub Verlag, 2008), S. 23ff.

³⁵⁹ Roßnagel/Desoi/Hornung, „Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik - Am Beispiel der smarten Videoüberwachung“, (2012), *Zeitschrift für Datenschutz*, Heft 10, S.459-462, S. 460.

³⁶⁰ Ibid.

³⁶¹ Ibid.

³⁶² Guarda/Zannone, „Towards the development of privacy-aware systems“, (2009), *Information and Software Technology*, Vol. 51, Nr. 2, S. 337-350.

³⁶³ Grimmelmann, „Regulation by software“, (2005), *Yale Law Journal*, Vol 114, S. 1719-1758.

³⁶⁴ Ibid.

³⁶⁵ Yeung/Dixon-Woods, „Design-based regulation and patient safety: a regulatory studies perspective“, (2010), *Social Science Medicine*, Vol 71, Nr. 3, 502-509.

Rechtsnorm in binäre Logik ohne Spielräume möglich ist.³⁶⁶ Dies bedeutet auch, dass die Technikneutralität des Datenschutzrechts im Rahmen einer Regulierung durch Technik überdacht werden sollte. Privacy by Design – Lösungen müssen auf der einen Seite flexibel und damit umfassend sein und auf der anderen Seite die spezifischen Charakteristiken von verschiedenen PITs, Geräten und System beachten.³⁶⁷ Nur durch ein fundamentales Umdenken im Hinblick auf Technikneutralität lassen sich spezifischen Gefahrenpotentiale durch Privacy by Design - Lösungen effektiv und kontrolliert angehen.

4. PETs

Privacy-Enhancing Technologies (PETs) sind für Privacy by Design grundlegend. Sie sind IT-Maßnahmen, die die Privatsphäre durch die Eliminierung und Minimierung von personenbezogenen Daten schützen und dadurch unzweckmäßige und ungewollte Ansammlung und Verarbeitung von personenbezogenen Daten verhindern, ohne dabei die Funktionalität des IT-Systems einzuschränken.³⁶⁸ PETs umfassen beispielsweise Verschlüsselungs-, kryptographische, Pseudonomisierungs- und Anonymisierungssoftware und –techniken, sowie Firewalls.³⁶⁹ PETs sind nicht als Substitute, sondern Komplementäre zu anderen Instrumenten zu verstehen. Insbesondere ergeben sich Synergieeffekte mit rechtlichen Vorgaben, die durch PETs in technische Spezifikationen umgewandelt werden.³⁷⁰ Im Rahmen von Privacy by Design sind sie technische Maßnahmen, die bereits in die Produktion und Herstellung von privatsphäreninvasiven Geräten berücksichtigt werden.

Zahlreiche Projekte im europäischen Rechtsraum haben das Ziel, privatsphärenschützende und andere Erwägungen in technische Entwicklungen zu integrieren. Das PISA (Privacy Incorporated Software Agents) Projekt, zum Beispiel, unterstützt mithilfe des Fünften European Framework Programms,³⁷¹ hat Privacy-Enhancing Technologies (PETs) entwickelt, welche die Privatsphäre von Personen schützen, wenn diese Dienstleistungen von Software Agenten benutzen.³⁷²

In diesem Papier werden IT-Maßnahmen des technischen Identitätsmanagements, der Anonymisierung, Pseudonymisierung, Löschung, der Do-Not-Track-Mechanismus, sowie die sog. Sticky Policies beispielhaft für PETs im Allgemeinen diskutiert. Die Darstellung ist nicht als abschließend zu verstehen.

³⁶⁶ Spindler, *Regulierung durch Technik*, Gutachten im Auftrag des Sachverständigenrates für Verbraucherfragen 2016, S. 2.

³⁶⁷ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 301-303.

³⁶⁸ Van Blarckom/Borking/Ork (Hrsg.), *Handbook of Privacy and Privacy-Enhancing technologies – The case of Intelligent Software Agents*, (PISA Consortium, 2003), S. 3, 33.

³⁶⁹ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 270.

³⁷⁰ Van Blarckom/Borking/Ork (Hrsg.), *Handbook of Privacy and Privacy-Enhancing technologies – The case of Intelligent Software Agents*, (PISA Consortium, 2003).

³⁷¹ <[http://www.2020-horizon.com/PISA-Privacy-Incorporated-Software-Agent-Building-a-privacy-guardian-for-the-electronic-age-\(PISA\)-s50085.html](http://www.2020-horizon.com/PISA-Privacy-Incorporated-Software-Agent-Building-a-privacy-guardian-for-the-electronic-age-(PISA)-s50085.html)> (zuletzt abgerufen am 30.11.2016).

³⁷² Dazu Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 266f., andere Projekte sind DISCREET, PRIME and PrivacyOS.

a. Technisches Identitätsmanagement

Datenschutzförderndes Identitätsmanagement bezieht sich auf die Möglichkeit, über die Verwendung seiner eigenen Identitätsinformationen selbst entscheiden bzw. verschiedene Identitäten zu unterscheiden und zwischen diesen auswählen zu können.³⁷³ Da es mehrere Identitäten gibt,³⁷⁴ gehört die Wahlmöglichkeit zwischen verschiedenen Identitäten zum Grundkonzept des Identity Management.³⁷⁵

Ein System des „Identity Protectors“ ist die Basis für PETs und ein erstes System wurde 1995 von den niederländischen und kanadischen Datenschutzbehörden vorgestellt.³⁷⁶ Ein Identity Protector schützt im Grunde die individuelle, wahre Identität eines Nutzers in allen datenverarbeitenden Prozessen in einem IT-System.³⁷⁷ Dies geschieht durch die Konvertierung der Identität in eine oder mehrere Pseudo-Identitäten für das IT-System.

Identitätsmanagement wurde prototypisch im Projekt PRIME (Privacy and Identity Management for Europe) realisiert.³⁷⁸ Es umschreibt die Gesamtheit von Authentifizierung, Autorisierung und Protokollierung.³⁷⁹ Bei der grundlegenden Authentifizierung wird durch die Eingabe einer Benutzerkennung und eines geheimen Passworts oder ergänzende biometrische Verfahren der Zugang zu einem Rechnersystem kontrolliert. Autorisierung und Zugriffskontrolle erfolgt i.d.R. durch Rollenzuweisung von Zugangskennung. Protokollierung ermöglicht den Nutzern ein späteres Nachvollziehen der Informationsfreigabe.

Technisches Identitätsmanagement erfasst mehrere Probleme des Datenschutzes. Durch Wahlmöglichkeiten zwischen verschiedenen Identitäten und Transparenz durch Protokollierung hat der Betroffene Kontrolle und Wissen über die Verwendung seiner personenbezogenen Daten. Die kontextspezifische Verwendung von Pseudonymen ermöglicht Datensparsamkeit. Darüber hinaus könnten auch intransparente Datenschutzerklärungen vermieden werden, wenn Policies mit Vorgaben der Nutzer automatisch abgeglichen werden und Nutzer bei Abweichungen gewarnt werden.

b. Löschung, Anonymisierung und Pseudonymisierung

Eine prominente Methode, Um den Grundsatz der Vertraulichkeit in Privacy by Design umzusetzen, ist durch die automatische, durch eingebaute Mechanismen vorgenommene Anonymisierung und Pseudonymisierung von personenbezogenen Daten.

Anonymität ist nach dem ISO standardisiert. Nach dem ISO99 stellt Anonymisierung sicher, „that a user may use a resource or service without disclosing the user’s identity. ... Anonymity is not intended to protect the subject identity ... Anonymity requires that other

³⁷³ S. 2, <<https://www.datenschutz-mv.de/datenschutz/publikationen/informat/idmgt/id-mgt.pdf>> (zuletzt abgerufen am 30.11.2016).

³⁷⁴ <http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf> (zuletzt abgerufen am 30.11.2016).

³⁷⁵ S. 5-7, <<https://www.datenschutz-mv.de/datenschutz/publikationen/informat/idmgt/id-mgt.pdf>> (zuletzt abgerufen am 30.11.2016).

³⁷⁶ Hes/Borking, *Privacy-enhancing Technologies: The path to anonymity*, (Registrierkammer, 1998).

³⁷⁷ Ibid., S 13.

³⁷⁸ <<http://www.fp7-prime.eu/project>> (zuletzt abgerufen am 30.11.2016).

³⁷⁹ S. 3, <<https://www.datenschutz-mv.de/datenschutz/publikationen/informat/idmgt/id-mgt.pdf>> (zuletzt abgerufen am 30.11.2016).

users or subjects are unable to determine the identity of a user bound to a subject or operation.” Pfitzmann & Hansen definieren Anonymität etwas weiter, so dass es jegliche Personen (nicht nur Nutzer) umfasst: “Anonymity of a subject means that the subject is not identifiable within the anonymity set”.³⁸⁰

In der DSGVO und dem BDSG spielt Anonymität im Rahmen des Geltungsbereiches eine Rolle. Wenn der Betroffene nicht mehr bestimmbar i.S.d. § 3 VI, I BDSG ist, ist das BDSG nicht anwendbar. § 3a BDSG erwähnt Anonymisierung und Pseudonymisierung als Regelbeispiele für die Möglichkeiten zur Erreichung der Ziele von Datenvermeidung und Datensparsamkeit.³⁸¹ Anonymisierung und Pseudonymisierung stehen in einem Stufenverhältnis zueinander, basierend auf dem Risiko der tatsächlichen oder faktischen Re-Identifizierung, welche bei der Pseudonymisierung, nicht aber bei der Anonymisierung noch möglich ist. Anerkannt ist gleichzeitig, dass eine optimale Schutzwirkung nur über Anonymisierung erreichbar ist.

Anonymisierung und Pseudonymisierung haben auch Wechselwirkungen mit der automatischen Löschung von Daten. Sobald der Personenbezug eines Datums nicht mehr erforderlich ist, soll die verantwortliche Stelle also zunächst die Daten löschen. Wenn Löschung nicht mehr in Betracht kommt, soll sie das Datum anonymisieren.³⁸² Pseudonymisierung genügt nur dann den gesetzlichen Vorgaben, wenn andere legitime Zwecke dies erforderlich machen. Heutzutage sind sowohl Anonymisierung und Pseudonymisierung technisch ohne unverhältnismäßigen Aufwand realisierbar, so dass dies als Bezugspunkt nicht mehr in Betracht kommt, sondern vielmehr die Frage, ob die verantwortliche Stelle zur Zweckerreichung auf die Nutzung personenbezogener Daten im Klardatum angewiesen ist.³⁸³ Das Stufenverhältnis Löschung – Anonymisierung – Pseudonymisierung wird den Privacy by Design Grundsätzen von Datensparsamkeit und Datenminimierung gerecht und unterstützt außerdem die Durchsetzung des Rechts auf Löschung von Daten.

Ein praktisches Beispiel für automatische Anonymisierung und Pseudonymisierung von „smarter“ Videoüberwachung ist zum Beispiel der „CamInSens“ zur Erkennung von Gefahren im öffentlichen Raum, welcher im Rahmen des Programms "Forschung für die zivile

³⁸⁰ <http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf> (zuletzt abgerufen am 30.11.2016).

³⁸⁰ Dazu: Schulz, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2014, C.H. Beck Verlag, Rn 70ff. zu § 3a BDSG.

³⁸⁰ Ibid., Rn. 73 zu § 3a BDSG.

³⁸⁰ Ibid., Rn 92 zu § 3a BDSG.

³⁸⁰ <<http://www.caminsens.org/index.html>> (zuletzt abgerufen am 30.11.2016).

³⁸⁰ <http://www.caminsens.org/PDF/CamInSens_Rechtliche_Aspekte.pdf> (zuletzt abgerufen am 30.11.2016); auch: Roßnagel/Desoi/Hornung, „Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik - Am Beispiel der smarten Videoüberwachung“, (2012), *Zeitschrift für Datenschutz*, Heft 10, S.459-462, S. 459 f.;

<http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf> (zuletzt abgerufen am 30.11.2016).

³⁸¹ Dazu: Schulz, *Beck'scher Online-Kommentar Datenschutzrecht*, Wolff/Brink (Hrsg.), 17. Edition 2014, C.H. Beck Verlag, Rn 70ff. zu § 3a BDSG.

³⁸² Ibid., Rn. 73 zu § 3a BDSG.

³⁸³ Ibid., Rn 92 zu § 3a BDSG.

Sicherheit" durch das Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der High-Tech-Strategie gefördert wurde.³⁸⁴ Die Universität Kassel hat im Rahmen der Projektgruppe verfassungsverträgliche Technikgestaltung ein Stufen-Modell entwickelt, welches die Eingriffe in das Recht auf informationelle Selbstbestimmung je nach Verdachtsstufe automatisch anpasst und damit den Eingriff in das allgemeine Persönlichkeitsrecht möglichst gering hält.³⁸⁵

- Auf der 1. Stufe werden Personen anonymisiert oder pseudonymisiert dargestellt. Gezielte Personenverfolgung erfolgt entweder automatisch oder durch Beobachter, wenn ein hinreichender Gefahrenverdacht (definiert) vorliegt.
- Auf der 2. Stufe werden auf dieser Grundlage identifizierte Personen, die sich auffällig verhalten gezielt mit Zoomfunktion überwacht, ohne dass ihre biometrischen Merkmale erfasst werden. Wenn automatisch oder durch den Beobachter eine konkrete unmittelbare Gefahr besteht, kann in die Personenerkennung übergegangen werden.
- Auf der 3. Stufe werden Personen anhand biometrischer Daten identifiziert und Videobilder so aufgenommen und gespeichert, dass das Geschehen später zu Beweis Zwecken nachvollzogen werden kann.

Diese Beispiele verdeutlichen das Zusammenspiel von Anonymisierung und Pseudonymisierung. Pseudonymisierung erlaubt hier die gezielte Aufdeckung von Anonymität bei Vorliegen eines entsprechenden Strafverfolgungsinteresses. Die beiden Mechanismen können also für eine ausgewogene Interessendurchsetzung fördern: Auf der einen Seite tragen sie dem Interesse der Betroffenen Rechnung, sich möglichst anonym zu bewegen; auf der anderen Seite erlauben sie den Strafverfolgungsbehörden bei Vorliegen einer Gefahr (hier kommt es natürlich auch auf die Definition von „Gefahr“ an) im öffentlichen Interesse eine Aufdeckung der Anonymität des Verdächtigen.

Ein durch das 7. Framework Programme unterstütztes Projekt hat 2015 ein Handbuch herausgegeben,³⁸⁶ das eine Übersicht über geförderte Projekte bietet. Die geförderten Projekte reichen von IT-Sicherheit, über Integrität von IT-Systemen, privatsphären- und datenschützende und technisch sichere Clouds, personalisierte und zentralisierte Authentifikationssysteme,

c. DNT-Mechanismus

Der Do-Not-Track (DNT) Mechanismus ist ein Maßnahme, durch welche ein Verbraucher seinem Vertragspartner signalisiert, dass seine Daten und Handlungen nicht verfolgt werden. Dazu wurde ein http-Header-Feld entwickelt, welches einer Web Applikation signalisiert, dass ihr Tracking oder Cross-Seiten-Tracking ausgeschaltet werden soll: 1 für opt-out; 0 für opt-in und NULL (also keine Sendung eines Befehls) für das Vorliegen keiner Präferenzen.

³⁸⁴ <<http://www.caminsens.org/index.html>> (zuletzt abgerufen am 30.11.2016).

³⁸⁵ <http://www.caminsens.org/PDF/CamInSens_Rechtliche_Aspekte.pdf> (zuletzt abgerufen am 30.11.2016); auch: Roßnagel/Desoi/Hornung, „Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik - Am Beispiel der smarten Videoüberwachung“, (2012), *Zeitschrift für Datenschutz*, Heft 10, S.459-462, S. 459 f.

³⁸⁶ Gramatica/Massacci, *FP7 ICT Trust & Security Projects Handbook*, (University of Trento, 2015).

Wenn Verbraucher das Do-Not-Track-Setting in ihrem Browser durch opt-out aktivieren, senden sie diesen http-Header an Vertragspartner und Dritte.

Schon 2007 gab es erste Initiativen in den U.S.A., DNT für Behavioural Advertisement durchzusetzen.³⁸⁷ Dabei wurde die Federal Trade Commission (FTC) angehalten, eine Do-Not-Track-Liste von Unternehmen zu erstellen, die einen dauerhaften Identifizierungsmechanismus verwenden, solchen Unternehmen entsprechende Informationspflichten aufzuerlegen, sowie unabhängiges Auditing der Unternehmenscompliance zu gewährleisten. Die FTC kam diesem Begehren nach und erließ 2010 außerdem einen Preliminary Staff Report,³⁸⁸ in dem sie vorschlagen, Verbrauchern einen DNT-Mechanismus zur Verfügung zu stellen, der es ihnen ermöglicht zu kontrollieren und zu wählen, ob und welche Webseiten Informationen über ihre Internetaktivitäten sammeln und für personalisierte Werbung verwenden dürfen. In 2015 hat das W3C (World Wide Web Consortium) die Zertifizierung eines standardisierten DNT-Mechanismus' angekündigt.³⁸⁹

Der relativ einfachen technischen Gestaltung des DNT-Mechanismus' steht das Fehlen einer weiteren Implementierung eines DNT-Mechanismus entgegen. Eine solche ist bisher am mangelnden Konsens zwischen Privatsphärenschränkern und der Industrie gescheitert. Nur einige wenige Unternehmen implementieren einen DNT. Darüber hinaus befolgen viele der Unternehmen, die DNT anbieten, die Präferenzen der Verbraucher nicht; die FTC hat einen Antrag des Consumer Watchdog bezüglich einer Verpflichtung für „edge providers“ wie Google, Facebook, Netflix, LinkedIn, und Youtube allerdings abgelehnt.³⁹⁰ Umstritten ist außerdem das default-setting, für Fälle in denen Verbraucher keine Präferenz angegeben haben.³⁹¹

d. Sticky Policies

Die sog. Sticky Policies wurden entwickelt, um den Transfer von Daten sicherer und nachvollziehbarer zu gestalten. Im Grunde geht es dabei um die Wahl von Privacy Policies durch Nutzer, welche dann automatisch weiterverarbeitet werden, dem Datenverarbeitungsprozess sozusagen die ganze Zeit ‚anhaften‘. Eine Voraussetzung dafür sind maschinenlesbare Policies.³⁹²

Sticky Policies sind deswegen für den Datenschutz durch Technik interessant, weil sie an die Einwilligung und Präferenzen des betroffenen Nutzers anknüpfen und diese technisch

³⁸⁷ <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>> (zuletzt abgerufen am 30.11.2016).

³⁸⁸ <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>> (zuletzt abgerufen am 30.11.2016).

³⁸⁹ <<https://lists.w3.org/Archives/Public/public-tracking/2015Jul/0000.html>> (zuletzt abgerufen am 30.11.2016).

³⁹⁰ <https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1266A1.pdf> (zuletzt abgerufen am 30.11.2016).

³⁹¹ Z.B. <<https://techcrunch.com/2015/04/03/microsoft-disables-do-not-track-as-the-default-setting-in-internet-explorer/>> (zuletzt abgerufen am 30.11.2016).

³⁹² Pearson/Mont, „Sticky Policies: An Approach for Managing Privacy across Multiple Parties“, (2011), *IEEE Computer Magazine*, Vol. 44, Nr. 9, S. 60–67, S.65-66.

unterstützen können.³⁹³ Beispielsweise kann ein Webbrowser Plug-in den Nutzern helfen, ihre Einwilligung kundbar zu machen und Präferenzen zu identifizieren, z.B. durch opt-in oder opt-out. Das Datenarchiv speichert Informationen über die personenbezogenen Daten, sowie Informationen über deren Speicherort und über die Identität von Empfängern der Daten; es wird im Falle jeder Änderung von Einwilligung und Präferenzen automatisch aktualisiert. Der Zugang zu Daten wird automatisch auf Basis der Einwilligung und Präferenzen kontrolliert und auch außerhalb einer Organisation technisch durchgesetzt. Durch einen Audit wird der Datenfluss innerhalb und außerhalb der Organisation getrackt. Schlussendlich gibt es ein offline compliance checking and risk assurance, durch welches die Administratoren der Organisation sicherstellen, dass Risiken und compliance identifiziert werden. Hier werden die personenbezogenen Daten und ihr Lebenszyklus bei der verantwortlichen Stelle stets mit ausgewertet. Obschon Verschlüsselung ein integraler Bestandteil des Datenschutzes durch Sticky Policies ist, muss der stets bestehende Missbrauchsgefahr (die sich daraus ergibt, dass jeder Nutzer mit autorisiertem Zugang zu den Daten diese an einen anderen nicht-autorisierten Nutzer weiterleiten kann) mit solchen Audits begegnet werden.³⁹⁴

Im Rahmen des EnCoRe Projekts wurden beispielsweise solche Sticky Policies entwickelt.³⁹⁵ In dem EnCoRe-System kann ein Nutzer die Granularität der vorher definierten Datenschutzpolices sowie andere Präferenzen wie z.B. in Bezug auf Benachrichtigungen, Lösungszeitpunkt, vereinbarte Zwecke und Zugriffsberechtigte auswählen. Darüber hinaus wählt er sog. Trusted Authorities aus, die die Schlüssel zur Entschlüsselung der Daten haben und auf Anfrage herausgeben. Das System kreiert aus den Präferenzen und deren Assoziation zu bestimmten Daten die Sticky Policies. Diese werden bei jeder Sendung der Daten durch das System mitgesandt. Auf diesem Wege soll ein grenzüberschreitendes, nachvollziehbares Datenmanagement ermöglicht werden.

III. Privacy by Default

Privacy by Default bezieht sich auf datenschutzfreundliche Grundeinstellungen eines Produkts oder Dienstleistungen. Im Gegensatz zum Privacy by Design ist Privacy by Default nicht in die Gestaltung des Produkts oder der Dienstleistung durch die Hersteller integriert, sondern beschreibt eine technische oder organisatorische Grundeinstellung, die darauf ausgelegt ist, Datenschutzgrundsätze wie Datenminimierung wirksam umzusetzen und Betroffenenrechte zu schützen, s. Art. 25 DSGVO. Art. 25 DSGVO bestimmt Privacy by Default als eine allgemeine Pflicht des für die Datenverarbeitung Verantwortlichen. Die Pflicht zu datenschutzfreundlichen Grundeinstellungen richtet sich also nicht an Hersteller, sondern die Erbringer einer Leistung, die theoretisch die Wahl haben zwischen datenschutzfreundlicheren und datenschutzschädlicheren Voreinstellungen.

Privacy by Default kann, gemäß Prinzip 2 der Privacy by Design – Grundsätze, verstanden werden als eine Voreinstellung, die sicherstellt, dass personenbezogene Daten in IT-

³⁹³ Zu diesen einzelnen Komponenten *ibid*.

³⁹⁴ <<http://doc.utwente.nl/65155/>> (zuletzt abgerufen am 30.11.2016).

³⁹⁵ Pearson/Mont, "Sticky Policies: An Approach for Managing Privacy across Multiple Parties", (2011), IEEE Computer Magazine, Vol. 44, Nr. 9, S. 60–67, S.60 ff.

Systemen oder Geschäftsmodellen automatisch geschützt werden, ohne dass der Betroffene Maßnahmen zum Schutz seiner Privatsphäre ergreifen muss. Dies wird i.d.R. durch Opt-outs geschehen.

IV. Zertifizierung, Audit, Datenschutzsiegel

Um Privacy by Design – und Privacy by Default - Lösungen zu implementieren, müssen Durchsetzungs- und Monitoring-Mechanismen geschaffen werden, die die Effektivität und Gemeinverträglichkeit algorithmischer Entscheidungen regelmäßig überprüfen. Klitou schlägt vor, Zertifizierung, Privacy Audits, Konformitätsdeklarationen, Rückrufaktionen und Sanktionen zu etablieren.³⁹⁶ Dies bedeutet, dass Hersteller von Produkten und Anbieter von Dienstleistungen für die Einhaltung der ihnen obliegenden Privacy by Design – Verpflichtungen haften müssen.

1. Vertragsrechtliche Lösung

Dies kann zum einen durch die Einführung von Privacy by Design und Privacy by Default als Kriterien für Vertragskonformität erfolgen.³⁹⁷ Es kann auch erwogen werden, für Fälle, in denen ein Produzent oder Anbieter nicht einer bestimmten Gerichtsbarkeit unterliegt, eine Produzentenhaftung einzuführen. Anspruchsgegner sollten dabei das Recht haben, sich durch den Einwand des Missbrauchs von Seiten des Nutzers oder der mangelnden Kausalität zwischen Datenschutzrechtsverletzung und Privacy by Design und Privacy by Default – Anwendungen von der Haftung zu befreien.³⁹⁸

2. Marktorientierte & aufsichtsrechtliche Lösung

Teil eines marktorientierten Lösungsansatzes wäre dagegen die Möglichkeit von Datenschutzzertifizierungen. Die DSGVO führt in Artikel 42 die Förderung von Zertifizierung ein. Zertifizierungsstellen sollen dazu dienen, sicherzustellen, dass die Bestimmungen der DSGVO eingehalten werden, Art. 42 I DSGVO.

a. Modelle und Vorteile

Generell zielt Zertifizierung auf die Schaffung von Marktanreizen durch Selbstregulierung. Marktmechanismen (z.B. Werbung mit dem Zertifizierungssiegel), Transparenz, interne Lernprozesse und Wettbewerb sollen zu einer Verbesserung des Datenschutzes führen.³⁹⁹ Die diskutierten Angebote auf dem Zertifizierungsmarkt beziehen sich auf unterschiedliche Gegenstände: Datensicherheit, Einhaltung von Verfahren (Compliance i.e.S., Datenschutzausbildung, produktbezogener Datenschutz und materielles Datenschutzniveau), die teilweise in Kombination, teilweise aber auch unter dem

³⁹⁶ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 307ff..

³⁹⁷ So Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016)

³⁹⁸ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 308.

³⁹⁹ Hornung/Hartl, „Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit“, (2014), *Zeitschrift für Datenschutz*, Heft 5, S. 219-225, S. 220.

umfassenden oder unspezifizierten Dachbegriff „Datenschutz“ angeboten werden.⁴⁰⁰ Zertifizierung könnte sich zum Beispiel auf eine verbindliche aufsichtsrechtlich organisierte Klassifizierung von IoT-Produkten beziehen.⁴⁰¹ So könnten eingebaute Sicherheitsvorkehrungen, Designcharakteristika und technische Spezifizierungen in „privacy safe“, „privacy compliant“ oder „privacy friendly“ eingeteilt werden.⁴⁰² Zum anderen könnte eine unabhängige, unternehmensexterne behördliche und verpflichtende Zertifizierung auch konkret Privacy by Design- und Privacy by Default - Lösungen unterstützen. In einem ersten Schritt müsste sichergestellt werden, dass Unternehmen und Hersteller eine „Declaration of Conformity“ abgeben. Auf der zweiten Stufe, überprüfen unabhängige Privacy Auditors die Produkte und Dienstleistungen auf die Umsetzungen von Privacy by Design – Standards. Drittens sollten zufällig ausgeführte Überprüfungen stattfinden.⁴⁰³

Der sächsische Datenschutzbeauftragte hat beispielsweise eine „web analytics“ Technik, den sog. E-Tracker, zertifiziert. Der E-Tracker⁴⁰⁴ sammelt und speichert Daten (Anzahl und Häufigkeiten von besuchen, Nutzung und Klickverhalten, Herkunft) zu Marketing- und Optimierungszwecken und erstellt pseudonyme Nutzungsprofile, die nur mit gesondert erteilter Zustimmung des Betroffenen genutzt werden.

In Deutschland werden Zertifizierungen angesichts der knappen Ressourcen der Datenschutzaufsichtsbehörden positiv angesehen, weil sie datenschutzrechtliche Prüfungen beschleunigen oder gar entfallen lassen können.⁴⁰⁵ Außerdem bietet die Datenschutzgrundverordnung die legislativen Rahmenbedingungen, nach denen die Datenschutz-Aufsichtsbehörden in erster Linie die Zertifizierungsvorgaben sowie die zertifizierenden Stellen überwachen, die Prüfarbeit selbst aber an die zertifizierenden Stellen und die datenverarbeitenden Unternehmen übergeben werden kann. Allerdings stellen sich hier wiederum Probleme, die bei der Selbstregulierung generell auftauchen (dazu unten, Kritik).

Generell werden Zertifizierungsmechanismen als positiv bewertet, da sie zumindest in Kombination mit „geeigneten Garantien“ (beispielsweise i.S.d. Art. 39 I a DSGVO) für die Durchsetzung von Datenschutzstandards bei einer außereuropäischen Stelle ein angemessenes Datenschutz-Niveau gewährleisten können.⁴⁰⁶ Je nach weiterem Verlauf der Diskussionen um „Safe Harbor“, das Schutzniveau des EU-US-Privacy Shield und die

⁴⁰⁰ Feik/von Lewinski, „Der Markt für Datenschutz-Zertifizierungen - Eine Übersicht“, (2014), *Zeitschrift für Datenschutz*, Heft 2, S. 59-62, S. 59 f.

⁴⁰¹ So Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, (Studie im Auftrag des Sachverständigenrats für Verbraucherfragen 2016)

⁴⁰² Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 309.

⁴⁰³ So ibid.; Zur Vermutungswirkung anerkannten Verhaltenskodizes: Spindler/Thorun/Wittmann, *Rechtsdurchsetzung im Verbraucherdatenschutz-Bestandsaufnahme und Handlungsempfehlungen*, (Friedrich Ebert Stiftung, 2016).

⁴⁰⁴ Informationen zum E-racker auf: <www.etracker.com> (zuletzt abgerufen am 30.11.2016).

⁴⁰⁵ Feik/von Lewinski, „Der Markt für Datenschutz-Zertifizierungen - Eine Übersicht“, (2014), *Zeitschrift für Datenschutz*, Heft 2, S. 59-62, S. 59f.

⁴⁰⁶ Dazu Kraska, „Datenschutz-zertifizierungen in der EU-Datenschutzgrundverordnung“, (2016), *Zeitschrift für Datenschutz*, Heft 4, S. 153-154, S. 153f.

Zukunft von EU-Standardverträgen könnte dies mittelfristig ein weiteres Instrument darstellen, personenbezogene Daten an außereuropäische Stellen zu übermitteln.

b. Kritik & Lösungsansätze

Problematisch an Zertifizierungsmechanismen ist allerdings, dass es noch keinen allgemeinen Zertifizierungsstandard gibt und sich die vorhandenen Zertifizierungsangebote auf Datensicherheit und technisch-organisatorische Maßnahmen beziehen, während die Frage der Rechtmäßigkeit von Datenerhebungen und –verarbeitungen oder flankierende Rechtsprobleme im AGB-Recht oder Verbraucherschutzaspekte, wie zum Beispiel das Kopplungsverbot, nur eine nachrangige Rolle spielen.⁴⁰⁷ Außerdem gibt es wegen der mangelnden Meldepflicht kein umfassendes Register für Zertifizierungsanbieter. Die in der DSGVO vorgesehenen Regelungen zur Anerkennung und Verhaltenskodizes und Akkreditierung von Kontrolleinrichtungen könnten die Ausgangslage hierbei verbessern.⁴⁰⁸

Angesichts der mangelnden Maßstäbe zur materiell-rechtlichen Standardisierung von Datenschutz wird vorgeschlagen, ein Ausführungsgesetz nach § 9a BDSG zu erlassen, um die Marktakteure nicht weiterhin auf Selbstregulierung zu verweisen.⁴⁰⁹ Außerdem könnte eine Datenschutzinstitution eingeführt werden, nach dem Modell der Stiftung Warentest oder des TÜV.⁴¹⁰ Solche Vorschläge dürften mit der DSGVO neuen Impetus erfahren, da Art. 42 DSGVO die Förderung von Zertifizierungsstellen nunmehr regelt.

Aufgrund der mangelnden Standards für technische und organisatorische Mindestmaßnahmen i.S.v. materiell-rechtlichen, messbaren und objektiven Parametrisierung des materiellen Datenschutzes auf nationaler und internationaler Ebene,⁴¹¹ hat sich Datenschutz noch nicht zu einem entscheidenden Qualitäts- oder Marktentscheidungsparameter entwickelt und Zertifizierungen und andere Beurteilungen greifen auf selbst definierte Maßstäbe zurück. Dies erschwert die inhaltliche Vergleichbarkeit von Zertifikaten.⁴¹² Als möglicher Standard wird daher vorgeschlagen sich an vorhandenen ISO-Normen zu orientieren, wie z.B. die ISO-Norm 27001 (Information security management systems) mit ihren Vorgaben zur Einführung eines Informationssicherheits-Managementsystems und die darauf aufbauende ISO 27002 (Code of practice for

⁴⁰⁷ Feik/von Lewinski, „Der Markt für Datenschutz-Zertifizierungen - Eine Übersicht“, (2014), *Zeitschrift für Datenschutz*, Heft 2, S. 59-62, S. 59f.

⁴⁰⁸ Spindler/Thorun/Wittmann, *Rechtsdurchsetzung im Verbraucherdatenschutz-Bestandsaufnahme und Handlungsempfehlungen*, (Friedrich Ebert Stiftung, 2016)

⁴⁰⁹ Feik/von Lewinski, „Der Markt für Datenschutz-Zertifizierungen - Eine Übersicht“, (2014), *Zeitschrift für Datenschutz*, Heft 2, S. 59-62, S. 59f.; diesbezügliche Entwicklungen sind jedoch ins Stocken geraten: Dazu Kraska, „Datenschutz-zertifizierungen in der EU-Datenschutzgrundverordnung“, (2016), *Zeitschrift für Datenschutz*, Heft 4, S. 153-154, S. 153 f.

⁴¹⁰ Feik/von Lewinski, „Der Markt für Datenschutz-Zertifizierungen - Eine Übersicht“, (2014), *Zeitschrift für Datenschutz*, Heft 2, S. 59-62, S. 59f.; dazu auch: Withus, „Prüfung oder Zertifizierung eines Compliance Management Systems – Voraussetzungen und mögliche Rechtsfolgen“, (2011), *Corporate Compliance Zeitschrift*, Heft 4, S. 125-133, S. 125f.

⁴¹¹ Dazu Kraska, „Datenschutz-zertifizierungen in der EU-Datenschutzgrundverordnung“, (2016), *Zeitschrift für Datenschutz*, Heft 4, S. 153-154, S. 153f.; Feik/von Lewinski, „Der Markt für Datenschutz-Zertifizierungen - Eine Übersicht“, (2014), *Zeitschrift für Datenschutz*, Heft 2, S. 59-62, S. 59f.

⁴¹² Feik/von Lewinski, „Der Markt für Datenschutz-Zertifizierungen - Eine Übersicht“, (2014), *Zeitschrift für Datenschutz*, Heft 2, S. 59-62, S. 59f.

information security management) Empfehlungen in Form von „Soll-Vorschriften“ für die Einführung von begleitenden Kontrollmechanismen.⁴¹³ Die Datenschutz-Aufsichtsbehörden arbeiten derzeit in ersten Projekten an Regelungskatalogen, auf Basis von ISO 27001/27002/27018 das System der „Soll-Vorgaben“ durch ein Konzept der „Pflicht-Vorgaben“ in Abhängigkeit der verarbeiteten personenbezogenen Datenkategorien zu ersetzen.⁴¹⁴

Mit Blick auf diese Entwicklungen, kann die Datenschutzgrundverordnung eine Möglichkeit sein, mittels von den Datenschutz-Aufsichtsbehörden überwachter Verhaltensregeln bzw. Zertifizierungsstandards die Anforderungen hinsichtlich der technischen Ausgestaltung industriespezifisch dem jeweiligen Stand der Technik entsprechend zu konkretisieren und laufend fortzuentwickeln. Hinsichtlich der Zertifizierungsmöglichkeiten sind mittel- und langfristige Modelle denkbar, bei denen Kontrollmaßnahmen von Datenschutz-Aufsichtsbehörden und auslagernden Unternehmen entbehrlich werden könnten.⁴¹⁵ Damit würde die Datenschutzgrundverordnung im Vergleich zur bisherigen Regelungslage ein großes Defizit in der praktischen Umsetzung schließen, da bei den Unternehmen vielfach Unklarheit hinsichtlich der genauen technischen und organisatorischen Mindestanforderungen besteht.

Ein weiteres Problem bezieht sich auf den Charakter von Zertifizierungsprozessen im Allgemeinen. Zertifizierung hat generell einen statischen und objektbezogenen Charakter, da sie sich immer auf ein konkretes Produkt oder eine konkrete Dienstleistung bezieht; daher wird sie als sinnvoll erachtet, wenn es sich um Produkte oder Dienstleistungen handelt, die eine gewisse Stabilität aufweisen.⁴¹⁶ Inwiefern Zertifizierung daher ein effektives Mittel ist, um Compliance in der innovationsschnellen IT-Branche zu erreichen, ist fraglich. Die spezifischen Charakteristika der Informationsgesellschaft fordern klassische Rechtssetzungs- und -durchsetzungsinstrumente heraus.⁴¹⁷ Möglicherweise kann sich durch Re-Zertifizierung eine gewisse Permanenz ergeben.⁴¹⁸

Außerdem ist problematisch, dass sich die Datenschutzfreundlichkeit eines IT-Produkts oder –dienstleistung oftmals aus der Einsatzumgebung ergeben. So kommt es bei Softwarekomponenten auch auf die verwendete Hardware, das benutzte Betriebssystem und

⁴¹³ Dazu Kraska, „Datenschutz-zertifizierungen in der EU-Datenschutzgrundverordnung“, (2016), *Zeitschrift für Datenschutz*, Heft 4, S. 153-154, S.153 f.

⁴¹⁴ Vgl. vertiefend z.B. das Trusted Cloud-Projekt unter Führung des Bundesministeriums für Wirtschaft und Energie unter <<http://www.trusted-cloud.de>> (zuletzt abgerufen am 30.11.2016) und <<http://www.tcdp.de>> (zuletzt abgerufen am 30.11.2016).

⁴¹⁵ Dazu Kraska, „Datenschutz-zertifizierungen in der EU-Datenschutzgrundverordnung“, (2016), *Zeitschrift für Datenschutz*, Heft 4, S. 153-154, S. 153 f.

⁴¹⁶ Hornung/Hartl, „Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutz-zertifizierung und Datenschutzaudit“, (2014), *Zeitschrift für Datenschutz*, Heft 5, S. 219-225, S. 220.

⁴¹⁷ Spindler/Thorun/Wittmann, *Rechtsdurchsetzung im Verbraucherdatenschutz-Bestandsaufnahme und Handlungsempfehlungen*, (Friedrich Ebert Stiftung, 2016).

⁴¹⁸ Hornung/Hartl, „Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutz-zertifizierung und Datenschutzaudit“, (2014), *Zeitschrift für Datenschutz*, Heft 5, S. 219-225, S. 220.

die spezielle Konfigurierung der Software an; damit ergeben sich Herausforderungen für eine differenzierte Prüfmethodik.⁴¹⁹

Diese Probleme zeigen, dass freiwillige Codes of Conduct, Best Practices und andere selbstregulierenden Maßnahmen nur eine Ergänzung zu einem Rechtssystem darstellen können.⁴²⁰ Eingebettet in ein funktionierendes System von Rechtsetzung und Rechtsdurchsetzung, können Ko-Regulierungsaktivitäten in Form von Verhaltenskodizes, Gütesiegeln und Zertifizierungen 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.⁴²¹

V. Zusammenfassung: Datenschutz durch Technik

Zusammenfassend lässt sich konstatieren, dass es mannigfaltige technische Maßnahmen gibt, die zur Verbesserung des Datenschutzes beitragen könnten. Das entsprechende Potential von PETs, wie zum Beispiel technisches Identitätsmanagement, die automatische Anonymisierung, Pseudonymisierung und Löschung von Daten, sowie DNT-Mechanismen und Sticky Policies, wurden hier beispielhaft dargestellt.

Es wird deutlich, dass ein umfassender Privatsphären- und Datenschutz nur mit holistischen Ansätzen verfolgt werden kann. Datenschutz durch Technik, die Nutzung von PETs für eine Umsetzung von Privacy by Design und Privacy by Default, kann durch eine staatlich überwachte Selbstregulierung umgesetzt werden. Damit befördert Datenschutz durch Technik einen gemischten regulativen Ansatz, der zum einen spezifische Techniken durch Beförderung von Standardisierung vorschreibt und zum anderen auf Marktmechanismen durch teilweise Selbstregulierung vertraut.⁴²² So trägt Privacy by Design zu einem juristisch-induzierten Marktbeeinflussungsprozess bei.⁴²³ Staatliche Aufsicht ist jedoch notwendig, um einen Ersatz von staatlicher Regulierung durch Vertrag und Technik⁴²⁴ und damit die Aushöhlung demokratischer Prozesse zu vermeiden.

Es muss allerdings auch berücksichtigt werden, dass es unmöglich ist, alle PITs in einer ubiquitären Informationsgesellschaft vorherzusehen.⁴²⁵ Ständige Forschung und Innovation ist daher unerlässlich, um ständig neue Sicherheitslücken abzudecken; ein statisches Privacy by Design und Privacy by Default wird, ähnlich wie regulative Maßnahmen hinter technischer Innovation zurückbleiben.

⁴¹⁹ Ibid.

⁴²⁰ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 305.

⁴²¹ Spindler/Thorun/Wittmann, *Rechtsdurchsetzung im Verbraucherdatenschutz-Bestandsaufnahme und Handlungsempfehlungen*, (Friedrich Ebert Stiftung, 2016).

⁴²² Dazu Hornung, "Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework", (2013), *The European Journal of Social Science Research*, Vol. 26, Nr. 1-2, S 181-186, S. 181 f.

⁴²³ Ibid., S. 188.

⁴²⁴ Dazu: Radin, "Regulation by contract, regulation by machine", (2004), *Stanford Public Law and Legal Theory Working Paper Series*, Research Paper No. 92, S. 1-15, S. 1f.

⁴²⁵ Klitou, *Privacy-Invasive Technologies and Privacy by Design*, (Asser Press Springer, 2014), S. 323 ff.

G. Schlussbemerkung

Das Working Paper hat sich mit einigen Problemen des Datenschutzes im IoT beschäftigt. Die Hypothese, dass der Privatsphärenschutz mithilfe von technischen Maßnahmen erfolgen kann, wurde belegt, ohne dass die Untersuchung als abschließend zu verstehen ist. Entsprechende Beispiele wurden dargestellt, nachdem zunächst die Probleme des Datenschutzes im IoT dargestellt wurden.

Materiell-rechtliche Probleme des Datenschutzes im IoT betreffen insbesondere die Wirksamkeitsvoraussetzungen von Einwilligungen. Hierbei geht es um eine mögliche Aushöhlung des Einwilligungserfordernisses durch eine Ausweitung von Datenverarbeitungen für Geschäftszwecke. Diese Aushöhlung wiegt umso schwerer, als dass der datenschutzrechtliche Zweckbindungsgrundsatz nicht gewährleistet ist, wenn Unternehmen mit ausufernden Leistungsbeschreibungen eine Erweiterung der Zwecke, für welche die Daten genutzt werden sollen, erreichen. Dies haben wir auch am Beispiel der HCA, über die verschiedenen IoT-Geräte verbunden werden können, gesehen. Dazu kommt, dass Verbraucher in der Regel formularmäßig in Datenschutzerklärungen einwilligen. Hier stellen sich die gleichen Probleme wie schon im AGB-Recht: Der Verbraucher befindet sich in einer strukturell unterlegenen Position. Im Datenschutzrecht kann dadurch die Freiwilligkeit der Einwilligungserteilung in Frage gestellt sein. Die Kontrollierbarkeit von Datenschutzerklärungen nach AGB-Recht ist daher grundsätzlich zu begrüßen, wenngleich sich daraus auch die aus dem AGB-Recht bekannten Probleme im Datenschutz doppeln.

Insbesondere bei der Rechtsdurchsetzung gibt es Probleme, die den Datenschutz im IoT erheblich beeinträchtigen. Abgesehen von den spezifischen Problemen im deutschen Recht, geht es hier insbesondere um die Sicherstellung eines weltweit hohen Schutzniveaus für Daten. Da Hersteller von IoT-Geräten sowie Cloud-Dienstleister sich oft nicht im europäischen Inland befinden, kommen Vereinbarungen wie dem Privacy Shield besondere Bedeutung zu. Es wiegt schwer, dass sowohl das Privacy Shield als auch der Export-Import-Standardvertrag von Datenschützern als unzureichend eingeschätzt wird. Rechtssicherheit besteht wegen der Anstrengungen, sie gerichtlich überprüfen zu lassen, noch nicht.

Auch wenn Datenschutz im IoT - wegen der Gegenüberstellung von PITs und PETs - ein prominenter Anwendungsbereich für technische Schutzmaßnahmen ist, muss klargestellt werden, dass technische Maßnahmen mit rechtlicher Regulierung verzahnt werden müssen. Nur dann kann sichergestellt sein, dass beispielsweise Privacy by Design nicht als bloße Selbstregulierung angesehen wird. Außerdem müssen erhebliche finanzielle Ressourcen mobilisiert werden, damit die Regulierung von technischem Datenschutz nicht hinter der Innovationsgeschwindigkeit der Industrie zurück bleibt. Darüber hinaus muss weitere Forschung betrieben werden, um die vielen Problemfelder, die im Rahmen dieses Working Papers nur angerissen werden konnten, abschließend zu untersuchen.

Mit dem grundlegenden BVerfG-Urteil zur Volkszählung ist die grundrechtliche und soziale Relevanz von Privatsphärenschutz klar geworden. Das IoT muss als privatsphärenintensives Anwendungsfeld besonders im Blickfeld eines regulativ eingreifenden Datenschutzrechts stehen, um informationelle Selbstbestimmung tatsächlich zu gewährleisten. Dabei sollte

auch diskutiert werden, ob Privatsphärenbelange datenschutzrechtlich überhaupt als Probleme von „Personenbezogenen Daten“ betrachten werden sollten. Eine breite Diskussion der gesamtgesellschaftlichen Phänomene und Probleme der Digitalisierung ist notwendig.

H. Literaturnachweise

Kommentare

Bamberger, Heinz/Roth, Herbert (Hrsg.), (2016), Beck'scher Online-Kommentar BGB, 40. Edition 2016, München: C.H. Beck Verlag

Boecken, Winfried/Düwell, Franz/Diller, Martin/Hanau, Hans (Hrsg.), (2016), Gesamtes Arbeitsrecht Nomos Kommentar, Baden-Baden: Nomos Verlag

Calliess, Christian/Ruffert, Matthias (Hrsg.), (2016), EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, 5. Auflage, München: C.H. Beck Verlag

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (Hrsg.), (2016), Bundesdatenschutzgesetz Kompaktkommentar zum BDSG, 5. Auflage, Frankfurt a. Main: Bund-Verlag

Ehmann, Eugen/Helfrich, Marcus (Hrsg.), (1999), EG-Datenschutzrichtlinie Kurzkommentar, Köln: Otto Schmidt Verlag

Gola, Peter/Schomerus, Rudolf (Hrsg.), (2015), Kommentar zum Bundesdatenschutzgesetz, 12. Auflage, München: C.H. Beck Verlag

Grobys, Marcel/Panzer, Andrea (Hrsg.), (2016), StichwortKommentar Arbeitsrecht, 2. Auflage, 8. Edition, Baden-Baden: Nomos Verlag

Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan (GesamtHrsg.), (2016), Beck-Online Grosskommentar, Stand 01.10.2016, München: C.H. Beck Verlag

Häberle, Peter (Hrsg.), (2016), Erbs/Kohlhaas Strafrechtliche Nebengesetze, Band 17, 210. Auflage, München: C.H. Beck Verlag

Jarass, Hans/Pieroth, Bodo (Hrsg.), (2014), Kommentar zum Grundgesetz, 13. Auflage, München: C.H. Beck Verlag,

Palandt, Otto (Hrsg.), (2015), Bürgerliches Gesetzbuch Kommentar, 74. Auflage, München: C.H. Beck Verlag

Rauscher, Thomas/Krüger, Wolfgang (Hrsg.), (2013), Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, 4. Auflage, München: C.H. Beck Verlag

Säcker, Franz/Rixecker, Roland/Oetker, Hartmut/Limberg, Bettina (Hrsg.), (2016), Münchener Kommentar zum BGB, 7. Auflage, München: C.H. Beck Verlag

Schwarze, Jürgen/Becker, Ulrich/Hatje, Armin/Schoo, Johann (Hrsg.), (2012), EU-Kommentar, 3. Auflage, Baden-Baden: Nomos Verlag

Simitis, Spiros (Hrsg.), (2014), Kommentar zum Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden: Nomos Verlag

Spindler, Gerald/Schuster, Fabian (Hrsg.), (2015), Recht der elektronischen Medien Kommentar, 3. Auflage, München: C.H. Beck Verlag

Staudinger, Julius (Hrsg.), (2013), Kommentar zum Bürgerlichen Gesetzbuch: Staudinger BGB - Buch 2: Recht der Schuldverhältnisse §§ 305-310; UKlaG (Recht der Allgemeinen Geschäftsbedingungen), 15. Auflage, Berlin: De Gruyter Verlag

Taeger, Jürgen/Gabel, Detlev (Hrsg.), (2013), BDSG und Datenschutzvorschriften des TKG und TMG Kommentar, 2. Auflage Frankfurt a. Main: Deutscher Fachverlag-Recht und Wirtschaft Verlag

Ulmer, Peter/Brandner, Erich/Hensen, Horst-Diether (Hrsg.), (2016), AGB-Recht Kommentar zu den §§ 305-310 BGB und zum UKlaG, 12. Auflage, Köln: Otto Schmidt Verlag

Walker, Wolf-Dietrich (Hrsg.), (2016), Unterlassungsklagengesetz Nomos Kommentar, Baden-Baden: Nomos Verlag

Wolff, Heinrich/Brink, Stefan (Hrsg.), (2016), Beck'scher Online-Kommentar Datenschutzrecht, 17. Edition, München: C.H. Beck Verlag

Wolf, Manfred/Lindacher, Walter/Pfeiffer, Thomas (Hrsg.), (2013), AGB-Recht Kommentar, 6. Auflage, München: C.H. Beck Verlag

Bücher

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), (2016), Handbuch IT- und Datenschutzrecht, München: C.H. Beck Verlag

Bala, Christian/Müller, Klaus (Hrsg.), (2014), Der Gläserne Verbraucher: Wird Datenschutz zum Verbraucherschutz-Beitrag zur Verbraucherforschung, Düsseldorf: Verbraucherzentrale NRW

Bala Christian/Schuldzinski, Wolfgang (Hrsg.), (2016), Schöne neue Verbraucherwelt? Big Data, Scoring und das Internet der Dinge, Beiträge zur Verbraucherforschung Band 5, Düsseldorf: Verbraucherzentrale NRW

Brownsword, Roger & Yeung, Karen (Hrsg.), (2008), Regulating technologies: Legal Futures, Regulatory Frames and Technological Fixes, London: Hart Publishing Verlag

Buchner, Benedikt (2006), Informationelle Selbstbestimmung im Privatrecht, Tübingen: Mohr Siebeck Verlag

Dorschel, Joachim (Hrsg.), (2015), Praxishandbuch Big Data Wirtschaft – Recht – Technik, Berlin: Springer Gabler Verlag

Grabitz, Eberhard/Hilf, Meinhard (Hrsg.), (2009), Das Recht der Europäischen Union, München: C.H. Beck Verlag

Gramatica, Martina/Massacci, Fabio, (2015), FP7 ICT Trust & Security Projects Handbook, University of Trento

Greengard, Samuel, (2015), The Internet of Things, Cambridge: MIT Press Verlag

- Hager, Johannes,(1983), Gesetzes- und sittenkonforme Auslegung und Aufrechterhaltung von Rechtsgeschäften, München: C.H.Beck Verlag
- Hauschka, Christoph/Moosmayer, Klaus/Lösler, Thomas (Hrsg.), (2016), Corporate Compliance Handbuch der Haftungsvermeidung im Unternehmen, München: C.H. Beck Verlag
- Hes, Ronald/Borking, John,(1998), Privacy-enhancing Technologies: The path to anonymity, Den Haag: Registratiekamer Verlag
- Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), (2015), Handbuch Multimedia-Recht Rechtsfragen des elektronischen Geschäftsverkehrs, München: C.H. Beck Verlag
- Klitou, Demetrius, (2014), Privacy-Invasive Technologies and Privacy by Design, Berlin: Asser Press Springer Verlag
- Kötz, Hein, (1996), Europäisches Vertragsrecht, Tübingen: Mohr Siebeck Verlag
- Lessig, Lawrence, (2006), Code and other laws of cyberspace Version 2.0, New York: Basic Books Verlag
- Schaar, Peter, (2002), Datenschutz im Internet: Die Grundlagen, München: C.H. Beck Verlag
- Schmidt, Harry, (1986), Vertragsfolgen der Nichteinbeziehung und Unwirksamkeit von Allgemeinen Geschäftsbedingungen, Frankfurt a. Main: Deutscher Fachverlag
- Schmidt-Salzer, Joachim, (1997), Das Recht der Allgemeinen Geschäfts- und Versicherungsbedingungen, Berlin: Duncker & Humblot Verlag
- Schulze, Reiner/Zuleeg, Manfred/Kadelbach, Stefan (Hrsg.), (2015), Europarecht – Handbuch für die deutsche Rechtspraxis, Baden-Baden: Nomos Verlag
- Skistims, Hendrik (2016), Smart Homes, Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Baden-Baden: Nomos Verlag
- Spindler, Gerald/Schuster, Fabian (Hrsg.), (2015), Recht der elektronischen Medien Kommentar, München: C.H. Beck Verlag
- Spindler, Gerald/Thorun, Christian/Wittmann, Jörn (2016), Rechtsdurchsetzung im Verbraucherdatenschutz-Bestandsaufnahme und Handlungsempfehlungen, Bonn: Friedrich Ebert Stiftung
- Tinnefeld, Marie-Theres/Buchner, Benedikt/Petri, Thomas, (2012), Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht, Berlin: De Gruyter Verlag

Zeitschriften

- Bauer, Stephan, (2008), Personalisierte Werbung auf Social Community-Websites - Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen, MultiMedia und Recht, Heft 7, S.435-438

- Dorner, Michael, (2014), Big Data und Dateneigentum, Computer und Recht, Band 30, Heft 9, S.617-628
- Faust, Sebastian/Spittka, Jan/Wybitul, Tim, (2016), Milliardenbußgelder nach der DS-GVO? - Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, Zeitschrift für Datenschutz, Heft 3, S. 120-125
- Feik, Sebastian/von Lewinski, Kai, (2014), Der Markt für Datenschutz-Zertifizierungen - Eine Übersicht, Zeitschrift für Datenschutz, Heft 2, S. 59-62
- Graf v. Westphalen, Friedrich, (2007), AGB-Recht im Jahr 2006, Neue Juristische Wochenschrift, Heft 31, S. 2228-2236
- Grimmelmann, James, (2005), Regulation by software, Yale Law Journal, Vol. 114, S. 1719-1758
- Guarda, Paolo/Zannone, Nicola, (2009), Towards the development of privacy-aware systems, Information and Software Technology, Vol. 51, Nr. 2, S. 337-350
- Härting, Niko, (2015), Zweckbindung und Zweckänderung im Datenschutzrecht, Neue Juristische Wochenschrift, Heft 45, S. 3284-3288
- Halfmeier, Axel, (2016), Die neue Datenschutzverbandsklage, Neue Juristische Wochenschrift, Heft 16, S. 1126-1129
- Hanloser, Stefan, (2009), EuGH: Umfang und Dauer des Auskunftsanspruchs über Datenempfänger, Datenschutzberater, Heft 7-8
- Heinrichs, Helmut, (1996), Das Gesetz zur Änderung des AGB-Gesetzes Umsetzung der EG-Richtlinie über mißbräuchliche Klauseln in Verbraucherverträgen durch den Bundesgesetzgeber, Neue Juristische Wochenschrift, Heft 34, S. 2190-2197
- Hornung, Gerrit/Hartl, Korbinian, (2014), Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit, Zeitschrift für Datenschutz, Heft 5, S. 219-225
- Hornung, Gerrit, (2013), Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework, The European Journal of Social Science Research, Vol. 26, Nr. 1-2, S 181-186
- Koops, Bert-Jaap, (2007), TILT Law & Technology Working Paper Series No. 005/2007, Brownsword & Yeung, (Hrsg.), Regulating Technologies, S. 157-174
- Kranig, Thomas, (2013), Zuständigkeit der Datenschutzaufsichtsbehörden - Feststellung des Status quo mit Ausblick auf die DS-GVO, Zeitschrift für Datenschutz, Heft 11, S. 550-557
- Kraska, Sebastian, (2016), Datenschutzzertifizierungen in der EU-Datenschutzgrundverordnung, Zeitschrift für Datenschutz, Heft 4, S. 153-154
- Kremer, Sascha, (2002), Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices, Computer und Recht, Heft 7, S. 438-446
- Kremer, Sascha, (2014), Datenschutzerklärungen von Social Media Diensten: Anwendbares Recht und AGB-Kontrolle“, Recht der Datenverarbeitung, Heft 2, S. 73-83

- Kühling, Jürgen/Martini, Mario, (2016), Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, Europäische Zeitschrift für Wirtschaftsrecht, Heft 12, S. 448-454
- Martiny, Dieter, (1996), Pflichtenorientierter Drittschutz beim Vertrag mit Schutzwirkung für Dritte - Eingrenzung uferloser Haftung, Juristenzeitschrift, S. 19-25
- Marwitz, Petra, (2003), Zwangskommerzialisierung vermögenswerter immaterieller Rechte, Zeitschrift für Medien und Kommunikationsrecht, Heft 5, S. 405-409.
- N.N., (2016), Der Digitale Mensch, Spektrum Kompakt Der digitale Mensch
- Ohly, Ansgar, (2004), Das neue UWG – Mehr Freiheit für den Wettbewerb?, Gewerblicher Rechtsschutz und Urheberrecht, Heft 11, S.889-900
- Pearson, Siani/ Mont, Marco, (2011), Sticky Policies: An Approach for Managing Privacy across Multiple Parties, IEEE Computer Magazine, Vol. 44, Nr. 9, S. 60–67
- Radin, Margaret Jane, (2004), Regulation by Contract, Regulation by Machine, 160 Journal of Institutional and Theoretical Economics, S. 1-15
- Reidenberg, Joel, (1997), Lex Informatica: The Formulation of Information Policy Rules through Technology, Texas Law Review, S. 553-593
- Ritter, Franziska/Schwichtenberg, Simon, (2016), Die Reform des UKlaG zur Eliminierung des datenschutzrechtlichen Vollzugsdefizits – neuer Weg, neue Chancen?, Verbraucher und Recht, Heft 3, S. 95-102
- Robak, Markus, (2016), Neue Abmahnrisiken im Datenschutzrecht, Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter und Wettbewerbsrecht, Heft 7, S. 139-141
- Roßnagel, Alexander/Desoi, Monika/Hornung, Gerrit, (2012), Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik - Am Beispiel der smarten Videoüberwachung, Zeitschrift für Datenschutz, Heft 10, S.459-462
- Roßnagel, Alexander, (2014), Fahrzeugdaten – wer darf über sie entscheiden?, Straßenverkehrsrecht, Heft 8, S. 281-287
- Sachs, Andreas/Meder, Miriam, (2013), Datenschutzrechtliche Anforderungen an App-Anbieter - Prüfungen am Beispiel von Android-Apps, Zeitschrift für Datenschutz, Heft 7, S. 303-308
- Schantz, Peter, (2016), Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht?, Neue Juristische Wochenschrift, Heft 26, S. 1841-1847
- Schuler, Karin/Weichert, Thilo, (2016), Ein „Export-Import-Standardvertrag“ für den Drittauslands-Datentransfer (2016), Datenschutz und Datensicherheit, Heft 6, S. 388-390
- Schwartz, Paul (2000), Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, Wisconsin Law Review, S. 743-788
- Stiftung Warentest, (2016), Test 3/2016, S. 57 – 61

Weichert, Thilo, (2001), Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, Neue Juristische Wochenschrift, Heft 20, S. 1463-1469

Wendehorst, Christiane, (2016), Die Digitalisierung und das BGB, Neue Juristische Wochenschrift, Heft 36, S. 2609-2613

Wisman, Tijmen, (2013), Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things, European Journal of Law and Technology, Vol. 4, No. 2, .S. (n.a.)

Withus, Karl-Heinz, (2011), Prüfung oder Zertifizierung eines Compliance Management Systems – Voraussetzungen und mögliche Rechtsfolgen, Corporate Compliance Zeitschrift, Heft 4, S. 125-133

Yeung, Karen/Dixon-Woods, Mary, (2010), Design-based regulation and patient safety: a regulatory studies perspective, Social Science Medicine, Vol. 71, Nr. 3, 502-509

Zenner, Andreas (2009), Der Vertrag mit Schutzwirkung zu Gunsten Dritter – Ein Institut im Lichte seiner Rechtsgrundlage, Neue Juristische Wochenschrift, Heft 15, S. 1030-1034

Working-Paper/Gutachten

Faust, Florian, (2016), Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag

Schmechel, Philipp, (2016), Verbraucherdatenschutz nach der EU-Datenschutzgrundverordnung, SVRV Working Paper Series Nr. 4/2016, Sachverständigenrat für Verbraucherfragen

Spindler, Gerald, (2016), Regulierung durch Technik, Gutachten im Auftrag des Sachverständigenrates für Verbraucherfragen

Wendehorst, Christiane, (2016), Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Studie im Auftrag des Sachverständigenrats für Verbraucherfragen

Internetseiten

ABI Research, (2014), Internet of Things vs. Internet of Everything: what's the difference? <<https://digitalstrategy.nl/files/Internet-of-Things-vs-Internet-of-everything-by-ABI-June-2014.pdf>> (Stand 30.11.2016)

Albrecht, Jan Philipp, (2015), Ergebnisse der Verhandlungen („Trilogie“) und die 10 wichtigsten Punkte - Federführender Ausschuss des Europäischen Parlaments: Bürgerliche Freiheiten, Justiz und Inneres (LIBE), EP-Verhandlungsführer („Berichterstatter“): Jan Philipp Albrecht, MdEP, Grüne / Europäische Freie Allianz, <https://www.janalbrecht.eu/fileadmin/material/Dokumente/20151217_Datenschutzreform_10_wichtige_Punkte_DE.pdf> (Stand 07.11.16)

Albrecht, Jan Philipp, (2015), EU-Datenschutzgrundverordnung: Stand der Dinge – 10 wichtige Punkte, <http://www.janalbrecht.eu/fileadmin/material/Dokumente/Datenschutzreform_Stand_der_Dinge_10_Punkte_110615.pdf> (Stand 14.11.2016)

Arbeitsgruppe, (2002), Handreichung „Datenschutzgerechtes eGovernment“,
<<http://www.bfdi.bund.de/SharedDocs/Publikationen/PM29-04HandreichungDatenschutzgerechteseGovernment.html>> (Stand 16.09.2016)

Artikel-29-Datenschutzgruppe, (2005), Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24.10.1995, (WP 114),
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_de.pdf> (Stand 30.11.2016)

Art 29 Data Protection Working Party (2016) Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> (Stand 15.11.2016)

Baker, Pam, (2015), Big Data: Protecting Privacy Is Good For Business,
<http://www.informationweek.com/software/enterprise-applications/big-data-protecting-privacy-is-good-for-business/a/d-id/1320367> (Stand 15.11.2016)

Berufsverbands der Datenschutzbeauftragten Deutschland (BvD) e.V., (2014),
Stellungnahme zur Änderung des UKlaG zugunsten der Klagemöglichkeit durch
Verbraucherschutzverbände bei Datenschutzverstößen
<https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/Standpunkte/140815-BvD-Stellungnahme_zur_Ank%C3%BCndigung_des_UKlaG.pdf> (zuletzt aufgerufen am 23.09.2016)

Bracy, Jedidiah, (2016), Model clauses in jeopardy with Irish DPA referral to CJEU,
<<https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu/>> (Stand 15.11.2016)

Bradley et al, (n.a.), Internet of Everything (IoE) Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector, <<http://internetofeverything.cisco.com/vas-public-sector-infographic/>> (Stand 09.11.2016)

Brookman., Justin, (2015), Progression of TPE to CR, TCS to LC,
<<https://lists.w3.org/Archives/Public/public-tracking/2015Jul/0000.html>> (zuletzt abgerufen am 28.11.2016)

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, (2015), 25.
Tätigkeitsbericht zum Datenschutz 2013 – 2014,
<https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/25TB_13_14.pdf;jsessionid=047ADA6C12D5BF27DE04AAB7DF1ADB96.1_cid319?__blob=publicationFile&v=10> (Stand 10.11.16)

Bundesministerium der Justiz und für Verbraucherschutz, (n.a.), Europäische
Zusammenarbeit im Verbraucherschutz,
<http://www.bmju.de/DE/Verbraucherportal/Verbraucherinformation/CPC/CPC_node.html>
(Stand 17.11.2016)

Bundesministerium für Wirtschaft und Energie, (n.a.), Trusted Cloud-Projekt <www.trusted-cloud.de> (Stand 15.11.2016)

Cavoukian, Ann, (2011), Privacy by Design, The 7 Foundational Principles, <**Fehler!
Hyperlink-Referenz ungültig.**> (Stand 30.11.2016)

Commission Implementing Decision of 12.7.2016, (2016), pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, Brussels, 12.7.2016, C(2016) 4176 final, <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf> (Stand 30.11.2016)

Data Protection Commissioner, (2016), Findings of International Privacy Sweep 2016 published, <<https://www.dataprotection.ie/docs/23-9-2016-International-Privacy-Sweep-2016/i/1597.htm>> (Stand 09.11.2016)

Datenschutzerklärung Home Connect App <<http://www.home-connect.com/de/de/datenschutz/datenschutz.html>>, (Stand 30.09.2016)

Datenschutzzentrum von Adobe, (2016), EU-U.S. Privacy Shield / EU-US-Datentransfer <<http://www.adobe.com/de/privacy/eudatatransfers.html>> (Stand 15.11.2016)

Der Sächsische Datenschutzbeauftragte, (2014), Anonymisierung der IP-Adressen in Webserver-Logfiles, <<https://www.saechsdsb.de/ipmask>> (Stand 05.11. 2016)

Düsseldorfer Kreis, (2016), Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, <https://www.lda.bayern.de/media/dk_einwilligung.pdf> (Stand 02.11.2016)

Elshout, Maartje et al., (2016), Study on consumers' attitudes towards Terms and Conditions (T&Cs), European Commission, Directorate-General for Justice and Consumers <http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/terms_and_conditions_final_report_en.pdf> (Stand 30.11.2016)

Et. al, (2016), Beschlüsse des 71. Deutschen Juristentags, <http://www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf> (Stand 30.11.2016)

Europäische Kommission, (2014), Pressemitteilung, Versicherungsvertragsrecht: Experten weisen auf Hemmnisse für das grenzüberschreitende Geschäft hin <http://europa.eu/rapid/press-release_IP-14-194_de.htm> (Stand 17.11.2016)

Europäische Kommission, (2015), Pressemitteilung, Ein digitaler Binnenmarkt für Europa: Kommission stellt 16 Initiativen zur Verwirklichung vor, <http://europa.eu/rapid/press-release_IP-15-4919_de.htm> (Stand 30.11.2016)

Europäische Kommission, (2016), Executive Summary of the Impact Assessment, accompanying the document Proposal for a Regulation of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws, Commission Staff Working Document, <<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0165>> (Stand 30.11.2016)

Europäische Kommission, (2016), Proposal for a Regulation of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws, COM (2016) 283 final, <http://ec.europa.eu/consumers/consumer_rights/unfair-trade/docs/cpc-revision-proposal_en.pdf> (Stand 30.11.2016)

Europäisches Parlament, Rat und Kommission, (2015) Gemeinsamer Leitfaden des Europäischen Parlaments, des Rates und der Kommission für Personen, die an der Abfassung von Rechtstexten der Europäischen Union mitwirken, <<http://eur-lex.europa.eu/content/techleg/KB0213228DEN.pdf>> (Stand 15.11.2016)

European Commission, (2016), Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive, <<https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive>> (Stand 15.11.2016)

European Data Protection Supervisor, (n.a.), Aufsicht und Durchsetzung <<https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/Supervision>> (Stand 06.10.16)

European Data Protection Supervisor, (2008), The EDPS and EU Research and Technological Development Policy paper, <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf> (Stand 15.11.2016)

Federal Trade Commission, (2015), Order RM-11757, In the Matter of Consumer Watchdog Petition for Rulemaking to Require Edge Providers to Honor Do Not Track <https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1266A1.pdf> (Stand 30.11.2016)

Fokusgruppe, (2016), Privacy by Design/Datenschutz durch Technik, Nationaler IT-Gipfel Saarbrücken 2016, <https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/11162016_IT_Gipfel_Thesenpapier.pdf?__blob=publicationFile&v=1> (Stand 30.11.16)

Gallagher, (2016), Sean Double-dip Internet-of-Things botnet attack felt across the Internet, <<http://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/>> (Stand 09.11.2016)

Greveler, Ulrich, (2015), Intelligente Stromzähler–Überwachungsinstrument von morgen?, <http://oliver-krischer.eu/fileadmin/user_upload/gruene_bt_krischer/fotos/3_Greveler.pdf> (Stand 30.11.2016).

Hansen, Marit et al., (2008), Datenschutzförderndes Identitätsmanagement, Hintergrundpapier zur Entschließung Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008, <<https://www.datenschutz-mv.de/datenschutz/publikationen/informat/idmgt/id-mgt.pdf>> (Stand 30.11.2016)

Herrmann, Dominik/Lindemann, Jens, (2016), Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights?, <<https://arxiv.org/abs/1602.01804>> (Stand 07.10.2016)

Horchert, Judith/Stöcker, Christian, (2015), Smart Home im Eigenbau-Die Sensorenresidenz, <<http://www.spiegel.de/netzwelt/gadgets/smart-home-in-st-pauli-technik-in-jeder-ecke-a-1061903.html>> (Stand 30.1.2016)

Internetauftritt Marktwächter, <<http://www.marktwaechter.de/>> (Stand 06.09.2016)

Johnson, Bobbie, (2010), Privacy no longer a social norm, says Facebook founder
<<https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>> (Stand 02.11.2016)

Kaiser, Ingo, (2016), Anforderungen an die Einwilligung gemäß der EU-DSGVO,
<<https://www.projekt29.de/datenschutzblog29/anforderungen-an-die-einwilligung-gemaess-der-eu-dsgvo>> (Stand 09.11.2016)

Kenny, Steve/Borking, John, (2002), The Value of Privacy Engineering, Journal of Information, Law and Technology, <<http://elj.warwick.ac.uk/jilt/02-1/kenny.html>>. New citation as at 1/1/04: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/> (Stand 30.11.2016)

Lahlou, Saadi/Jegou, Francois, (2004), European disappearing computer privacy design guidelines, < <http://eprints.lse.ac.uk/33125/>> (Stand 15.11.2016)

Lardineus, Frederic, (2015), Microsoft Will Remove “Do Not Track” As The Default Setting In Its New Browsers, <<https://techcrunch.com/2015/04/03/microsoft-disables-do-not-track-as-the-default-setting-in-internet-explorer/>> (Stand 28.11.2016)

Möchel, Erich, (2016), Machtvolle Rückkehr der DDoS-Attacken,
<<http://fm4.orf.at/stories/1773571/>> (Stand 09.11.2016)

Müller, Klaus, (2016), Erweitertes Verbandsklagerecht: Datenschutzverstöße werden sich nicht mehr lohnen, <<http://www.vzbv.de/pressemitteilung/erweitertes-verbandsklagerecht-datenschutzverstoesse-werden-sich-nicht-mehr-lohnen>> (zuletzt abgerufen am 10.11.2016)

Müller, Klaus, (2016) Reaktion auf die UKlaG-Reform,
<<http://www.vzbv.de/pressemitteilung/erweitertes-verbandsklagerecht-datenschutzverstoesse-werden-sich-nicht-mehr-lohnen>> (Stand 10.11.16)

N.a., (n.a.), Das Projekt CamInSens, <<http://www.caminsens.org/index.html>> (zuletzt abgerufen am 15.11.2016)

N.a, (n.a.), Declaration of Internet Rights
<http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf> (zuletzt abgerufen am 02.11.2016)

N.a., (n.a.), Deine Daten verlangen! Schicke ein Auskunftersuchen an Facebook!,
<http://europe-v-facebook.org/DE/Daten_verlangen_/daten_verlangen_.html> (Stand 25.08.2016)

N.a, (n.a.), Informationen zum E-racker, <www.etracker.com> (Stand 28.11.2016)

N.a, (n.a.), Prime-#Preventing, Interdicting and Mitigating Extremism, <<http://www.fp7-prime.eu/project>> (Stand 30.11.2016)

N.a, (n.a.), Privacy Incorporated Software Agent: Building a privacy guardian for the electronic age (PISA), <[http://www.2020-horizon.com/PISA-Privacy-Incorporated-Software-Agent-Building-a-privacy-guardian-for-the-electronic-age-\(PISA\)-s50085.html](http://www.2020-horizon.com/PISA-Privacy-Incorporated-Software-Agent-Building-a-privacy-guardian-for-the-electronic-age-(PISA)-s50085.html)> (Stand 30.11.2016)

N.a, (n.a.), Schritt für Schritt – Anleitung “Beschwerde gegen die irische Behörde bei der EU”
<http://europe-v-facebook.org/DE/Daten_verlangen_/Beschwerde_einreichen/beschwerde_einreichen.html>
(Stand 25.08.2016)

N.a., (2009), Petition 7180-Datenschutz - Durchsetzung des Auskunftsanspruchs,
<https://epetitionen.bundestag.de/petitionen/_2009/_09/_12/Petition_7180.nc.html> (Stand 07.10.2016)

N.a., (2011), Hewlett Packard Privacy Statement,
<http://www8.hp.com/us/en/pdf/hp_fy11_gcr_privacy_tcm_245_1357687.pdf> (Stand 15.11.2016)

N.a, (2016) Finanzmarktwächter-Sinnvoller Ansatz mit Verbesserungspotenzial,
<<http://www.die-bank.de/news/sinnvoller-ansatz-mit-verbesserungspotenzial-8118/>> (zuletzt abgerufen am 14.10.2016)

Niemitz, Marcus/Somorovsky, Juraj/Mainka, Christian/Schwenk, Jörg, (2015), Not so Smart: On Smart TV Apps,
<<https://www.nds.rub.de/media/nds/veroeffentlichungen/2015/08/31/SmartTvAttacks.pdf>>
(Stand 20.10.2016)

Paramaguru, Abi et al, (2008), Distinguishing PETs from PITs: Developing technology with privacy in mind, Submission to the Australian Law Reform Commission on the Review of Australian Privacy Laws Discussion Paper 72,
<http://www.cyberlawcentre.org/ipp/publications/papers/ALRC_DP72_Technology_final.pdf>
(Stand 30.11.2016)

Petition des Center for Democracy & Technology an die Federal Trade Commission, (2009), In advance of the FTC Town Hall, Behavioral Advertising: Tracking, Targeting, and Technology, <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>> (Stand 30.11.2016)

Pfitzmann, Andreas/Hansen, Marit, (2010), A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Maisch, Nicole, (2019) Marktwächter – gute Bilanz mit Luft nach oben,
<<https://www.gruene-bundestag.de/presse/pressemitteilungen/2016/august/marktwaechter-gute-bilanz-mit-luft-nach-oben-25-08-2016.html>> (Stand 14.10.2016)

Preliminary FTC Staff Report, (2010), Protecting Consumer Privacy in an Era of Rapid Change, A proposed framework for business and policymakers
<<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>> (Stand 30.11.2016)

Müller, Edda, (2007), Consumer Watchdogs: Stärkung der Verbraucher
<http://www.vzbv.de/sites/default/files/mediapics/consumer_watchdogs_20_juni_2007.pdf>
(zuletzt abgerufen am 26.09.2016)

Reidenberg, Joel, (2002), Privacy protection and the interdependence of law, technology and self-regulation, Vortrag zum 20. Geburtstag des C. R. I. D
<<http://reidenberg.home.sprynet.com>> (Stand 15.11.2016)

Rodotá, Stefano, (n.a.), Towards a Declaration of Internet Rights,
<http://www.camera.it/application/xmanager/projects/leg17/attachments/upload_file/upload_files/000/000/194/Internet_Libe_inglese.pdf> (Stand 02.11.2016)

Roßnagel, Alexander, (n.N.), Rechtliche Aspekte: Die Entwicklung des Drei-Stufen-Modells anhand der Methode KORA
<http://www.caminsens.org/PDF/CamInSens_Rechtliche_Aspekte.pdf> (zuletzt abgerufen am 15.11.2016)

Schrems, Maximilian, (2016), Rapid Press Update: Facebook & NSA-Surveillance: Following "Safe Harbor" decision, Irish Data Protection Commissioner to bring EU-US data flows before CJEU again, <http://www.europe-v-facebook.org/PA_MCs.pdf> (Stand 15.11.2016)

Schulzki-Haddouti, Christiane, (2012), "Facebooks Geschäftsmodell ist illegal",
<<https://futurezone.at/netzpolitik/facebook-gegeschaeftsmodell-ist-illegal/24.583.706>> (Stand 13.10.2016)

Schulzki-Haddouti, Christiane, (2016), Ideengeschichte des Privacy by Design,
<<https://www.datenschutzbeauftragter-online.de/datenschutz-ideengeschichte-privacy-by-design-teil-1/9929/>> (Stand 28.11.2016)

SPD-Bundestagsfraktion, (2012), Verbraucherinteressen stärken-Marktwächter einführen,
<http://kerstintack.de/imperia/md/content/bezirkhannover/kerstintack/2013/dokumentation_marktwaechter_nov_12.pdf> (Stand 26.09.2016)

Sprenger, Polly, (n.a.), Sun on Privacy: 'Get Over It',
<<http://archive.wired.com/politics/law/news/1999/01/17538>> (Stand 02.11.2016)

Tang, Qiang, (2008), On Using Encryption Techniques to Enhance Sticky Policies Enforcement, <<http://doc.utwente.nl/65155/>> (Stand 28.11.2016)

Thomson, Darren et. al., (2015), State of Privacy Report 2015,
<<http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf>> (Stand 14.10.16)

Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, (2016), 2. Tätigkeitsbericht des TLfDI zum Datenschutz: Nicht-öffentlicher Bereich 2014/2015,
<https://www.tlfdi.de/imperia/md/content/datenschutz/taetigkeitsberichte/2_t__tigkeitsbericht.pdf> (Stand 7.11.2016)

VZBV Pressemitteilung, (2015), Finanzmarktwächter und Marktwächter Digitale Welt starten und bauen Marktbeobachtung auf,
<<http://www.vzbv.de/pressemitteilung/finanzmarktwaechter-und-marktwaechter-digitale-welt-starten-und-bauen>> (Stand 06.09.2016)

Weinberg, Jonathan, (2004) RFID and Privacy,
<<https://poseidon01.ssrn.com/delivery.php?ID=907117081025013120100021005065120072>>

02603204600906507810812209606712612507008701302503205209612603901500111502
40210920041030260220530750091021010800870011100650030211111250800680830710
65023075083088119006080111024028086006126104073119008065088&EXT=pdf> (Stand
30.11.2016).

Wewel, Uwe, (2016), Finanzwächter oder Nachtwächter?, <<http://www.cash-online.de/recht-steuern/2016/finanzwaechter-oder-nachtwaechter/326871/2>> (Stand 14.10.2016)

I. Annex

I. Datenschutzerklärung HCA

Datenschutzerklärung für die Home Connect App

Die Home Connect GmbH mit Sitz in Carl-Wery-Straße 34, 81739 München, Deutschland (nachfolgend „Home Connect“ oder „Wir“) ist die verantwortliche Stelle für die Erhebung, Verarbeitung und Nutzung Ihrer personenbezogenen Daten im Zusammenhang mit der Home Connect App (nachfolgend „App“).

Wir erheben, verarbeiten und nutzen Ihre personenbezogenen Daten in Übereinstimmung mit den anwendbaren Datenschutzgesetzen und erläutern Ihnen den Datenumgang im Folgenden näher.

1. Kategorien von personenbezogenen Daten

Im Zusammenhang mit der Nutzung der App erhebt, verarbeitet und nutzt Home Connect im Wesentlichen die folgenden Kategorien personenbezogener Daten:

a. Nutzer-Stammdaten

Daten, die wir im Zusammenhang mit dem Anlegen eines Nutzerkontos (Registrierung) erheben und verwenden sind:

- Angaben, die Sie im Rahmen der Registrierung machen, wie:
 - Vor- und Nachname
 - E-Mail-Adresse (Benutzerkennung)
 - das Land, indem Sie Ihr(e) Hausgerät(e) betreiben
 - Passwort als Zugriffsschutz.
- Informationen, die wir im Zusammenhang mit der Registrierung erheben und speichern:
 - Spracheinstellung Ihres mobilen Endgerätes
 - Einverständnis mit der Geltung der Nutzungsbedingungen und Bestätigung der Kenntnisnahme der Datenschutzerklärung
 - Status des Nutzerkontos (aktiviert/deaktiviert)
 - App Tracking-Voreinstellung (erfolgt in Abhängigkeit der Landeswahl, siehe dazu unten 5.).

b. Geräte-Stammdaten

Daten, die wir im Zusammenhang mit der Verbindung Ihres Hausgerätes mit dem Nutzerkonto erheben und verwenden, sind:

- Marke des Hausgerätes (z.B. Bosch oder Siemens)

- Seriennummer und ggf. Fabrikationsdatum des Hausgerätes (sog. E-Nummer und FD-Nummer, diese Angaben finden sich auch auf dem Typenschild des Hausgerätes)
- Die eindeutige Kennung des im Hausgerät eingesetzten Netzwerkadapters (sog. MAC-Adresse).

Diese Daten werden im Rahmen der „Hausgerät verbinden“-Funktion für jedes verbundene Hausgerät Ihrem Nutzerkonto zugeordnet.

c. Geräte-Nutzungsdaten

Daten, die wir im Zusammenhang mit der Nutzung des Hausgerätes erheben und verwenden sind:

- Vorgenommene Grundeinstellungen, Programmauswahl und Programmeinstellungen am Hausgerät oder über die App,
- Gerätezustandsdaten wie Umgebungsbedingungen, Zustände von Bauteilen, Zustandsänderungen am Hausgerät (z.B. Wechsel des Betriebsmodus, Öffnen oder Schließen der Türe/des Frontpanels, Temperaturänderungen, Füllstände) und Zustandsmeldungen des Hausgerätes (z.B. Gerät ist überhitzt, Wassertank ist leer etc.). Die Geräte-Nutzungsdaten werden bezogen auf das jeweilige Hausgerät (siehe b.) auf dem Home Connect Server gespeichert und automatisch nach 10 Tagen wieder gelöscht.

d. App-Nutzungsdaten

App-Nutzungsdaten sind Daten aus Ihrer Interaktion mit der App wie z.B. verwendete Funktionalitäten der App, Klickverhalten in Bezug auf Bedienelemente der App, Auswahl in Dropdown-Menüs, Einstellungen von On/Off-Schaltern. Siehe dazu auch unten 5.

2. Verwendungszwecke

Die genannten Datenkategorien nutzen wir – und soweit dafür Ihr Einverständnis erforderlich nur mit Ihrem Einverständnis – zur

- Bereitstellung der Funktionalitäten der App sowie der über die App angebotenen Dienste (1.a.-c.)
- Beseitigung von Störungen (1.b. und c.)
- Verbesserung der Benutzerfreundlichkeit der App (1.d.).
- Verbesserung unseres Produkt- und Dienstleistungsangebots, insbesondere im Hinblick auf nicht genutzte Programme bzw. häufig genutzte Programme und sonstige Funktionen der App und des Hausgerätes (1.c. und d.)

3. Steuerung der Datenverarbeitung

a. Konnektivität Ihres Hausgerätes

Über die App können Sie die Konnektivität Ihres Hausgerätes steuern:

- Sie können bei Bedarf die Verbindung zum Home Connect Server gesondert nach Hausgerät trennen (Menüpunkt Einstellungen ◇ Verbindungseinstellungen) mit der Folge, dass die
 - Geräte-Nutzungsdaten (1.c.) nicht mehr an Home Connect Server übermittelt werden,
 - gewisse Funktionalitäten der App nicht mehr zur Verfügung stehen, insbesondere eine Bedienung des Hausgerätes außerhalb der Reichweite des Wi-Fi-Netzes auch bei bestehender Internet-Datenverbindung nicht mehr möglich ist.
- Sie können bei Bedarf die Wi-Fi-Verbindung gesondert nach Hausgerät ausschalten (Menüpunkt Einstellungen ◇ Verbindungseinstellungen) mit der Folge, dass
 - Geräte-Nutzungsdaten (1.c.) nicht mehr an Home Connect Server übermittelt werden,
 - eine Bedienung des Gerätes nur noch am Gerät selbst möglich ist, nicht mehr aber über die App.

b. Nutzerkonten und lokale App-Daten

Über die App können Sie Ihre Nutzerkonten steuern und lokal vorgehaltene App-Daten löschen.

- Sie können Ihr Nutzerkonto löschen („Einstellungen“ ◇ „Mein Konto“ ◇ „Benutzerkonto löschen“). Dies hat zur Folge, dass die
 - Verknüpfung Ihres Hausgerätes mit Ihrem Nutzerkonto gelöscht wird,
 - Ihr Hausgerät keine Geräte-Nutzungsdaten mehr an den Home Connect Server sendet, soweit keine weiteren Nutzerkonten mit dem Hausgerät verknüpft sind (siehe oben 1.b.). Auf dem Home Connect Server vorhandene Nutzungsdaten werden nach spätestens 10 Tagen gelöscht (siehe oben 1.c.)
- Durch das Löschen der App entfernen Sie auch alle lokal gespeicherten nutzerbezogenen Daten.

c. Werkzustand des Hausgerätes

Sie können Ihr Hausgerät am Hausgerät in den Werkzustand versetzen. Dies hat zur Folge, dass

- durch das Zurücksetzen der Netzwerkeinstellungen die Verbindung des Hausgerätes mit dem Home Connect Server getrennt wird,
- die Verknüpfung des Hausgerätes mit zuvor verknüpften Nutzerkonten gelöscht wird (erfordert die Verbindung des Hausgerätes mit dem Internet) und somit Ihr Hausgerät in der App auch nicht mehr angezeigt wird,

Für das Zurücksetzen Ihres Hausgerätes in den Werkzustand konsultieren Sie bitte die Gebrauchsanweisung Ihres Hausgerätes.

4. Übermittlung oder Weitergabe Ihrer Daten an Dritte

Zur Realisierung der App und der darüber angebotenen Dienstleistungen arbeiten wir mit verschiedenen Dienstleistern zusammen. Soweit wir diese Dienstleister zur streng weisungsgebundenen Datenverarbeitung als Auftragsdatenverarbeiter verpflichtet haben, bedarf eine Datenverarbeitung durch diese Dienstleister keiner Einwilligung durch Sie. Die entsprechenden Dienstleister können ihren Sitz auch im Ausland haben, weshalb auch eine grenzüberschreitende Weitergabe der Daten ins Ausland möglich ist.

In anderen Fällen, soweit für die Weitergabe Ihrer personenbezogenen Daten an Dienstleister aus datenschutzrechtlichen Gründen Ihre Einwilligung erforderlich ist, informieren wir Sie gesondert und übermitteln Ihre Daten nicht ohne Ihre vorherige Einwilligung.

5. Erfassung der App-Nutzung

Die App bietet die Möglichkeit zur Erfassung von App-Nutzungsdaten (siehe oben 1.d.) und setzt dazu den Dienst Adobe Analytics von Adobe Systems Software Ireland Limited, 4–6 Riverwalk, Citywest Business Campus, Dublin 24, Republic of Ireland (nachfolgend „Adobe“) ein.

Soweit die Funktion „Nutzungsdaten erfassen“ aktiviert ist, werden App-Nutzungsdaten an einen Server von Adobe gesendet, die eine Analyse der Benutzung der App durch Sie ermöglichen (siehe oben 1.d.). Die App-Nutzungsdaten werden in der Regel an einen Server von Adobe in den USA übertragen und dort gespeichert. Für diese App wurde die IP-Anonymisierung aktiviert, so dass die von Ihnen verwendete IP-Adresse zuvor gekürzt wird. Im Auftrag von Home Connect wird Adobe diese Informationen benutzen, um Ihre Nutzung der App auszuwerten und um Reports über die App-Aktivitäten für Home Connect zusammenzustellen. Die im Rahmen von Adobe-Analytics von Ihrem mobilen Endgerät übermittelte IP-Adresse wird ohne Ihr gesondertes Einverständnis nicht mit anderen Daten von Adobe oder von Home Connect zusammengeführt.

Sie können die Erfassung von App-Nutzungsdaten (inkl. Ihrer IP-Adresse) durch Adobe sowie die Verarbeitung dieser Daten durch Adobe steuern, indem Sie die Funktion „Nutzungsdaten erfassen“ aktivieren oder deaktivieren. Je nach Rechtslage in Ihrem Land kann es sein, dass die Funktion „Nutzungsdaten erfassen“ standardmäßig aktiv ist.

6. Fehlerberichte

Wir setzen HockeyApp (www.hockeyapp.net) zur Erstellung und Versendung von anonymen Fehlerberichten bei unplanmäßigem Verhalten der App, insbesondere bei Abstürzen, ein. Unser Dienstleister und Home Connect erhält Fehlerberichte nur nach Ihrer vorherigen expliziten Zustimmung. Ihre Zustimmung fragen wir vor jeder Übermittlung gesondert ab.

7. Datensicherheit

Um Ihre Daten bspw. vor Manipulationen, Verlust und unbefugtem Zugriff durch Dritte zu schützen, setzen wir technische und organisatorische Maßnahmen ein. Zu diesen Maßnahmen gehört u.a. der Einsatz modernster Verschlüsselungstechnologie, sichere Zertifikate, der Einsatz einer Firewall am Home Connect Server und der Passwortschutz der Home Connect App. Die Datensicherheit der Home Connect App ist von der TÜV Trust IT geprüft und zertifiziert worden. Unsere Sicherheitsmaßnahmen überprüfen und verbessern wir fortlaufend entsprechend des technologischen Fortschritts.

8. Änderung der Datenschutzerklärung

Im Zuge der Weiterentwicklung der App – unter anderem bedingt durch die Implementierung neuer Technologien oder die Einführung neuer Dienstleistungen – kann es erforderlich werden, diese Datenschutzerklärung anzupassen. Home Connect behält sich das Recht vor, die vorliegende Erklärung nach Bedarf zu ändern oder zu ergänzen. Home Connect wird immer die aktuelle Fassung der Datenschutzerklärung in der App hinterlegen, so dass Sie sich jederzeit über die aktuelle Fassung der Datenschutzerklärung informieren können.

9. Rechte und Kontaktinformationen

Erteilte Einwilligungen in einen zustimmungspflichtigen Datenumgang können Sie jederzeit mit Wirkung für die Zukunft widerrufen. Den Widerruf können Sie in der Regel ausüben durch die Betätigung der entsprechenden Einstellung innerhalb der App, im Übrigen durch die Nutzung der nachfolgend genannten Kontaktmöglichkeit.

Sollten Sie Fragen zum Datenschutz haben oder Ihre datenschutzrechtlichen Rechte auf Widerruf der Einwilligung, Auskunft, Berichtigung, Löschung oder Sperrung ausüben wollen, kontaktieren Sie uns über die in der App hinterlegten Kontaktinformationen.

Stand: September 2015

II. Export-Import-Standardvertrag

Vertragstext (Auszug)⁴²⁶:

Export-Import-Standardvertrag für personenbezogene Daten in Drittländer ohne angemessenes Datenschutzniveau gemäß Artikel 26 Abs. 2 EG-DSRL bzw. 46 DSGVO für den Datentransfer personenbezogener Daten an Stellen, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist, zwischen (Bezeichnung und Anschrift der Organisation – Exporteur in der EU) und (Bezeichnung und Anschrift der Organisation – Importeur im Drittstaat)

Die Parteien Vereinbaren folgenden Vertrag:

Artikel 1 Begriffsdefinition und Bezeichnungen

[...]

Artikel 2 Gegenstand und Geltungsbereich

- (1) Der vorliegende Vertrag soll für die in den Anhängen 1 und 2 näher bezeichnete Verarbeitung personenbezogener Daten sicherstellen, dass die Persönlichkeitsrechte der von dem Transfer in ein Drittland ohne angemessener Datenschutz betroffenen Personen geschützt werden, indem die innerhalb des Geltungsbereiches der EG-DSRL bzw. der DSGVO geltenden Schutzregeln zwischen dem Datenexporteur und dem Datenimporteur vereinbart werden.
- (2) Der vorliegende Vertrag zielt ausschließlich darauf ab, beim Datentransfer ein angemessenes Datenschutzniveau zu schaffen und ersetzt nicht die darüber hinaus gehende Zulässigkeitsprüfung durch den Exporteur als verantwortliche Stelle. Der Exporteur garantiert im Falle von Transfers deren Zulässigkeit.

Artikel 3 Einzelheiten des Transfers

[...]

Artikel 4 Pflichten des Exporteurs

Der Exporteur garantiert, dass

- a) Die Verarbeitung personenbezogener Daten einschließlich des Transfers entsprechend die Bestimmungen des anwendbaren, in Europa geltende Datenschutzrecht durchgeführt wurde und auch weiterhin durchgeführt wird;
- b) Alle nötigen rechtlichen Voraussetzungen für die Zulässigkeit des Transfers (z.B. die Durchführung der Mitbestimmung) vor Abschluss dieses Vertrages geschaffen sind;
- c) Er sich davon überzeugt hat, dass der Importeur seine Rechtspflichten aus dem vorliegenden Vertrag zu erfüllen in der Lage ist, dass dieser insbesondere hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag

⁴²⁶ Volltext siehe Schuler/Weichert, „Ein „Export-Import-Standardvertrag“ für den Drittauslands-Datentransfer“ (2016), *Datenschutz und Datensicherheit*, Heft 6, S. 388-390.

beschriebenen technischen und organisatorischen Maßnahmen und das Ergebnis der Prüfung schriftlich dokumentiert ist. Die Prüfung ist während des Bestehens des Vertrags in regelmäßigen Abständen zu wiederholen und ebenfalls zu dokumentieren;

- d) Er für die Einhaltung datenschutzrechtlicher Pflichten des Importeurs hinsichtlich der transferierten Daten sorgt und diesen während der gesamten Vertragsdauer anweist, wie die transferierten personenbezogenen Daten in Übereinstimmung mit den Bestimmungen des für ihn selbst anwendbaren, in Europa geltenden Datenschutzrechts zu verarbeiten sind, unabhängig davon, ob es sich um Daten der Transferkategorie 1 oder 2 handelt

[...]

Artikel 5 Pflichten des Importeurs

Der Importeur garantiert, dass

- a) Er die vom Exporteur transferierten personenbezogenen Daten entsprechend den Bestimmungen des für den Exporteur anwendbaren in Europa geltenden Datenschutzrechts und nur entsprechend dem in Anhang 1 vereinbarten Umfang und zu den dort vereinbarten Zwecken verarbeitet;

[...]

Artikel 6 Haftung und Sanktionen

- (1) Die Parteien vereinbaren, dass jede Person, die durch eine Verletzung der in Artikel 5 genannten Pflichten einen Schaden erlitten hat, berechtigt ist, vom Exporteur Schadenersatz für den erlittenen Schaden zu erlangen. Erfolgt durch die unzulässige Datenverarbeitung für eine Person eine schwerwiegende Beeinträchtigung ihres Rechts auf Datenschutz, so hat sie darüber hinausgehend gegenüber dem Exporteur einen Anspruch auf angemessene Geldentschädigung

[...]

Artikel 7 Drittbegünstigungsklausel

[...]

Artikel 8 Änderung des Vertrags

[...]

Artikel 9 Beendigung des Vertrags

[...]

Artikel 10 Anwendbares Recht

Für den vorliegenden Vertrag gilt das Recht des Mitgliedsstaats der EU, in dem der Exporteur niedergelassen ist, nämlich (XY).

Anhang 1 Beschreibung der Datenverarbeitung

Allgemeine Angaben (XY)

Datenexporteur und fachverantwortliche Stelle (XY)

Datenimporteur und fachverantwortliche Stelle (XY)

Bezeichnung des Verfahrens, das den Transfer erforderlich macht (XY)

Beschreibung der Verarbeitungsschritte des Verfahrens, in denen die transferierten Daten verarbeitet werden sollen (XY)

Beschreibung des generellen Zwecks, der durch den Transfer der Daten erreicht werden soll (XY)

Beschreibung der Daten (XY)

(Gruppe) pbz. Daten (XY)

Transferkategorie (1/2) (XY)

Bez. Arten pbz. Daten

Betroffene Personen / Gruppen (XY)

Zulässige Verarbeitungsschritte für diese Daten (Transferkategorie 1) Zulässiger Nutzungszweck für diese Daten (Transferkategorie 2) (XY)

Löschfrist (XY)

Behandlung bei Vertragsende (Rückgabe, Löschung, Entsorgung, Zeitpunkt) (XY)

Anhang 2 Technisch-organisatorische Maßnahmen

Der Importeur ergreift zur Verwirklichung der Schutzziele

- Datensparsamkeit
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Nichtverkettbarkeit
- Transparenz
- Intervenierbarkeit

Folgende technisch-organisatorische Maßnahmen gemäß Art. 17 EG-DSRL bzw. Art. 32 DSGVO:

Zur Absicherung des Transfers der Daten zwischen Exporteur und Importeur (XY)

Zum Schutz der Daten auf den Systemen und im Zuständigkeitsbereich des Importeurs (XY)

Zur sicheren Umsetzung aller in dem vorliegenden Vertrag getroffenen Vereinbarungen und resultierenden Pflichten (XY)

Anhang 3 Verträge zur Datenweitergabe durch den Importeur

[...]

Ob die Adressaten des Vorschlags wie die EU-Kommission, Unternehmen, die am Datentransfer zwischen Europa und Drittländern beteiligt sind, Datenschutzbehörden, Betriebsräte und Unternehmensverbände, den "Export-Import-Standardvertrag" als Grundlage für ihr weiteres Verhalten und Handeln nutzen, bleibt abzuwarten.

Zusammenfassend lässt sich sagen, dass die größten Probleme im Bereich der Rechtsdurchsetzung das Unwissen der Bürger ist, wie sie sich im Falle einer Datenschutzverletzung verhalten sollen, der Ressourcen- und Personalmangel in den Aufsichtsbehörden und zum Teil auch nicht zu Ende durchdachte gesetzliche Neuregelungen die zu erheblichen Unsicherheiten auf allen Ebenen führen.

Sachverständigenrat für Verbraucherfragen

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

Der Sachverständigenrat ist unabhängig und hat seinen Sitz in Berlin.

Vorsitzende des Sachverständigenrats ist Prof. Dr. Lucia Reisch.