Betrieblicher Datenschutz

Rechtshandbuch

Bearbeitet von
Prof. Dr. Nikolaus Forgó, Prof. Dr. Marcus Helfrich, Prof. Dr. Jochen Schneider, Marian Arning, Till Baer, Benno Barnitzke, Julia Bichlmaier, Dr. Christiane Bierekoven, Dr. Dirk Bieresborn, Prof. Dr. Georg Borges, Tobias Born, Isabell Conrad, Dr. Kai Cornelius, Dr. Eugen Ehmann, Dr. Sandro Gaycken, Dr. Uwe Günther, Dr. Nils Christian Haag, Dr. Oliver M. Habel, Dr. Stefan Hanloser, Dominik Hausen, Christian Hawellek, Joerg Heidrich, Dr. Michael Karger, Lars Klatte, JProf. Dr. Timoleon Kosmides, Dr. Sebastian Kraska, Dr. Jens Lütcke, Dr. Flemming Moos, Eckart C. Müller, Dr. Stephan Ott, Laura Schabmair, Hans-Hermann Schild, Prof. Dr. Fabian Schmieder, Jörn Schoof, Dr. Christian Schröder, Dr. Georg F. Schröder, Dr. Axel Spies, Dr. Christoph Wegener, Dr. Hans Peter Wiesemann, Dr. Anna Zeiter

2. Auflage 2017. Buch. LX, 1332 S. In Leinen
ISBN 978 3 406 69541 4
Format (B x L): 16,0 x 24,0 cm

deutsche Aufsichtsbehörden federführend, soweit eine deutsche Niederlassung als Hauptniederlassung beteiligt ist.[317]

Unter geringeren Voraussetzungen besteht keine Zuständigkeit deutscher Aufsichtsbehörden. Insbesondere reicht die **Ausrichtung** der Tätigkeit auf den deutschen Markt als solche nicht aus. **268**

3. Unternehmen mit (Haupt-)Niederlassung im Drittstaat. Für Datenverarbeitung von Unternehmen mit einziger Niederlassung oder Hauptniederlassung in einem Drittstaat sind europäische Aufsichtsbehörden unter den Voraussetzungen des Art. 55 Abs. 1 DS-GVO zuständig.[318] **Deutsche Aufsichtsbehörden** sind dann international zuständig, wenn die Datenverarbeitung auch von einer deutschen Niederlassung gesteuert wird[319] oder wenn aufgrund von Auswirkungen ein hinreichender Bezug zum Inland besteht.[320] Darüber hinaus können deutsche Aufsichtsbehörden auch zuständig sein, wenn die Tätigkeit auf den deutschen Markt ausgerichtet ist.[321] **269**

Soweit mehrere europäische Aufsichtsbehörden zuständig sind, sind diese grundsätzlich unabhängig voneinander. Die Regeln über die federführende Zuständigkeit greifen mangels Hauptniederlassung in der EU nicht.[322] Die Aufsichtsbehörden können jedoch nach Art. 60, 61 DS-GVO **kooperieren.** **270**

---

317 → Rn. 229 ff.
318 → Rn. 197 ff.
319 → Rn. 200 i. V. m. 166 ff.
320 → Rn. 201 ff.
321 → Rn. 205 i. V. m. 130 ff., 177 ff.
322 → Rn. 238.

Kapitel 4. Internationaler Datenschutz

Übersicht

Literatur: *Bamberger/Mulligan,* Privacy On the Ground, 63 Stan. L. Rev. 352 (201); *BNA,* World Data Protection Report 11/08; *Crovitz,* The Right to Privacy from Brandeis to Flickr, Wall Street Journal v. 27.7.2011, abrufbar unter http://online.wsj.com/article/SB10001424052311190355490457646199072988075 6.html (Stand: 3/2016); *Fuchs,* Personenbezogene Daten zwischen EU und den USA, BB 2015, 3074; *Gola,* Die Entwicklung des Datenschutzrechts im ersten Halbjahr 2015, NJW 2015, 2628; *Greenleaf/Mc-Leish,* Hong Kong's privacy enforcement: Issues exposed, but powers lacking, PL&B International (Ausgabe 116) April 2012, 25; *ders.,* International DP agreements after the GDPR and Schrems, PL&B 2/2016, p. 12; *Harper/Spies,* A Reasonable Expectation of Privacy? Data Protection in the United States and Germany, Studie des American Institute of Contemporary German Study (AICGS) Nr. 22 (2006), abrufbar unter http://www.aicgs.org/publication/a-reasonable-expectation-of-privacy-data-protection-in-the-united-states-and-germany/ („AICGS") (Stand: 3/2016); *Hartmann* (Hrsg.), Internationale E-Discovery und Information Governance („IED"), Berlin 2011; *Korff* (Hrsg.), Vergleichsstudie: Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments, Mai 2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_hallenges/final_report_country_report_B4_india.pdf (Stand: 3/2016); *Kuner,* International Data Privacy Law, Oxford Press; *Linkomies,* From Safe Harbor to Privacy Shield_ Where are we now?, PL&B 2/2016, 3: *dies.,* Asia Pacific is high on the privacy heat-map, PL&B 6/2015, 20; *Renuncio-Mateos,* Latin America: DP Legislative Developments Roll on, PL&B International, Februar 2011, 17; *Ribeiro,* India Exempts Outsourcers From New Privacy Rules, Business Center vom 24.8.2011; *Schmidt/Weichert,* Datenschutz, Grundlagen, Entwicklungen und Kontroversen, 2012; *Spies,* USA: Neue Datenschutzvorschriften auf dem Prüfstand, ZD 2011, 12; *ders.,* USA: Regierung stellt neue Datenschutz-Prinzipien vor – Consumer Privacy Bill of Rights, ZD Focus 4/2012, VI; *ders.,* EU/U. S. Data Transfers: New Privacy Shield, How does it look and what happens next?, 5.2.2016, AICGS Publikationen; *ders.,* Anmerkungen zum Schrems-Urteil des EuGH, ZD 2015, 549; *Spies/Stutz,* Microsoft als Initialzünder für mehr Datenschutz in den USA?, DuD 2006, 170; *Waters,* APEC and OECD privacy developments PL&B International, (Ausgabe 116) April 2012, 28; *Weidner-Braun,* Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, 2012; *Working Party* (Artikel-29-Datenschutzgruppe), Stellungnahme: Opinion on the level of protection of personal data in New Zealand, 11/2011; *dies.,* Stellungnahme: Opinion on the level of protection of personal data in the Eastern Republic of Uruguay, 6/2010.

Spies

A. Einführung

Der internationale Datenschutz spielt in einer von der **Globalisierung** getriebenen Wirtschaft eine immer wichtigere Rolle und wird teilweise von international agierenden Unternehmen als Standortfaktor angesehen. Der Leitgedanke des internationalen Datenschutzes ist, dass der Datenschutz nicht an der Grenze des Landes endet und die nationalen Vorschriften nicht durch das Verlagern der Daten in unsichere Länder ausgehebelt werden dürfen. Neuere Bestrebungen u. a. in **Russland** gehen gar soweit, dass die Daten russischer Staatsbürger in Russland abgespeichert werden dürfen. Eine Verlagerung der Daten darf aber auch in anderen Fällen nicht dazu führen, dass die Souveränität des Ziellandes für Daten unter seiner Jurisdiktion vom Ausgangsland nicht anerkannt wird. Das Problem ist, dass die Konzeptionen des Datenschutzes nicht auf der ganzen Welt deckungsgleich sind. Nicht jedes Land folgt den strengen Vorgaben des EU-Datenschutzes,[1] wenngleich die EU-Kommission einen starken Exportwillen ihres Datenschutzregimes entwickelt hat. Viele Staaten gehen eigene Wege, wie z. B. über freiwillige Industriestandards und Vereinbarungen mit dem Betroffenen, die weit mehr Spielraum gewähren als es die Datenschützer und Unternehmen aus Europa gewöhnt sind. **1**

Etliche Unterschiede bestehen zwischen den Konzeptionen der **USA** auf der Grundlage der „Privacy" und dem europäischen Datenschutz. So wird der Begriff „data protection" in den USA in erster Linie auf die physische Sicherheit der Daten angewandt. Es gibt eine Reihe von Konfliktfeldern zwischen den USA und der EU, z. B. die Übermittlung von Passagierdaten, die Datensammlung in den USA zu Spionagezwecken,[2] der Zugriff auf Daten beim Cloud Computing,[3] die Datenübermittlung aus der EU für Gerichtsverfahren in den USA.[4] Auf der US-Seite hegen manche die Befürchtung, dass die EU ihr Datenschutzkonzept auf möglichst viele Länder ausdehnen will (z. B. nach Südafrika und Brasilien – für beide ist die EU ein sehr wichtiger Handelspartner). Nach der *Schrems*-Entscheidung des EuGH,[5] die zur Nichtigkeit des „Safe Harbors" führte, setzte die politische Debatte um einen neuen EU/US „Privacy Shield" ein, der seit dem 1.8.2016 bald für die Industrie nutzbar ist. Allerdings gehen manche Vorgaben für die auf der neuen Privacy Shield Liste registrierten Unternehmen über Safe Harbor hinaus, sodass fraglich ist, ob sich viele US-Unternehmen als Datenimporteure auf die neue Liste setzen werden. Es ist durchaus möglich, dass sich der EuGH mit den Regeln über den Privacy Shield befassen wird, was zu weiterer Rechtsunsicherheit bei den beteiligten Unternehmen führen dürfte. **2**

In **Afrika** setzen neuerdings auch in Ländern neben Südafrika Bestrebungen nach einem höheren Datenschutzniveau ein. Die Afrikanische Union verabschiedete im Jahre 2014 eine Konvention zur digitalen Sicherheit und zum Datenschutz („Convention on Cyber Security and Personal Data Protection 2014")[6] mit einem Mo- **3**

[1] → *Spies*, V.2.
[2] → *Spies*, V.2 Rn. 18 f.
[3] Cloud Computing, → VI.5.
[4] E-Discovery, → *Spies*, XII.2.
[5] *EuGH*, Urt. v. 6.10.2015 – C-362/14, Rn. 37 ff., ZD 2015, 549 m. Anm. *Spies*.
[6] http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf (Stand: 3/2016).

dellgesetz zum Datenschutz. Einige kleine afrikanische Länder, haben daraufhin Datenschutzgesetze verabschiedet.

4 In **Asien** findet man es eine große Bandbreite von Datenschutzkonzepten – manche Länder decken nur strafrechtliche Teilaspekte des Datenschutzes ab, manche asiatische Jurisdiktionen, wie Hongkong oder Singapur, haben umfangreiche Gesetze und Vorschriften, die nahe an das EU-Konzept herankommen. In allen Ländern stellt sich die Frage, ob die im Prinzip bestehenden Vorschriften auch tatsächlich durchgesetzt werden und die Daten aus Europa sicher sind. Ein EU-äquivalentes Datenschutzniveau streben nun **Japan** und **Südkorea** an. Auch innerhalb Europas ist der Datenschutz keineswegs vereinheitlicht. Die **Schweiz** als Nichtmitglied der EU hat das EU-Datenschutzkonzept (mit einigen Besonderheiten) übernommen.[7] Auch **Russland** hat das seit 2006 existierende Bundesdatenschutzgesetz zum 1.7.2011 reformiert und den EU-Regeln weiter angenähert.[8] Neuere Entwicklungen in Russland fordern Unternehmen sogar auf, Daten russischer Bürger in Russland zu speichern („Localisation Law").[9] Die **Türkei** hat am 7.4.2016 ein neues Datenschutzgesetz veröffentlicht, das sich kaum überraschend bei der Definition der wichtigsten Konzepte und Rechtsbegriffe wie data controller, data processor, sensitive data usw. an die EU-VO anlehnt.[10] Ein Datentransfer aus der Türkei ins Ausland bedarf danach der Zustimmung eines neuen Datenschutzrates.

B. Nordamerika

I. USA

5 Die USA sind seit vielen Jahren der wichtigste Handelspartner der EU. Entsprechend groß ist der Datenexport und -import. Aufsehenerregende Fälle, in denen es zu einem Bruch der Datensicherheit bei Unternehmen gekommen ist (Sony, Epsilon, Citigroup) sowie eine sehr kritische und besorgniserregende Artikelserie des Wall Street Journal „What They Know" über die Online-Datensammlung in den USA[11] könnten den Eindruck erwecken, dass es in den USA keinen Schutz der persönlichen Daten gibt oder dass jedenfalls dieser Schutz nicht durchgesetzt wird. Diese Entwicklung

[7] Botschaft vom 19.2.2003 zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8.11.2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung: http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20030016, sowie Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung: http://www.admin.ch/ch/d/ff/2003/2167.pdf (Stand: 4/2016).

[8] Russisches Bundesgesetz No 261-FZ vom 25.7.2011 – mit zahlreichen Änderungen des Bundesgesetzes „zakon o personoalych dannych" – rückwirkend zum 1.7.2011, http://www.consultant.ru (Stand: 7/2013). Relevant aus Sicht eines ausländischen Unternehmens ist insbesondere der Art. 12 dieses neuen Gesetzes mit strengeren Vorschriften zur internationalen Datenübermittlungen und zu einer neuen Liste zu Ländern außerhalb der Konvention des Europarates zum Schutz personenbezogener Daten von 1981, die aus russischer Sicht ein angemessenes Datenschutzniveau bieten. Russland hat diese Konvention unterzeichnet.

[9] *Zimbler/Adreeva,* Privacy Law & Business Report 2016, S. 26 f.

[10] Hurriyet Daily News v. 7.4.2014, http://www.hurriyetdailynews.com/law-on-data-protection--approved-by-president.aspx?pageID=238&nid=97485 (Stand: 4/2016).

[11] http://online.wsj.com/public/page/what-they-know-digital-privacy.html (Stand: 7/2013).

endete schließlich in der viel diskutierten *Schrems*-Entscheidung in welcher der EuGH feststellte, dass zwischen der EU und den USA kein angemessenes Datenschutzniveau besteht[12] und den Stein für einen neuen „Privacy Shield" ins Rollen brachte. Im Wesentlichen bekräftigte der EuGH, dass das vereinbarte Datenschutzniveau unter „Safe Harbor" nicht ausreiche, um einen Datenexport in die USA zu ermöglichen. Es folgte ein rechtlicher Schwebezustand mit einer energisch geführten gesellschaftlichen Debatte. Die EU-Kommission veröffentlichte am 29.3.16 den Entwurf einer Entscheidung zur Angemessenheit des Datenschutzes nach dem Privacy Shield.[13] Besonders wichtig für die Industrie ist Annex 2 der veröffentlichen Dokumente, der ein ausführliches Schreiben mit detaillierten Ausführungen über die neue Privacy Shield-Liste enthält, auf der sich US-Unternehmen als Datenimporteure registrieren können (sog. Privacy Shield Framework Principles).[14] Die Privacy Shield-Liste ersetzt die Safe Harbor-Liste, geht aber mit einigen Bestimmungen über sie hinaus.[15]

In den USA gibt es ein allumfassendes Recht der informationellen Selbstbestimmung mit Verfassungsrang nicht, sondern „nur" ein verfassungsrechtlich verankertes Recht auf Privacy, das dem Bürger Abwehrrechte verleiht. Damit geht eine größere Rolle der Vertragsautonomie einher. Was unter **„Privacy"** zu verstehen ist, ist umstritten – eine allgemein passende deutsche Übersetzung für den Begriff gibt es nicht.[16] Die wohl wichtigste Entscheidung zur Privacy ist die berühmte Entscheidung des US Supreme Court *Roe v. Wade* aus dem Jahre 1973[17] zur Freiheit von staatlicher Einflussnahme bei Abtreibungen. Es gibt keine dem deutschen „Volkszählungsurteil" vergleichbare höchstrichterliche US-Entscheidung zu einem Datenschutzgrundrecht (Recht auf informationelle Selbstbestimmung), das auch Dritten entgegengehalten werden kann. Trotz einiger Ambitionen der **Federal Trade Commission (FTC)** existiert derzeit keine unabhängige Datenschutzbehörde des Bundes, die ein solches Recht im Privatrecht durchsetzt. Die Federal Trade Commission sieht sich gerne in der Rolle einer Datenschutzbehörde nach europäischer Auffassung, erfüllt aber die Kriterien in der RL 95/46/EG für die Unabhängigkeit und Spezialisierung einer Datenschutzbehörde nicht. Die FTC hat umfassende Aufgaben für den Kundenschutz (mit Ausnahme des Banken- und Versicherungsbereichs) allgemein und für die Fusionskontrolle. Sie besteht seit 75 Jahren und kann gegen „unfair or deceptive business practices affecting consumers"[18] vorgehen. Vermutlich wird die FTC unter der neuen Trump-Administration nur sehr zurückhaltend zugunsten der Privacy von Verbrauchern eingreifen.

---

[12] *EuGH,* Urt. v. 6.10.2015 – C-362/14, Rn. 37 ff., ZD 2015, 549 m. Anm. *Spies.*

[13] http://europa.eu/rapid/press-release_IP-16–433_en.htm (mit Anlagen – Schreiben der US-Regierung) (Stand: 4/2016).

[14] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf (Stand: 4/2016).

[15] Näher dazu → Rn. 11 ff.

[16] Zur Unterscheidung der Begriffe „Privacy" und „Datenschutz" *Spies/Stutz,* DuD 2006, 171. Der Rechtsbegriff „Privacy" ist gut 120 Jahre alt und beruht auf einem bahnbrechenden *Harvard Law Review*-Aufsatz von *Warren* und *Brandeis* im Jahre 1890. Schon damals ging es den Autoren um Grenzen für „neue Medien" – damals Lichtbilder als Neuerung in Zeitungen; siehe auch *Crovitz,* Wall Street Journal v. 27.7.2011: The Right to Privacy from Brandeis to Flickr, abrufbar unter http://online.wsj.com/article/SB10001424053111903554904576461990729880756.html (Stand: 3/2016) und *Daley/Esteban/Withers* in: Hartmann, IED, S. 284–288.

[17] *U. S. Supreme Court,* Entscheidung v. 22.1.1973, 410 U. S. 113 – Roe v. Wade.

[18] 15 U. S. C. § 45(a).

6 **Unfaire Praktiken** sind gegeben, wenn der Schaden für den Kunden (a) erheblich ist, (b) nicht durch andere Vorteile aufgewogen wird und (c) vernünftigerweise nicht zu vermeiden war.[19] „Täuschend" ist eine Geschäftspraktik dann, wenn die folgenden drei Elemente gegeben sind: (a) wahrscheinlich irreführende Geschäftspraktik oder Unterlassen, (b) Irreführung liegt aus der Sicht eines verständigen Verbrauchers vor, sowie (c) substantielle Auswirkungen oder Wahrscheinlichkeit, den Verbraucher in seinem Handeln bei einer Entscheidung für ein Produkt oder Dienst zu beeinflussen.[20]

7 Bei der Auslegung dieser Begriffe gerade im Bereich des Datenschutzes hat die FTC ein großes **Ermessen.** In letzter Zeit hat die FTC einige Verfahren gegen Unternehmen durchgeführt, die trotz eines gesetzlichen Gebotes keine oder fehlerhafte **Datenschutzerklärungen** (privacy policies) im Geschäftsverkehr benutzt haben. Die FTC geht derzeit auch sehr gezielt gegen Verletzungen des Datenschutzes von Kindern (COPPA) durch Mobilfunk-Downloads (Apps) vor.[21]

8 Das neue Privacy Shield-Maßnahmenpaket wird die Rolle der FTC vermutlich stärken, da die Behörde in die Streitbelegung über EU-Daten und in die Zusammenarbeit mit den europäischen Datenschutzbehörden enger eingebunden wird.

9 Ein Teil der Datenschutzaufgaben wird nicht von der FTC wahrgenommen, sondern vom **US-Handelsministerium** (es überwacht die Privacy Shield Framework Principles – → *Spies*, V.2, auch m. w. N. zum NSA-Überwachungsskandal in → Rn. 18 f.) für Datenübermittlungen aus der EU/EEA und der Schweiz in die USA. Seit dem 21.7.2011 ist für den Kundenschutz im Finanzbereich (und damit den Datenschutz in diesem Bereich) das neugeschaffene **Consumer Financial Protection Bureau** zuständig. Telekommunikationsanbieter (Carrier) fallen ebenfalls nicht unter die Jurisdiktion der FTC, sondern der **Federal Communications Commission** (FCC).[22] Damit ist es für Carrier wie schon nach den Safe Harbor Principles nicht möglich, soweit Verkehrs- und Kundendaten betroffen sind, sich unter dem neuen Privacy Shield Framework registrieren zu lassen.[23] Die Carrier unterliegen gleichwohl strengen Regeln der FCC für die Verarbeitung von Kundendaten.[24]

10 Nach der gefestigten richterlichen Auslegung des Vierten Verfassungszusatzes (Schutz vor Durchsuchungen)[25] gibt es in den USA **keine feste Zweckbindung** der

---

[19] 15 U. S. C § 45(n); see also FTC Policy Statement on Unfairness (17.12.1980), abrufbar unter http://www.ftc.gov/bcp/policystmt/ad-unfair.htm (Stand: 3/2016).

[20] FTC Policy Statement on Deception (14.10.1983), abrufbar unter http://www.ftc.gov/bcp/policystmt/ad-decept.htm (Stand: 3/2016).

[21] Klageschrift: http://www.ftc.gov/os/caselist/1023251/110815w3cmpt.pdf (Stand: 3/2016).

[22] Die FCC am 1.4.2016 ein groß angelegtes Konsultationsverfahren zur Datenverarbeitung durch Anbieter von Internetzugang auf den Weg gebracht; siehe *Spies*, MMR Aktuell 2016, 37715.

[23] Privacy Shield Framework (Annex II: http://europa.eu/rapid/press-release_IP-16–433_en.htm), Abs. I 2.

[24] Am 7.12.2007 veröffentlichte die FCC eine neue Regelung für den Umgang mit Customer Proprietary Network Information (CPNI). Diese Regelungen betreffen Digital Phone Service der Kunden und Informationen über ihre Digital Phone-Pakete und Call Detail Records (CDR). Nach dem CPNI Vorschriften gibt es zahlreiche Beschränkung, wie die Carrier diese Informationen (wie Datum, Uhrzeit, Dauer, Zielnummer) verwenden dürfen. Sie müssen regelmäßig der FCC gegenüber zertifizieren, dass die CNI-Regeln intern auch umgesetzt werden. Im Einzelnen siehe http://www.fcc.gov/guides/protecting-your-telephone-calling-records (Stand: 4/2016). Die FCC will die CPNI-Regeln auf weitere Datensätze der ISP ausdehnen.

[25] „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon

Datenverarbeitung, sondern es kommt darauf an, welche vernünftigen Erwartungen der Verbraucher im Geschäftsverkehr hat, dass seine Daten nicht weitergegeben werden (reasonable expectation of privacy).[26] Bei der Auslegung spielt die Privacy Policy des Unternehmens eine wichtige Rolle. Die Einzelheiten bestimmt das Fallrecht der Gerichte.

Ein Beispiel: Ein Berufungsgericht in New Jersey hat entschieden, dass in einem Scheidungsverfahren ein Ehemann keine **reasonable expectation of privacy** habe, wenn die Ehefrau heimlich mit einem ins Auto-Handschuhfach eingebauten GPS-System dessen Fahrten verfolge. Das Argument: Die Fahrten fänden im öffentlichen Straßenraum statt und die Ehefrau habe eine finanzielle und rechtliche Verbindung zu dem Fahrzeug. Eine **reasonable expectation of privacy** des Ehemanns, dass der Aufenthaltsort des Fahrzeugs geheim bleibe, bestände nicht.[27] In Deutschland würde ein solches eigenmächtiges Vorgehen wohl zu einem Beweisverwertungsverbot führen.[28] Insgesamt haben die Privatautonomie des Einzelnen und seine Entscheidung, wie er über seine Daten verfügt, einen hohen Rang. Die einmal legal gewonnen Daten gelten im Prinzip als Handelsware (commodity).[29] **11**

In dem neuen **Privacy Shield Framework** findet man allerdings einige Beschränkungen, wonach der Empfänger von EU/EEA-Daten, der auf der neuen Liste registriert ist, die Betroffen über „die Zwecke informieren muss, für die es der personenbezogenen Daten über sie sammelt und nutzt."[30] Für eine Datennutzung, die „materiell unterschiedlich" (materially different) von dem oder den Zwecken ist, für welche die Daten ursprünglich mit Einwilligung der Betroffen gesammelt wurden, muss der Datenimporteur ein „Opt-out" zugunsten des Betroffenen vorsehen.[31] Dritte dürfen die nach dem Privacy Shield Framework übermittelten Daten nur für „begrenzte und spezifische Zwecke verarbeiten, die vereinbar mit der Zustimmung sind, die der Betroffene gegeben hat" und unter der weiteren Voraussetzung, dass dasselbe Datenschutzniveau wie nach dem Privacy Shield Framework weiter eingehalten wird.[32] Der neue Privacy Shield ist seit dem 1.8.2016 einsatzfähig. Die **12**

---

probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[26] Leitentscheidung des US Supreme Court siehe *Katz v. United States,* 389 U.S. 347 (1967). Die Consumer Privacy Bill of Rights von Präsident *Obama* vermeidet eine direkte Verknüpfung der Daten mit einer Zweckbindung: im Einzelnen zu der Consumer Privacy Bill of Rights siehe *Spies,* ZD Focus 4/2012, VI und VII.

[27] http://www.nj.com/news/index.ssf/2011/07/judge_rules_use_of_gps_to_trac.html (Stand: 3/2016).

[28] Vgl. *OLG Oldenburg,* B. v. 20.5.2008 – 13 WF 93/08, NJW 2008, 3508 – Verletzung des Rechts auf informationelle Selbstbestimmung wegen unzulässiger Ermittlungsmethode.

[29] Eine gute Übersicht von *Harper* über das US-Privacy-Konzept findet man in *Harper/Spies,* A Reasonable Expectation of Privacy? Data Protection in the United States and Germany, Studie des American Institute of Contemporary German Study (AICGS) Nr. 22 (2006), abrufbar unter http://www.aicgs.org/publication/a-reasonable-expectation-of-privacy-data-protection-in-the-united-states-and-germany/ (Stand: 7/2013).

[30] Privacy Shield Framework Principles (http://europa.eu/rapid/press-release_IP-16–433_en.htm (mit Anlagen – Schreiben der US-Regierung) – (Stand: 4/2016) Abs. II (1) (a) (iv).

[31] Privacy Shield Framework Principles (http://europa.eu/rapid/press-release_IP-16–433_en.htm (mit Anlagen – Schreiben der US-Regierung) – (Stand: 4/2016) Abs. II (2) (a). Eine Ausnahme besteht, wenn ein Dritter die Daten erhält, der als Vertreter (Agent) des Datenimporteurs auftritt.

[32] Privacy Shield Framework Principles (http://europa.eu/rapid/press-release_IP-16–433_en.htm (mit Anlagen – Schreiben der US-Regierung) – (Stand: 4/2016) Abs. II (3) (a).

Artikel-29-Datenschutzgruppe hat einige Punkte des Konzeptes beanstandet.[33] Die EU-Kommission wird wohl im Sommer 2017 bei der jährlichen Review einige streitige Fragen mit der US Regierung schnellstmöglich klären (→ *Spies*, V.2). Es ist derzeit noch nicht abzusehen, ob der EuGH das Privacy Shield Framework als gegen EU-Recht verstoßend für nichtig erklären wird.

II. Einige Konsequenzen

13

Einige wichtige US-Gesetze zum Schutz der Privacy:[34]
- Verarbeitung medizinischer Daten (HIPAA, Healthcare Insurance Portability Accountability Act, 1996),
- Verarbeitung von Bankdaten (Gramm-Leach-Bliley-Act, 1999),
- Sicherstellung korrekter Kreditreporte und zum Schutz vor Identitätsdiebstahl (FACT, Fair and Accurate Credit Transaction Act, 2003),
- Verarbeitung personenbezogener Daten online für Kinder unter 13 Jahren (COPPA, Children's Online Privacy Protection Act, 2000),
- Telekommunikationsdatenverarbeitung (Communications Act 1996 und FCC-Regeln zu CPNI, Customer Proprietary Network Information),
- Electronic Communications Privacy Act (ECPA, 1986),
- Überwachungsmaßnahmen (Presidential Policy Directive (PPD) 28, 2014)

14 Die Abwehransprüche bei Verletzung der Privacy bestimmen sich weitgehend nach US-Deliktsrecht oder nach Spezialgesetzen.[35] Besonders sind hier zu nennen das **allgemeine Deliktsrecht** (general tort law), besonders die in den 1960er Jahren von *Prosser* entwickelten Privacy Torts.[36] Für Nicht-US-Bürger nimmt der US Judicial Redress Act eine besondere Stellung ein. Das Gesetz autorisiert das Department of Justice (DOJ) Bürgern ausländischer Herkunft ein Zivilverfahren unter dem Privacy Act von 1974 gegen US Regierungseinrichtungen zu eröffnen.[37] Dies war Teil des Maßnahmenpakets zur Umsetzung der Anforderungen der *Schrems*-Entscheidung.

15 Weiterhin großzügig bleibt der Zugang der US-Sicherheitsbehörden zu persönlichen Daten aller Art. Legislatorisch wird dies durch Sec. 702 FISA Amendments Act, EO 12333, section 215 USA Patriot Act und Sec. 215 USA Freedom Act of 2015 sichergestellt. Die Gesetze unterscheiden sich im Wesentlichen in der Art der Daten, die beschafft werden, und je nach Staatsbürgerschaft, ob eine gerichtliche Verfügung für die Datenbeschaffung notwendig ist. Unter dem neu gefassten Free-

[33] Opinion 1/2016 on the EU-US Privacy Shield draft adequacy decision (WP 238), 13.4.2016: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en. pdf.

[34] Vgl. zuletzt die Analyse in dem Entscheidungsentwurf der EU-Kommission zur Angemessenheit des neuen Privacy Shield Framework vom 29.3.2016 (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf) und das Schreiben des Office of the Director of the National Intelligence Office – General Counsel vom 22.2.2016 zur Anwendung des Presidential Policy Directive 28 (PPD).

[35] *Harper* in: Harper/*Spies*, AICGS, S. 35 f.

[36] Darunter u. a. das Eindringen in die Privatsphäre, das öffentliche Verbreiten von die Privatsphäre berührenden Fakten, fehlerhafte Presseveröffentlichung und das Ausnutzen der Attribute einer Person zu kommerziellen Zwecken.

[37] https://www.congress.gov/bill/114th-congress/house-bill/1428 (Stand: 4/2016).