CR
COMPUTER UND RECHT

Zeitschrift
für die Praxis
des Rechts
der Informations-
technologien

Verlag Dr. Otto Schmidt Köln

www.cr-online.de

Niko Härting

Datenschutzreform in Europa: Einigung im EU-Parlament

Kritische Anmerkungen

Der LIBE-Ausschuss des Europäischen Parlaments (Committee for Civil Liberties, Justice and Home Affairs) hat am 21.10.2013 eine Vielzahl von Änderungsanträgen beschlossen zu dem Vorschlag für eine Grundverordnung zum Datenschutz (DS-GVO), den die EU-Kommission am 25.1.2012 veröffentlicht hat. Die Änderungsanträge sind von dem erklärten Bestreben getragen, den Schutz europäischer Bürger noch deutlicher zu verbessern, als dies von der EU-Kommission beabsichtigt ist. Nach einem kurzen Überblick (I.) geht der Beitrag auf wesentliche Kritikpunkte (II.) wie die Vernachlässigung der Bürgerrechte, der mittelständischen Wirtschaft, der Kommunikationsfreiheit, der Pseudonymität und Anonymität, des Prinzips der Accountability und des Rechtsschutzes ein, bevor er mit einem Ausblick (III.) schließt.

I. Überblick

Der LIBE-Ausschuss des Europäischen Parlaments (Committee for Civil Liberties, Justice and Home Affairs) hat am 21.10.2013 eine Vielzahl von Änderungsanträgen beschlossen[1] zu dem Vorschlag für eine Grundverordnung zum Datenschutz (DS-GVO), den die EU-Kommission am 25.1.2012 veröffentlicht hat[2]. Die Änderungsanträge sind von dem erklärten Bestreben getragen, den Schutz europäischer Bürger noch deutlicher zu verbessern, als dies von der EU-Kommission beabsichtigt ist[3].

Die Änderungen sind insgesamt zu umfangreich, um sie in einem kurzen Überblick angemessen darzustellen. Die nachfolgende Kritik beschränkt sich auf einige Kernpunkte. Dabei wird die bravouröse Leistung des *LIBE-Ausschusses* nicht verkannt. Der *LIBE-Ausschuss* hat es geschafft, in übersichtlicher Zeit eine Vielzahl von Änderungsvorschlägen nicht nur zu sichten sondern auch zu diskutieren und sich auf einen Kompromiss zu verständigen, der von einem breiten parlamentarischen Konsens getragen ist.

Zahlreiche Änderungen, die der *LIBE-Ausschuss* vorschlägt, sind zu begrüßen, können jedoch an dieser Stelle nicht im Einzelnen gewürdigt werden. So möchte der

▷ RA Prof. Niko Härting, HÄRTING Rechtsanwälte, Berlin.

1 Siehe Pressemitteilung des EU-Parlaments v. 21.10.2013, www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20131021IPR22706%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN den Compromise amendements on Articles 1-29 und den Compromise amendements on Articles 30- 91, beide v. 7.10.2013 und abrufbar unter: www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131021_1830.htm.

2 DS-GVO, KOM(2012) 11 endg.

3 *Josef Weidenholzer*, Innenausschuss stimmt über Datenschutz ab, Beitrag v. 19.10.2013, *www.weidenholzer.eu/2013/10/19/innenausschuss-stimmt-uber-datenschutzreform-ab/*.

Ausschuss auf die Schaffung eines neuen „Rechts auf Vergessenwerden" ebenso verzichten wie auf ein „Recht auf Datenportabilität". In Art. 23 DS-GVO wird der Versuch unternommen, den Grundsatz der „Privacy by Design" zu präzisieren. Zugleich werden in den Art. 12 ff. DS-GVO zahlreiche, ausführliche Vorschläge für eine Präzisierung von Informationspflichten entwickelt, die die Transparenz von Datenverarbeitungsvorgängen fördern. In Art. 22 DS-GVO wird das Profiling durch den *LIBE-Ausschuss* jedenfalls stimmiger behandelt, als dies in dem Vorschlag der *EU-Kommission* der Fall war, und Art. 30 DS-GVO bietet in der *LIBE*-Fassung deutlich verbesserte, weil konkretisierte Ansätze zur Regelungen von Anforderungen an die Datensicherheit. Uneingeschränkt zu begrüßen sind zu guter Letzt die zahlreichen Streichungen von Ermächtigungsbefugnissen der *EU-Kommission* zum Erlass von „delegierten Rechtsakten" und die Streichung aller Bestimmungen, die der *EU-Kommission* eine Letztentscheidungsbefugnis zuweisen bei Meinungsverschiedenheiten der verschiedenen nationalen Aufsichtsbehörden.

II. Kritikpunkte

Trotz aller deutlichen Fortschritte ist nicht zu verkennen, dass die LIBE-Vorschläge auch vielfältigen Anlass für deutliche Kritik liefern. Nur einige ausgewählte Kritikpunkte sollen nachfolgend behandelt werden.

1. Vernachlässigung der Bürgerrechte

Die DS-GVO soll ein europaweit einheitliches Datenschutzrecht schaffen – sowohl für den nicht-öffentlichen (privatwirtschaftlichen) als auch für den öffentlichen (behördlichen) Bereich. Dies scheint im *LIBE-Ausschuss* vergessen worden zu sein. Kein einziger nennenswerter Änderungsantrag befasst sich mit dem Schutz des Bürgers gegen den informationshungrigen Staat.

a) Zu enger Regelungsbereich

Im öffentlichen Bereich droht – jedenfalls für Deutschland – ein Ausverkauf der Bürgerrechte. Die DS-GVO deckt gerade einmal die Themenbereiche des Datenschutzes ab, die im BDSG geregelt sind. Das BDSG ist jedoch nur ein kleiner Bruchteil des Datenschutzrechts, das seit dem Volkszählungsurteil des BVerfG vor knapp 30 Jahren[4] rasant gewachsen ist und sich auf eine unübersehbare Vielzahl von Spezialgesetzen des Bundes und der Länder verteilt.

Als Beispiele seien das Meldegesetz und das Gesetz über ein Ausländerzentralregister genannt – Gesetze, die in jüngerer Zeit nach intensiven Debatten neu gefasst[5] bzw. geändert[6] wurden. Bei beiden Gesetzen handelt es sich um Gesetze zum Datenschutz im öffentlichen Bereich, die nicht von der geplanten EU-Richtlinie für den Datenschutz in den Bereichen Politik und Justiz[7] erfasst sind. Das Melderegister und das Ausländerzentralregister würden somit in den Anwendungsbereich der DS-GVO fallen, die keine der ausgefeilten Schutzregelungen der deutschen Spezialgesetze kennt.

4 BVerfG v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 ff.
5 Gesetz zur Fortentwicklung des Meldewesens (MeldFortG), BGbl. 2013, 1084 ff.
6 Gesetz zur Änderung des AZR-Gesetzes v. 20.12.2012, BGBl. I 2012, 2745 ff.
7 Richtlinie für die behördliche Datenverarbeitung zwecks Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung (KOM(2012) 10 endg.).

b) Sonderregelung für Sozialdatenschutz

Nur an einer Stelle bemüht sich der *LIBE-Ausschuss* zumindest darum, die Errungenschaften von dreißig Jahren spezialgesetzlicher Regulierung nicht vollständig aus dem Auge zu verlieren. In einem neuen Art. 82 a soll der Sozialdatenschutz behandelt werden („Processing in the social security context"):

„Die Mitgliedsstaaten können, in Übereinstimmung mit der Bestimmungen dieser Verordnung, Spezialregelungen erlassen zur Bestimmung der Voraussetzungen für die Verarbeitung personenbezogener Daten durch öffentliche und private Einrichtungen und Abteilungen im Zusammenhang mit sozialer Sicherheit, wenn dies im öffentlichen Interesse erfolgt."

Damit wäre gewährleistet, dass die Bestimmungen des SGB X zum Sozialdatenschutz[8] nicht vollkommen obsolet würden. Im Umkehrschluss verstärkt dies jedoch den Befund, dass der Datenschutz im Melde- und Ausländerrecht und in einer Vielzahl anderer spezialgesetzlich geregelter Materien nachhaltig geschwächt würde.

c) Vakuum durch Wegfall nationaler Spezialgesetze

Spezialgesetzliche Regelungen der EU-Mitgliedsstaaten bleiben nicht schon deshalb erhalten, weil es sich bei der DS-GVO lediglich um eine „Grund"-Verordnung handelt. Die Verordnung ist das probate europarechtliche Instrument, wenn es nicht – wie bei einer Richtlinie – um einheitliche Minimalstandards, sondern um eine vollständige Rechtsvereinheitlichung geht, vgl. Art. 288 AEUV. Die Ergänzung der „Grund"-Verordnung durch Spezialregelungen ist daher Aufgabe des europäischen Gesetzgebers und kann nicht den Gesetzgebern der Mitgliedsstaaten überlassen werden.

Die *EU-Kommission* hat den ergänzenden Regelungsbedarf zutreffend erkannt und möchte sich daher weitreichende Befugnisse zur Ergänzung der DS-GVO durch delegierte Rechtsakte und Durchführungsrechtsakte einräumen. Der *LIBE-Ausschuss* möchte diese Befugnisse größtenteils streichen. Dies ist zwar begrüßenswert, da dies einer rechtsstaatlich bedenklichen Machtfülle der *EU-Kommission* im Bereich des Datenschutzes[9] entgegenwirkt. Es entsteht durch die Streichungen jedoch ein Vakuum, das der *LIBE-Ausschuss* nicht zu füllen versteht.

2. Vernachlässigung der mittelständischen Wirtschaft

Im privatwirtschaftlichen (nicht-öffentlichen) Bereich würden die Bestimmungen der DS-GVO nicht nur „Internetgiganten" oder nur die „digitale Wirtschaft" treffen. Vielmehr müsste sich jeder Kleinunternehmer, der eine Kundendatenbank führt oder auch nur mit Kunden per E-Mail korrespondiert fragen, ob er bei der Datenverarbeitung die Bestimmungen der DS-GVO in vollem Umfang beachtet.

Den Belangen der mittelständischen Wirtschaft trägt der *LIBE-Ausschuss* unzureichend Rechnung und schafft nur wenige Erleichterungen. So soll für alle Unternehmen die Verpflichtung gelten, standardisierte Datenschutzerklärungen zu fertigen (Art. 13 a der *LIBE*-Vorschläge). Dies wird manchen Berater freuen, nicht jedoch die betroffenen Unternehmen, für die es ein schwa-

8 Vgl. §§ 67 – 85a SGB X.
9 Vgl. *Härting*, BB 2012, 459 f.

cher Trost ist, wenn es Art. 14 Abs. 4 (bb) der *LIBE*-Vorschläge kleinen Unternehmen und „Mikrounternehmen“[10] erlaubt, weitergehende Informationen nur dann zu erteilen, wenn ein Betroffener dies verlangt.

Die *EU-Kommission* wollte sich Befugnisse vorbehalten, auf dem Verordnungsweg Erleichterungen für mittelständische Unternehmen zu schaffen. Die entsprechenden Befugnisnormen (Art. 12 Abs. 6 und Art. 14 Abs. 7 zu Informationspflichten; Art. 22 Abs. 4 zur Auftragsdatenverarbeitung; Art. 33 Abs. 6 zur Datenschutz-Folgenabschätzung) möchte der *LIBE-Ausschuss* ersatzlos streichen. Satz 4 des Erwägungsgrundes 10 wird dadurch zum leeren Programmsatz:

„Um der besonderen Situation von Microunternehmen, kleinen und mittelgroßen Unternehmen Rechnung zu tragen, enthält diese Verordnung eine Reihe von Ausnahmen (‚a number of derogations‘)“

3. Fixierung auf die Online-Wirtschaft

Die Aufmerksamkeit des *LIBE-Ausschusses* richtet sich nahezu ausschließlich auf den Online-Datenschutz. Die zum Teil äußerst detailversessenen Vorschläge orientieren sich an (großen) Unternehmen, die über das Internet Informationen sammeln und verarbeiten. Unternehmensinterne Datenverarbeitungsprozesse erreichen dagegen nur selten das *LIBE*-Blickfeld.

a) Ampelsystem für Intensität einer Datenverarbeitung

Besonders deutlich wird die Internet-Fixiertheit der Vorschläge an Art. 13 a DS-GVO. Dort wird der begrüßenswerte Versuch unternommen, eine Norm zu formulieren, die nach dem „Ampelprinzip“ Verbrauchern in einfacher Weise erklärt, in welcher Intensität eine Informationsverarbeitung erfolgt. Dabei geht es um sechs Kategorien (Art. 13 a Abs. 1):

„a) ob personenbezogene Daten gesammelt werden über das Minimum hinaus, das für jeden einzelnen Zweck der Verarbeitung notwendig ist;

b) ob personenbezogene Daten vorgehalten (‚retained‘) werden über das Minimum hinaus, das für jeden einzelnen Zweck der Verarbeitung notwendig ist;

c) ob personenbezogene Daten verarbeitet werden für andere Zwecke als den Zweck, für den sie gesammelt wurden;

d) ob personenbezogene Daten verbreitet (‚dissemianted‘) werden an kommerzielle Dritte;

e) ob personenbezogene Daten verkauft oder vermietet werden;

f) ob personenbezogene Daten vorgehalten (‚retained‘) werden in verschlüsselter Form.“

b) Praktikabilität für kleine Einzelhändler?

Ein solches „Ampelsystem“ erscheint für Online-Dienste wie *Facebook, Google* und Co. vorstellbar. Ob dies jedoch auch für komplexe Datenverarbeitungssysteme einer Versicherung oder für die Kundendatenbank eines Pizza-Lieferdienstes gelten sollte, ist zweifelhaft, zumal es keinerlei Ausnahmen oder Erleichterungen für Kleinunternehmen geben soll. Wieso soll sich ein kleiner (Offline-)Buchhändler der Mühe unterziehen, seine Kunden nicht nur (auf Anfrage) über alle gespeicherten Daten gem. Art. 14 DS-GVO zu unterrichten, sondern darüber hinaus spezialisierte Berater mit der Anfertigung einer „standardisierten Datenschutzerklärung“ beauftragen? Was für *Amazon* recht ist, ist für den kleinen Einzelhändler noch lange nicht billig.

4. Erweiterung der Kommunikationsverbote

Der *LIBE-Ausschuss* hält am Verbotsprinzip eisern fest (Art. 6 DS-GVO). Begreift man den Datenschutz unter den Gegebenheiten der digitalen Informations- und Kommunikationstechnik als – zwangsläufige – Kommunikationsregulierung[11], bedeutet dies ein europaweites Kommunikationsverbot (mit Erlaubnisvorbehalt).

a) Grundrechtlicher Vorrang statt Abwägung

Dies ist problematisch, da sowohl der Datenschutz als auch die Kommunikationsfreiheit Grundrechte sind (Art. 8 und 11 Grundrechte-Charta). Dies verbietet eine faktische „Voreinstellung“, die dem Datenschutz im Zweifel den Vorrang einräumt[12]. Im Verhältnis der beiden Grundfreiheiten darf es keine „Privacy by Default“ geben.

b) Definition „personenbezogene Daten“

Das Verbotsprinzip wird durch die *LIBE*-Vorschläge verschärft, indem die Definition des Begriffs personenbezogener Daten erheblich erweitert wird – in einer Weise, die eines der Ausschussmitglieder, wie folgt, beschreibt:

„Breite Definition von personenbezogenen Daten: Alle Daten sind schützenswert.“[13]

Dem Abgeordneten ist zuzustimmen: Ob ein einzelnes Datum die Persönlichkeitsrechte eines Bürgers gefährden kann, lässt sich nicht feststellen, ohne dass man den Kontext eines Datenverarbeitungsprozesses kennt[14]. Dies spricht für einen sehr weiten Anwendungsbereich des Datenschutzrechts, keineswegs jedoch dafür, ohne Rücksicht auf den jeweiligen Kontext jedwede Datenverarbeitung zu verbieten[15]. Dass eine datenschutzrechtliche Regulierung auch ohne flächendeckende Verbote vorstellbar ist, ist nicht zu leugnen[16].

Art. 4 Abs. 2 DS-GVO sieht nach den *LIBE*-Vorschlägen eine denkbare weite Definition des Personenbezugs von Daten (und damit der Reichweite des Verbotsprinzips) vor:

„‚Personenbezogene Daten‘ sind alle Informationen, die sich auf eine identifizierte oder idenifizierbare Person (‚Datensubjekt‘) beziehen; eine identifizierbare Person ist eine Person, die identifiziert werden kann, direkt oder indirekt, insbesondere unter Bezugnahme auf ein Identifikationsmerkmal, wie beispielsweise einen Namen, eine Identifikationsnummer, Standortdaten, ein eindeutiges Zuordnungsmerkmal (‚unique identifier‘) oder ein oder mehr Faktoren, die spezifisch sind für die physische, psycho-

10 Zu den Definitionen vgl. Empfehlung der *EU- Kommission* v. 6.5.2003, 2003/361/EC.

11 Reporters Without Borders, „Internet Enemies Report 2012? v. 12.3.2012, S. 6 zur Überschrift „threat to net neutrality and online free speech“.

12 Vgl. in Bezug auf das deutsche Recht *Härting*, ITRB 2012, 109 (110 f.).

13 *Josef Weidenholzer*, Innenausschuss stimmt über Datenschutz ab, Beitrag v. 19.10.2013, *www.weidenholzer.eu/2013/10/19/innenausschuss-stimmt-uber-datenschutzreform-ab/*.

14 BVerfG v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 ff.

15 Vgl. *Härting*, BB 2012, 459 (463).

16 Vgl. *Schneider/Härting*, Alternativentwurf Stand Januar 2013, *www.schneider-haerting.de/2013/01/alternativentwurf-ds-gvo-fassung-januar-2013/*.

logische, genetische, seelische, wirtschaftliche, kulturelle oder soziale oder geschlechtliche Identität dieser Person."

Nach dieser Definition kommt es beispielsweise nicht mehr darauf an, ob sich Informationen lediglich auf ein Pseudonym (z.B. „Schatz28") beziehen, das keinerlei Rückschlüsse auf den „Klarnamen" zulässt[17]. Jede individualisierbare Information soll vielmehr als personenbezogen angesehen.

c) Absolutheit der Personenbezogenheit

Nicht weniger weitgehend soll es in Erwägungsgrund 23 Satz 2 und 3 heißen:

„Um zu bestimmen, ob eine Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, von denen es im gewöhnlichen Fall (‚reasonably') erwartet werden kann, dass sie entweder vom Verantwortlichen (‚controller') oder von einer beliebigen anderen Person (‚any other person') eingesetzt werden, um eine einzelne Person direkt oder indirekt zu identifizieren oder zu bestimmen (‚single out'). Um festzustellen, ob Mittel im gewöhnlichen Fall (‚reasonably') erwartet werden können, um eine einzelne Person zu identifizieren, sollten alle objektiven Faktoren berücksichtigt werden, wie beispielsweise die Kosten und die Zeit, die für die Identifizierung notwendig ist unter Berücksichtigung sowohl der verfügbaren Technologie zur Zeit der Verarbeitung als auch der technologischen Entwicklung."

Diese breite Formulierung stellt ersichtlich den Versuch dar, einen „absoluten" Begriff der Personenbezogenheit[18] zu zementieren und alle Schlupflöcher für eine Relativierung für alle Zeiten zu schließen. Verstärkt werden soll dies durch den Erwägungsgrund 24, der nach den *LIBE*-Vorstellungen lauten soll:

„Wenn Identifikationsmerkmale geliefert (‚provided') werden durch Geräte (‚devices'), Apps (‚applications'). Werkzeuge und Protokolle, wie beispielsweise IP-Adressen, Cookies (‚cookie identifieres') und RFID-Etiketten (‚tags'), ist diese Verordnung auf die Verarbeitung dieser Daten anwendbar, es sei denn die Identifikationsmerkmale beziehen sich nicht auf eine identifizierte oder identifizierbare natürliche Person."

Wie es nach den breiten Definitionen des Art. 4 Abs. 2 DS-GVO und des Erwägungsgrundes 23 noch denkbar sein soll, dass sich eine IP-Adresse dennoch keiner Person zuordnen lässt, ist schwer nachvollziehbar. Für IP-Adressen wäre der Streit um den Personenbezug[19] geklärt. Für IP-Adressen wäre das Datenschutzrecht nur dann nicht anwendbar, wenn sich lediglich ein Bezug zu einer juristischen Person bejahen lässt, für die das Datenschutzrecht nicht gilt[20].

5. Keine Anreize für Pseudonymität und Anonymität

Der *LIBE-Ausschuss* schlägt eine Definition pseudonymer Daten vor (§ 4 Abs. 2 a DS-GVO):

„Unter ‚pseudonymen Daten' sind personenbezogene Daten zu verstehen, die keinem einzelnen (‚specific') Datensubjekt zugeordnet werden können ohne die Nutzung zusätzlicher Informationen, solange diese zusätzlichen Informationen separat gehalten werden und technischen und organisatorischen Mitteln (‚means') unterliegen, die die Nicht-Zuordnung gewährleisten."

Dass der *LIBE-Ausschuss* – anders als die *EU-Kommission*[21] – den Begriff pseudonymer Daten verwendet, ist ein Fortschritt. Die Definition ist jedoch unglücklich, da sie nur zu Daten passt, die zunächst mit „Klarnamen" versehen waren und dann pseudonymisiert worden sind. Nur bei einer Pseudonymisierung entstehen die beiden Datenbestände (pseudonyme Daten/"Zusatzinformationen"), von denen die Definition ausgeht[22].

a) Pseudonymisierung und Pseudonymität

Bei der Netzkommunikation ist die Pseudonymisierung die Ausnahme, die (anfängliche) Pseudonymität jedoch weit verbreitet[23]. Wer im Online-Chat den Namen „Hero49" verwendet, handelt pseudonym, ohne dass der Chatbetreiber im Normalfall über einen (separaten) Bestand von Zuordnungsdaten („Zusatzinformationen") verfügt, der eine Reidentifizierung ermöglicht.

Dass der *LIBE-Ausschuss* von Regelungen absehen möchte, die Anreize schaffen für eine pseudonyme Netzkommunikation, wäre – jedenfalls in Deutschland – ein bedauerlicher Rückschritt. Die Verpflichtung zur Ermöglichung einer anonymen oder pseudonymen Nutzung in § 13 Abs. 6 TMG würde ersatzlos fortfallen.

b) Kontraproduktive Dynamik

Durch Erwägungsgrund 38 Satz 2 soll gleichwohl ein Anreiz für eine Pseudonymisierung geschaffen werden:

„Für den Fall, dass die Interessen oder Grundrechte und -freiheiten (‚fundamental rights and freedoms') des Datensubjekts nicht überwiegen, sollte vermutet werden, dass die Verarbeitung ausschließlich pseudonymer Daten die berechtigten Erwartungen des Datensubjekts erfüllt, die sich aus seinem Verhältnis zu dem Verantwortlichen (‚controller') ergeben."

Wegen des Vorbehalts überwiegender Interessen und Rechte des Betroffenen erschöpft sich der Wert der vorgeschlagenen Vermutung darin, dass die Pseudonymisierung dafür sprechen kann, dass die Abwägung nach Art. 6 Abs. 1 (f) DS-GVO („legitimes Interesse") zugunsten des Datenverarbeiters ausfällt. Dies schafft für den Datenverarbeiter wenig Rechtssicherheit und legt die Erwägung nahe, durch die Einholung von Einwilligungen Sicherheit zu schaffen. Wenn es aber für eine rechtssichere Datenverarbeitung der Einwilligung der Betroffenen bedarf, gibt es wenig Anlass, diese Einwilligung nur für pseudonymisierte Verfahren einzuholen und nicht sogleich auf die „Klarnamen" zu erstrecken[24]. Der zögerliche Ansatz, der den Erwägungsgrund 38 prägt, ist daher kontraproduktiv.

c) Kein Datenschutz für anonyme Daten

Der Begriff der Anonymisierung wird lediglich in Art. 81 der *LIBE*-Vorschläge im Zusammenhang mit Gesundheitsdaten verwendet. Eine Definition des Begriffs (vgl. § 3 Abs. 6 BDSG) soll es nicht geben.

In Erwägungsgrund 23 Satz 4 und 5 möchte der *LIBE-Ausschuss* klarstellen, dass das Datenschutzrecht nicht für anonyme Daten gilt:

„Die Prinzipien des Datenschutzes sollten daher nicht für anonyme Daten gelten, bei denen es sich um Informationen handelt, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Diese Verordnung betrifft daher nicht die Verarbeitung solcher anonymer Daten, einschließlich der Verarbeitung

17 Vgl. *Härting*, Internetrecht, 5. Aufl. 2014, Rz. 185 ff.
18 Vgl. *Weichert* in Däubler/Klebe/Wedde/Weichert, 3. Aufl. 2010, § 3 Rz. 3.
19 *Krüger/Maucher*, MMR 2011, 433 (436 ff.).
20 Erwägungsgrund 12 der DS-GVO, KOM(2012) 11 endg.
21 *Eckhardt/Kramer*, DuD 2013, 287 (288 f.).
22 Vgl. *Härting*, NJW 2013, 2065 (2068 f.).
23 Vgl. *Härting*, NJW 2013, 2065 (2068 f.).
24 Vgl. *Härting*, NJW 2013, 2065 (2070 f.).

zu statistischen Zwecken oder zu Zwecken der Forschung."

d) Realitätsferne Negativdefinition

Dies ist nicht mehr als eine Negativdefinition: Daten, die keinen Personebezug haben, sind anonym und unterliegen daher nicht dem Datenschutzrecht. Angesichts der unendlichen Weite des Begriffs der Personenbezogenheit, die der *LIBE-Ausschuss* in Art. 4 Abs. 2 vorschlägt, ist es äußerst fraglich, ob es überhaupt noch Daten geben kann, die entsprechend der negativen Definition als anonym angesehen werden können.

Unter den Bedingungen der heutigen Informationsverarbeitung ist die Unterscheidbarkeit personenbezogener und damit schutzwürdiger Informationen von anonymen Daten ohne Persönlichkeitsrelevanz zu einer Illusion geworden[25]. Eine „absolute Anonymität" gibt es nicht mehr. Dieser Befund sollte indes nicht Anlass sein, an dem unterschiedslosen Verbotsprinzip festzuhalten und dieses immer weiter auf alle Bereiche der Kommunikation zu erstrecken. Gefragt sind vielmehr Regelungsmodelle, die abgestuft sind und Verbote auf persönlichkeitsriskante Vorgänge beschränken. Wenn man – wie es zu fordern ist – anonymisierte Daten auch dann vom Verbot ausnimmt, wenn keine „absolute Anonymität" erreicht wird, lässt sich durch passgenaue Regelungen (insbesondere Re-Identifizierungsverbote[26]) ein Schutz der Persönlichkeitsrechte erreichen, der den Besonderheiten von anonymisierten Daten besser Rechnung trägt als ein Pauschalverbot.

6. Das doppelte Gesicht der Einwilligung und das falsche Verständnis von „Accountability"

Die datenschutzrechtliche Einwilligung hat ein doppeltes Gesicht: Sie ist einerseits ein Instrument der Selbstbestimmung des Bürgers. Andererseits ist die Einwilligung auch ein Instrument, das den Bürger in die Pflicht nimmt, selbst für den Schutz seiner Privatsphäre zu sorgen.

Der *LIBE-Ausschuss* möchte an der zentralen Bedeutung der Einwilligung im Gefüge des Datenschutzrechts festhalten. Dem alternativen Regelungskonzept der „Accountability" des Datenverarbeiters treten die *LIBE*-Vorschläge in keiner Weise nahe.

a) Sinn und Unsinn vorformulierter Einwilligungen

Der Diensteanbeiter, der eine Einwilligung vorformuliert, wird stets bemüht sein, die Einwilligung möglichst weit zu fassen und sie auf eine Vielzahl von Verarbeitungs- und Nutzungsvorgängen zu erstrecken:

„Fast an jedem Ort, an dem sich der Einzelne heute bewegt – vor allem online – wird er mit langen und komplexen Datenschutzbestimmungen konfrontiert, die routiniert von Juristen für Juristen geschrieben worden sind. Sodann wird der Einzelne gefragt, entweder ‚einzuwilligen' oder den gewünschten Dienst nicht in Anspruch zu nehmen. Die binäre Auswahl entspricht nicht dem, was sich die Architekten des Datenschutzrechts vor vier Jahrzehnten vorstellten, als sie von dem Bild mündiger Bürger ausgingen, die informierte Entscheidungen über die Verarbeitung ihrer personenbezogenen Daten treffen. In der Praxis ist dies gewiss nicht der optimale Mechanismus, um sicherzustellen, dass sowohl die Privatsphäre als auch der freie Informationsfluss geschützt werden."[27]

Je weiter der Spielraum, den sich der Datenverarbeiter durch eine Einwilligung verschafft, desto geringer ist die Wahrscheinlichkeit, dass er in Zukunft die Nutzer um weitere Einwilligungen bitten muss:

„Die informationelle Selbstbestimmung flüchtet sich in die Einwilligung. Sie versucht neutral zu sein in der Sache – ob bestimmte Arten der Sammlung, Nutzung und Verbreitung von personenbezogenen Daten gut oder schlecht ist – und konzentriert sich stattdessen darauf, ob Personen verschiedenen Datenschutzbestimmungen zugestimmt haben. Die Einwilligung legitimiert nahezu jede Form der Sammlung, Nutzung und Verbreitung von personenbezogenen Daten."[28]

b) Accountability des Datenverarbeiters für Schutz der Privatsphäre

Um „Accountability" als Alternative zur Einwilligung ging es 2009 in dem Galway Project, an dem zahlreiche Datenschutzexperten aus Europa und den USA mitwirkten. Zum Abschluss des Projekts veröffentlichten die Experten ein Diskussionspapier, in dem ein neuer, „accountability-orientierter Ansatz" folgendermaßen definiert wurde[29]:

„Eine accountability-orientierte Herangehensweise an Datenverarbeitung zeichnet sich dadurch aus, dass die Definition von Zielen im Mittelpunkt steht, die Organisationen zum Schutz von Persönlichkeitsrechten zu beachten haben. Die Ziele fußen auf gesetzlichen Vorgaben, wobei den Organisationen Spielräume bei der Bestimmung geeigneter Maßnahmen zur Erreichung dieser Ziele gelassen werden. Eine accountability-orientierte Herangehensweise ermöglicht es Organisationen, Methoden und Wege zu entwickeln, um diese Ziele in einer Weise zu erreichen, die am besten zu ihren Geschäftsmodellen, Technologien und zu den Bedürfnissen ihrer Kunden passt."

„Accountability" bedeutet demnach eine Verlagerung der Verantwortung für den Schutz der Privatsphäre auf den Datenverarbeiter. Der Datenverarbeiter erhält vom Gesetzgeber klare Zielvorgaben („goals" und „criteria"). Wie er die vorgegebenen Ziele erreicht, bleibt seinem Ermessen („discretion") überlassen. Hierdurch erhält der Datenverarbeiter den notwendigen Spielraum, um seine Technologie und sein Geschäftsmodell datenschutzfreundlich auszugestalten.

Der *LIBE-Ausschuss* versteht den Begriff der „Accountability" falsch und definiert ihn in Art. 5 (f) DS-GVO als

„Einhaltung (‚compliance') der Bestimmungen dieser Verordnung".

Nach Auffassung des Ausschusses ist somit „Accountability" nicht mehr als die (selbstverständliche bzw. redundante) Verpflichtung des Datenverarbeiters zur Einhaltung des Datenschutzrechts.

c) Einwilligung statt Accountability

Statt auf „Accountability" setzt der *LIBE-Ausschuss* auf die Einwilligung, die – anders als nach dem Willen der *EU-Kommission*[30] – auch dann gelten soll, wenn ein „er-

25 Vgl. *Giesen*, OLG Köln v. 10.2.2012 – 6 U 187/11, CR 2012, 550 (551); *Peifer*, K&R 2011, 543 (544).

26 Vgl. *Härting*, NJW 2013, 2065.

27 *Cate/Mayer-Schönberger*, Notice and consent in a world of Big Data, International Data Privacy Law, 2013, Vol. 3, No. 2, S. 67 (67), *http://m.idpl.oxfordjournals.org/content/3/2/67.full.pdf*.

28 *Solove*, Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review 1880 (2013), 1880, *www.harvardlawreview.org/media/pdf/vol126_solove.pdf*.

29 Centre for Information Policy Leadership Data Protection Accountability: The Essential Elements, Oktober 2009, *www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf*.

hebliches Ungleichgewicht" zwischen dem Datenverarbeiter und dem Betroffenen besteht (§ 7 Abs. 4 DS-GVO):

„Die Einwilligung soll zweckgebunden (‚purpose-limited') sein und ihre Gültigkeit verlieren, wenn der Zweck nicht mehr existiert oder sobald die Verarbeitung personenbezogener Daten nicht mehr notwendig ist, um den Zweck zu verfolgen, zu dem sie ursprünglich gesammelt wurden. Der Abschluss eines Vertrages oder die Bereitstellung eines Dienstes soll nicht von einer Einwilligung abhängig gemacht werden, die sich auf die Verarbeitung von Daten erstreckt, sie nicht notwendig ist für die Erfüllung des Vertrages oder die Bereitstellung des Dienstes gem. Art. 6 (1) (b)."

7. Vernachlässigung der Kommunikationsfreiheit

Die Schaffung einer Balance zwischen Persönlichkeitsschutz und freier Kommunikation gehört zu den Kernaufgaben eines modernen Datenschutzrechts[31]. Daher ist es äußerst unbefriedigend, dass Art. 80 DS-GVO die Schaffung einer Balance den EU-Mitgliedsstaaten überlässt. Nach den Vorstellungen der *EU-Kommission* soll es bei einer Regelung bleiben, die sich von dem – viel zu allgemein gefassten – „Medienprivileg" des Art. 9 DS-RL[32] nicht unterscheidet. Die Änderungen, die der *LIBE-Ausschuss* vorschlägt, sind marginal und daher enttäuschend.

Begreift man das Datenschutzrecht unter den Gegebenheiten der digitalen, vernetzten Informationssyteme (auch) als Kommunikationsregulierung, so greift es zu kurz, den vollständigen Verzicht auf eine eigene Abwägung damit zu begründen, dass die Medienregulierung den Kompetenzen des europäischen Gesetzgebers entzogen ist. Die Trennung zwischen Datenschutz- und Kommunikationsrecht ist gekünstelt. Wenn man von jeglichen Kommunikationsregeln absehen wollte, müsste man konsequenterweise eine Regelung schaffen, die die Bestimmungen der DS-GVO für nicht anwendbar erklärt, soweit es um Kommunikationshandlungen geht, die durch Art. 11 Grundrechte-Charta (Meinungs- und Informationsfreiheit) geschützt sind.

Art. 16 AEUV, der die Gesetzgebungskompetenz der EU für den gesamten Bereich des Datenschutzes schafft, stammt aus dem Jahre 2008[33]. Schon damals war klar, dass das Datenschutzrecht und das Kommunikationsrecht in weiten Bereichen zwei Seiten derselben Medaille darstellen. Vom *EU-Parlament* würde man sich daher eine deutlich großzügigere Auslegung des Art. 16 AEUV wünschen, um der Bedeutung des Art. 11 Grundrechte-Charta im gebotenen Maße Rechnung zu tragen und einen Zustand zu verhindern, der an einer entscheidenden Stelle statt einer Vereinheitlichung des Rechts einen Flickenteppich schafft.

8. Rudimentärer Rechtsschutz gegen Maßnahmen der Datenschutzbehörden

Den Datenschutzaufsichtsbehörden soll nach den Vorstellungen des *LIBE-Ausschusses* eine Vielzahl von Aufgaben zuwachsen. Der Aufgabenkatalog (Art. 52 DS-GVO) ist deutlich umfangreicher, als dies in dem Vorschlag der *EU-Kommission* vorgesehen war. Viel zu kurz kommt dabei die rechtsstaatliche Ausgestaltung der Verfahren.

a) Weder Verfahrensbeschleunigung noch Beanstandungsrechte

Wenn eine Datenschutzbehörde dem europäischen Bürger (und Unternehmer) gegenübertritt, handelt sie zwangsläufig in Ausübung von Hoheitsgewalt. Daher ist es misslich, dass die *EU-Kommission* den Rechtsschutz gegen Maßnahmen der Aufsichtsbehörden in Art. 74 DS-GVO nur rudimentär behandelt und sich die LIBE-Vorschläge zu Art. 74 in Marginalien erschöpfen. Es fehlen insbesondere Bestimmungen, die einen zügigen Verfahrensablauf gewährleisten, sei es über Verpflichtungen der Behörden, Verfahren in angemessener Zeit per (justiziablem) Verwaltungsakt zu beenden, sei es durch Maßnahmen des einstweiligen Rechtsschutzes oder durch Untätigkeitsklagen. Wenig bürgerfreundlich ist es zudem, dass der LIBE-Ausschuss zwar die Rolle des *Europäischen Datenschutzrats* (European Data Protection Board) als oberste europäische Datenschutzbehörde stärken möchte, dem Bürger jedoch keine Möglichkeit einräumt, im Rahmen des Konsistenzverfahrens (Art. 57 ff. DS-GVO) die Entscheidung einer nationalen Aufsichtsbehörde als inkonsistent bzw. übermäßig zu beanstanden.

b) EU-Datenschutzsiegel: Freiwilliges Genehmigungsverfahren

Nach Art. 39 der *LIBE*-Vorschläge sollen die Aufsichtsbehörden zu zentralen Zertifizierungsstellen werden. Jeder Datenverarbeiter soll nach Art. 39 Abs. 1 a und b DS-GVO einen Anspruch auf Durchführung eines Zertifizierungsverfahrens haben, ohne jedoch zu einer solchen Zertifizierung verpflichtet zu sein:

„Jeder Verantwortliche (‚controller') oder Verarbeiter (‚processor') kann jede Datenschutzaufsichtsbehörde in der Union gegen eine angemessene Gebühr (‚reasonable fee') bitten (‚request') zu zertifizieren, dass die Verarbeitung personenbezogener Daten den bestimmungen dieser Verordnung entspricht, insbesondere den Prinzipien, die in den Art. 5, 23 und 30 geregelt sind, sowie den Verpflichtungen des Verantwortlichen und des Verarbeiters und den Rechten der Datensubjekte.

Die Zertifizierung soll freiwillig, erschwinglich (‚affordable')", und verfügbar in einem Verfahren verfügbar sein, das transparent ist und nicht unangemessen beschwerlich (‚unduly burdensome').

Nach Art. 39 Abs. 1 d DS-GVO sollen private Zertifizierer unterstützend tätig werden dürfen, sofern sie über eine Akkreditierung einer Aufsichtsbehörde verfügen. Den Datenschutzbehörden wird auf diese Weise die Aufgabe einer umfassenden Aufsicht über privatwirtschaftliche Zertifizierungsstellen zugewiesen. Für die Zertifikate sieht Art. 39 Abs. 1 e DS-GVO die einheitliche Bezeichnung „Europäisches Datenschutzsiegel" vor.

In einem Zertifizierungsverfahren müsste die Datenschutzbehörde prüfen, ob Datenverarbeitungsverfahren rechtskonform sind. Stellt die Behörde Rechtsverstöße fest, so könnte sie sich nicht darauf beschränken, die Zertifizierung zu verweigern. Sie müsste vielmehr darauf bestehen, dass die Rechtsverstöße abgestellt werden. Hinsichtlich des Prüfungsprogramms und des Ablaufs würde ein Zertifizierungsverfahren somit einem (freiwilligen) Genehmigungsverfahren entsprechen. Der *LIBE-*

30 Genannt wird in Erwägungsgrund 34 als Beispiel für ein solches „erhebliches Ungleichgewicht" lediglich das Arbeitsverhältnis.

31 Vgl. *Härting/Schneider*, ZRP 2011, 233 ff.; *Härting*, ITRB 2010, 280 (281 f.).

32 Vgl. *Härting*, Internetrecht, 5. Aufl. 2014, Rz. 380.

33 Konsolidierte Fassung des AEUV, bekannt gemacht im ABl. EG Nr. C 115 v. 9.5.2008, S. 47 ff.

Ausschuss nutzt das Etikett eines „Datenschutzsiegels", um Unternehmen dazu zu veranlassen, Datenverarbeitungsverfahren (möglichst vorab) genehmigen zu lassen.

9. Rechtsstaatswidrige Sanktionen

Die Vollzugsdefizite des Datenschutzrechts sind hinlänglich bekannt. Daher ist es richtig, die Stellung der Aufsichtsbehörden zu stärken und ein wirksames Sanktionssystem einzuführen. Die *EU-Kommission* möchte den Behörden die Möglichkeit geben, Bußgelder bis zu einer Höhe von 2 % des weltweiten Jahresumsatzes eines Unternehmens zu verhängen. Der *LIBE-Ausschuss* erachtet dies nicht für ausreichend und schlägt folgende Regelung (als Art. 79 Abs. 2a und b) vor):

„Gegen jedermann, der die Bestimmungen dieser Verordnung nicht einhält, wird die Aufsichtsbehörde mindestens eine der folgenden Sanktionen verhängen:

a) eine schriftliche Verwarnung im Falle eines erstmaligen und nicht-vorsätzlichen Verstoßes;

b) regelmäßige, periodische Datenschutzaudits;

c) ein Bußgeld i.H.v. bis zu 100 000 000 € oder bis zu 5 % des jährlichen, weltweiten Umsatzes im Falle eines Unternehmens, wobei es auf den jeweils höheren Betrag ankommt.

Falls der Verantwortliche (controller) oder der Verarbeiter (processor) ein gültiges „Europäisches Datenschutzsiegel" besitzt gem. Art. 39, soll ein Bußgeld ... nur im Falle vorsätzlichen oder fahrlässigen Verhaltens verhängt werden."

a) Verstoß gegen Grundrecht auf faires Verfahren

Anders als im Vorschlag der *EU-Kommission* vorgesehen, ermöglicht diese Regelung eine Verhängung drakonischer Bußgelder, ohne dass ein Verschulden erforderlich ist. Dies ist ein klarer Verstoß gegen das Schuldprinzip, das in Art. 6 Abs. 2 EMRK verankert ist:

„Jede Person, die einer Straftat angeklagt ist, gilt bis zum gesetzlichen Beweis ihrer Schuld als unschuldig."

Der *Europäische Gerichtshof für Menschenrechte* (*EGMR*) hat mehrfach entschieden, dass Art. 6 EMRK nicht nur im Strafverfahren, sondern auch auf Bußgelder anwendbar ist[34].

b) Verstoß gegen Schuldprinzip und Menschenwürde

Das *BVerfG* leitet das Schuldprinzip aus der Menschenwürdegarantie ab (Art. 1 Abs. 1 GG). Nach dem „Ewigkeitsvorbehalt" des Art. 79 Abs. 3 GG ist das Schuldprinzip daher jeglichen Einschränkungen durch den deutschen oder europäischen Gesetzgeber entzogen:

„Das Strafrecht beruht auf dem Schuldgrundsatz. Dieser setzt die Eigenverantwortung des Menschen voraus, der sein Handeln selbst bestimmt und sich kraft seiner Willensfreiheit zwischen Recht und Unrecht entscheiden kann. Dem Schutz der Menschenwürde liegt die Vorstellung vom Menschen als einem geistig-sittlichen Wesen zugrunde, das darauf angelegt ist, in Freiheit sich selbst zu bestimmen und sich zu entfalten... Auf dem Gebiet der Strafrechtspflege bestimmt Art. 1 Abs. 1 GG die Auffassung vom Wesen der Strafe und das Verhältnis von Schuld und Sühne... Der Grundsatz, dass jede Strafe Schuld voraussetzt, hat seine Grundlage damit in der Menschenwürdegarantie des Art. 1 Abs. 1 GG .... Das Schuldprinzip gehört zu der wegen Art. 79 Abs. 3 GG unverfügbaren Verfassungsidentität, die auch vor Eingriffen durch die supranational ausgeübte öffentliche Gewalt geschützt ist.[35]."

c) Unfaire Verknüpfung mit EU-Datenschutzsiegel

Rechtsstaatlich bedenklich ist es zudem, wenn (in Art. 79 Abs. 2 b der *LIBE*-Vorschläge) die Verhängung eines Bußgeldes bei fehlendem Verschulden davon abhängen soll, ob ein Unternehmen über ein gültiges „Europäisches Datenschutzsiegel" verfügt, da die Datenschutzbehörden damit zugleich für die Zertifizierung (Art. 39 der *LIBE*-Vorschläge) und – bei fehlender Zertifizierung – für die Verhängung von Bußgeldern zuständig wären. Welches Unternehmen würde es – in einem laufenden Zertifizierungsverfahren – wagen, den Rechtsauffassungen einer Aufsichtsbehörde zur Auslegung der DS-GVO zu widersprechen, wenn es befürchten müsste, dass die Behörde ein (drakonisches) Bußgeld verhängt, wenn sich das Unternehmen nicht den Vorstellungen der Behörde fügt?

III. Ausblick

Nach der *EU-Kommission* hat sich jetzt auch das *EU-Parlament* (durch den *LIBE-Ausschuss*) klar zu der Datenschutzreform positioniert. Dies erhöht den Druck auf den *Europäischen Rat*, gleichfalls eine Verständigung zu erzielen. Eine solche Verständigung würde in einem nächsten Schritt dazu führen, dass alle drei Beteiligten (*Kommission, Parlament* und *Rat*) über einen gemeinsamen Vorschlag verhandeln. Ob und wann mit einer Verabschiedung neuer Datenschutzregelungen zu rechnen ist, bleibt daher nach wie vor offen.

34 EGMR v. 23.10.1984 – 8544/79 – Öztürk v. Germany; EGMR v. 19.10.2004 – 66273/01 – Falk v. Niederlande.

35 BVerfG v. 30.6.2009 – 2 BvE 2/08, 2 BvE 5/08, 2 BvR 1010/08, 2 BvR 1022/08, 2 BvR 1259/08, 2 BvR 182/09 – Lissabon-Vertrag.