Berlin, im Mai 2012
Stellungnahme Nr. 47/2012
www.anwaltverein.de

Stellungnahme

des Deutschen Anwaltvereins

durch die Ausschüsse Informationsrecht und Verfassungsrecht

zum Vorschlag für
„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)

und zum Vorschlag für
„Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“ (KOM(2012) 10 endgültig)

Mitglieder des Informationsrechtsausschusses:	Mitglieder des Verfassungsrechtsausschusses
Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender und Berichterstatter) Rechtsanwältin Isabell Conrad, München Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter) Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf Rechtsanwalt Prof. Dr. Jochen Schneider, München (Berichterstatter) Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München (Berichterstatter) Rechtsanwalt und Notar Ulrich Volk, Wiesbaden Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart Zuständiger DAV-Geschäftsführer: Rechtsanwalt Thomas Marx, DAV-Berlin	Rechtsanwalt Prof. Dr. Thomas Mayen (Vorsitzender und Berichterstatter) Rechtsanwältin und Notarin Mechtild Düsing, Münster Rechtsanwalt Roland Gerold, München Rechtsanwalt Dr. Rainard Menke, Stuttgart Rechtsanwalt Prof. Dr. Frank Rottmann, Leipzig (Berichterstatter) Rechtsanwältin Dr. Birgit Spießhofer, Berlin Rechtsanwalt Dr. Thomas Schröer, Frankfurt am Main Rechtsanwalt Prof. Dr Christian Winterhoff, Hamburg (Berichterstatter) Rechtsanwältin Dr. Antje Wittmann, Münster (Berichterstatterin) Zuständiger DAV-Geschäftsführer: Rechtsanwalt Dr. Nicolas Lührig, DAV-Berlin

Verteiler Europa:

- Europäisches Parlament
    - Ausschuss Bürgerliche Freiheiten, Justiz und Inneres
    - Ausschuss Wirtschaft und Währung
    - Ausschuss Beschäftigung und soziale Angelegenheiten
    - Ausschuss Industrie, Forschung und Energie
    - Ausschuss Binnenmarkt und Verbraucherschutz
- Europäische Kommission
    - Generaldirektion Justiz
- Rat der Europäischen Union
- Der Europäische Datenschutzbeauftragte
- Ständige Vertretung der Bundesrepublik Deutschland bei der EU
- Justizreferenten der Landesvertretungen
- Rat der Europäischen Anwaltschaften (CCBE)
- Vertreter der Freien Berufe in Brüssel
- Deutsche Industrie- und Handelskammertag (DIHK) in Brüssel
- Bundesverband der Deutschen Industrie (BDI) in Brüssel

Verteiler Deutschland:

- Deutscher Bundestag
    - Innenausschuss
    - Rechtsausschuss

- Bundesregierung
    - Bundesministerium des Innern
    - Bundesministerium der Justiz

- Bundesverfassungsgericht

- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Arbeitskreise Recht der Bundestagsfraktionen
- Innenministerien und Senatsverwaltungen für Inneres der Länder
- Justizminister und Justizsenatoren der Länder
- Die Datenschutzbeauftragten der Bundesländer

- Präsidentin des Bundesverwaltungsgerichts
- Präsidenten der Oberverwaltungsgerichte und Verwaltungsgerichtshöfe

- Bund Deutscher Verwaltungsrichter und Verwaltungsrichterinnen
- Bundesrechtsanwaltskammer
- Bundesnotarkammer
- Bundesverband der Freien Berufe
- Deutscher Richterbund
- Deutscher Notarverein e.V.
- Deutscher Steuerberaterverband
- GRUR
- BITKOM
- DGRI

- DAV-Vorstand und Geschäftsführung
- Vorsitzende der DAV-Gesetzgebungsausschüsse
- Vorsitzende der DAV-Landesverbände
- Mitglieder des DAV-Verwaltungsrechtsausschusses
- Mitglieder des DAV-Umweltrechtsausschusses
- Vorsitzende des FORUMs Junge Anwaltschaft

- Redaktion NVwZ
- Redaktion NJW
- Redaktion DVBL
- Redaktion DÖV
- Juve-Verlag
- Redaktion Anwaltsblatt
- ver.di Bundesverwaltung, Fachbereich Bund und Länder, Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit 67.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Der Deutsche Anwaltverein hat durch seinen Informationsrechtsausschuss im Januar 2011 in 12 Anmerkungen Stellung genommen (DAV-Stellungnahme Nr. 4/2011, abrufbar unter www.anwaltverein.de) zu dem „Gesamtkonzept für den Datenschutz in der Europäischen Union“, das die EU-Kommission am 4.11.2010 veröffentlicht hatte (http://ec.europa.eu/health/data_collection/docs/com_2010_0609_de.pdf). Das „Gesamtkonzept“ bildete die Grundlage für die Entwürfe einer neuen Datenschutz-Richtlinie (DSRL-neu) und einer Datenschutz-Grundverordnung (DS-GVO), die die Kommission am 25.1.2012 vorgelegt hat.

Die beiden Entwürfe geben Anlass zu einigen grundsätzlichen Ausführungen (Teil I), einer kritischen Würdigung anhand der 12 Anmerkungen des DAV durch den Informationsrechtsausschuss (Teil II) und zu einigen Schlussbemerkungen zu ausgewählten Einzelpunkten (Teil III).

I. Grundsätzliches

1. Das geltende europäische Datenschutzrecht wird den Anforderungen der Informationsgesellschaft des 21. Jahrhunderts nicht gerecht. Die Datenschutzrichtlinie (DSRL) stammt aus dem Jahre 1995 und gibt keine hinreichenden Antworten auf die Herausforderungen der Informations- und Kommunikationstechnologie. Daher ist es richtig, das europäische Datenschutzrecht umfassend zu erneuern. In Anbetracht der technischen, gesellschaftlichen und rechtlichen Komplexität der Materie ist dies eine **Herkulesaufgabe**, zumal globale Wechselwirkungen zu berücksichtigen sind, da die vernetzte Kommunikation keine europäischen Außengrenzen kennt.

2. Der Versuch, Teilbereiche des europäischen Datenschutzrechts im Bereich der privaten Wirtschaft vollständig zu **harmonisieren**, verdient grundsätzlich Anerkennung. In der Tat sind aufgrund der geltenden DSRL in den einzelnen EU-Mitgliedsstaaten recht unterschiedliche Datenschutzgesetze und -standards entstanden. Dies ist ein Hemmnis für Unternehmen, die europaweit agieren.

3. Die beiden Entwurfe stehen nicht in Einklang mit dem in Art. 5 Abs. 3 EUV verbindlich vorgegebenen Subsidiaritätsprinzip. Ebenfalls nicht erforderlich ist es, dass die Datenschutzrichtlinie den gesamten Bereich der polizeilichen und justiziellen Tätigkeit erfassen soll – unabhängig davon, ob die Datenverarbeitung auf innerstaatlicher Ebene oder grenzüberschreitend erfolgt (unten b).

   a) Eine verbindliche Vollregelung des Datenschutzes im nicht-öffentlichen und öffentlichen Bereich durch Verordnung statt durch eine (die Vollharmonisierung *ebenfalls* ermöglichende) Richtlinie ist weder geeignet noch erforderlich für die angestrebte Harmonisierung des Datenschutzrechts. Anders als die bestehende, schon auf eine Vollharmonisierung nationaler Datenschutzgewährleistungen zielende Richtlinie führt eine Verordnungs-

regelung mit umfassendem verbindlichen Geltungsanspruch zur nahezu vollständigen Verdrängung mitgliedstaatlicher Datenschutzregelungen. Dies ist bezogen auf das Ziel der angestrebten Harmonisierung des Datenschutzniveaus deshalb problematisch, weil die Bestimmungen der Datenschutz-Grundverordnung nur ein sehr hohes Abstraktionsniveau aufweisen, das Anforderungen generalisiert und die differenzierten Schutzrechte des allgemeinen und fachrechtlichen Datenschutzes der Mitgliedstaaten nivelliert. Ob dies durch delegierte Rechtsakte der Kommission aufgefangen wird, ist völlig ungewiss und rechtlich nicht gewährleistet. Das von der Kommission betonte Ziel, durch den Erlass der vorgeschlagenen Verordnung die Rechtssicherheit für Wirtschaft und Staat bei der Verarbeitung personenbezogener Daten zu erhöhen, wird damit verfehlt.

Zudem wird durch die Nutzung der Rechtsform „Verordnung“ der gesamte Bereich des Schutzes personenbezogener Daten dem Anwendungsbereich der einschlägigen grundgesetzlichen Grundrechte und mithin der Judikatur des Bundesverfassungsgerichts entzogen. Auf den Vollzug von Verordnungen der Union kommen *nur die europäischen Grundrechte* nach der Grundrechtecharta zur Anwendung, während die deutschen Grundrechte grundsätzlich unanwendbar sind.[1] Der Grundrechtsschutz auf europäischer Ebene stellt sich zwar in materieller Hinsicht im Zuge eines Vergleichs zu dem Grundrechtsschutz auf nationaler Ebene als prinzipiell ausreichend dar. Demgegenüber sind die Möglichkeiten zur Geltendmachung einer Grundrechtsverletzung im Wege eines Vergleichs als unzureichend zu bewerten. Der Europäische Gerichtshof ist darüber hinaus nach seinem Selbstverständnis *kein Gerichtshof für Menschen- oder Grundrechte*. Eine solche spezifisch grundrechtsbezogene gerichtliche Funktion kann der Europäische Gerichtshof auch nicht leisten. Er ist – abgesehen von dem hier nicht anwendbaren Art. 263 Abs. 4 AEUV – nicht zuständig für den unmittelbaren Schutz von Individualinteressen, durch welche grundrechtstypische Gefährdungslagen jedenfalls zum Teil gekennzeichnet sind.[2] Zudem sieht das Unionsrecht keine der deutschen Verfassungsbeschwerde vergleichbare Möglichkeit der direkten Grundrechtsklage beim EuGH vor.

b) Eine vollständige Harmonisierung im Bereich der **öffentlichen Verwaltung und Justiz** halten wir ebenfalls nicht für erforderlich. Nach der Begründung der Kommission soll die Datenschutzrichtlinie – in Abgrenzung zum Anwendungsbereich des bisherigen Rahmenbeschlusses 2008/977/JI – für den gesamten Bereich der polizeilichen und justiziellen Tätigkeit gelten, unabhängig davon, ob die Datenverarbeitung auf innerstaatlicher Ebene oder grenzüberschreitend erfolgt (Richtlinienvorschlag, a. a. O., S. 2, 7). Der Großteil der von Polizei- und Justizbehörden erhobenen Daten wird aber rein

[1] Vgl. BVerfGE 118, 79 (95 f.); BVerfG, Beschluss vom 29. April 2010, Az. 2 BvR 871/04 u. a. (Leitsatz Nr. 1) = NVwZ-RR 2010, 585 (585);; Streinz/Michl, in: Streinz, EUV/AEUV, 2. Aufl. 2012, GR-Charta Art. 51 Rn. 6-8.

[2] Vgl. auch die Schlussanträge der Generalanwältin Eleanor Sharpston vom 30. September 2010, Rs C-34/09 (Zamprano ./. ONEM), Rn. 155.

innerstaatliche Vorgänge betreffen. Polizei- und Strafrecht stellen von jeher einen Kernbereich der Staatlichkeit (sog. *Domaine reservé*) dar.[3]

Zudem überzeugt es nicht, wenn gerade in den besonders grundrechtssensiblen Bereichen von Polizei und Justiz nur **Mindeststandards** getroffen werden, die zum Teil deutlich hinter der Verordnung zurückbleiben. Zum anderen entsteht durch die Trennung eine Gemengelange im öffentlichen Bereich: Ein und dieselben Datenbestände sind unter Beachtung der strengen Bestimmungen der DS-GVO zu verarbeiten, wenn Behörden außerhalb des Anwendungsbereichs der DSRL-neu agieren. Sobald diese Datenbestände einer Nutzung durch Polizei und Justiz zugeführt werden, sollen andere Standards gelten. Dies wirft schwierige Abgrenzungsfragen auf, da nahezu jede Behörde aus den Bereichen von Polizei und Justiz zugleich Aufgaben wahrnehmen wird, die nicht in den Anwendungsbereich der DSRL-neu fallen.

4. Bei der vielfach geäußerten Kritik am geltenden europäischen Datenschutzrecht geht es primär um das **materielle Datenschutzrecht für die nicht-öffentliche Datenverarbeitung**, also um das starre Verbotsprinzip, die starre Anknüpfung des Anwendungsbereichs an den wenig randscharfen Begriff der Personenbezogenheit, die unzulänglichen Transparenzbestimmungen und die fehlenden Kriterien der Abwägung zwischen Persönlichkeitsschutz und Kommunikationsfreiheit. Auf diese Kritik finden sich in der DS-GVO und der DSRL-neu kaum Antworten. Das materielle Datenschutzrecht soll vielmehr in seiner Grundstruktur bestehen bleiben. Den Herausforderungen der aktuellen Informations- und Kommunikationstechnologie wäre das Datenschutzrecht damit trotz der nicht zu verkennenden Ansätze (wie etwa zu privacy by design) nicht gewachsen.

5. Die DS-GVO setzt auf eine umfassende behördliche Kontrolle und Durchsetzung des Datenschutzrechts. Es soll eine **pyramidenartige Behördenstruktur** entstehen, die dem Datenschutzrecht in ganz Europa mit empfindlichen Sanktionen zur Durchsetzung verhilft.

   a) Dies begegnet zunächst insoweit Bedenken, als die Rechtsdurchsetzung unter der Federführung der Europäischen Kommission stehen und die Kommission zugleich umfangreiche Befugnisse erhalten soll, per delegiertem Rechtsakt und durch Durchführungsrechtsakte Recht zu setzen. Eine solche **Vereinigung legislativer und exekutiver Befugnisse** unter dem Dach der Kommission wäre rechtsstaatlich höchst problematisch.

   b) Sodann ist die Ausprägung der „völligen Unabhängigkeit“ der nationalen Datenschutzbehörden für den Bereich der privaten Datenverarbeitung zu revidieren und einer dem Demokratieprinzip entsprechenden Ausgestaltung zuzuführen. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts sind weisungsfreie Räume innerhalb der unmittelbaren Staatsverwaltung mit dem Demokratieprinzip des Grundgesetzes unvereinbar.[4] In einer Entscheidung vom 9. März 2010 hat der Europäische Gerichtshof[5] diese

[3] Vgl. nur Vogel, in: Grabitz/Hilf, Das Recht der Europäischen Union, Art. 83 AEUV Rn. 1.
[4] Vgl. nur BVerfGE 107, 59 (86-94).
[5] Vgl. EuGH, Urteil vom 9. März 2010, Rs. C-518/07 = Slg. 2010, S. I-1885.

Anforderungen für das Demokratiegebot des Unionsrechts nicht übernommen. Eine staatliche Aufsicht gleich welcher Art ermögliche es der Regierung des betroffenen Landes oder einer Stelle der ihr untergeordneten Verwaltung, auf Entscheidungen der Kontrollstelle unmittelbar oder mittelbar Einfluss zu nehmen; es lasse sich nicht ausschließen, dass die Aufsichtsstellen, die Teil der allgemeinen Verwaltung und damit der Regierung unterstellt sind, nicht zu objektivem Vorgehen in der Lage sind, wenn sie die Vorschriften über die Verarbeitung personenbezogener Daten auslegen und anwenden.

Diese Rechtsprechung vernachlässigt, dass in einer Demokratie alle staatliche Gewalt vom Volk als dem Souverän ausgeht und Entscheidungen der staatlichen Verwaltung daher durch das Volk legitimiert sein müssen. Dies ist nur dann der Fall, wenn sich die Bestellung der Amtsträger auf das Staatsvolk zurückführen lässt und das Handeln der Amtsträger selbst eine ausreichende sachlich-inhaltliche Legitimation erfährt, d. h. die Amtsträger im Auftrag und nach Weisung der Regierung handeln und die Regierung damit in die Lage versetzen, die Sachverantwortung gegenüber Volk und Parlament zu übernehmen. Auch wenn die Rechtsprechung des EuGH für das Unionsrecht maßgeblich ist, müssen diese Kritikpunkte doch jeweils bei der Entscheidung des Unionsgesetzgebers, ob er weisungsfreie Räume der staatlichen Verwaltung vorgeben will, beachtet werden. Hier gilt es in besonderer Weise sensibel zu sein. Eine Häufung weisungsunabhängiger Behörden (wie sie im Unionsrecht derzeit zu beobachten ist) begründet die Gefahr einer „Renaissance des anachronistischen Verwaltungsstaats“[6].

Im Falle des Verordnungsvorschlags kommt nun hinzu, dass die Unabhängigkeit der Datenschutzbehörden nur gegenüber den nationalen Institutionen/Behörden gilt, nicht aber gegenüber der Kommission. Dieser sollen im Gegenteil nach dem Verordnungsvorschlag erhebliche Einwirkungsmöglichkeiten gegenüber den Datenschutzbehörden zukommen. Stellungnahmen der Kommission sollen die Datenschutzbehörden „so weit wie möglich Rechnung“ tragen (Art. 59 Abs. 2 des Verordnungsvorschlags); unter den Voraussetzungen des Art. 60 des Verordnungsvorschlags kann die Kommission geplante Maßnahmen einer nationalen Datenschutzbehörde aussetzen. Es ist nicht erkennbar, weshalb insoweit nicht die Gefahr einer politischen Einflussnahme auf die Entscheidungen der Kontrollstellen bestehen soll.

6. Das neue europäische Datenschutzrecht soll nach dem Willen der Kommission nicht für die **EU-Verwaltung** gelten. Stattdessen soll die an die DSRL angelehnte EU-Verordnung Nr. 45/2001 vom 18.12.2000 unverändert fortgelten. Dies ist nicht konsequent. Wenn die EU-Kommission eine mächtige Rolle bei der europaweiten Fortentwicklung und Durchsetzung des Datenschutzrechts erhalten soll, müssen die Bürger darauf vertrauen können, dass sich europäische Behörden an die **selbstgesetzten Standards** halten.

[6] Gärditz, AöR Bd. 135 (2010), S. 251.

7. Insgesamt fehlt der DS-GVO das Bewusstsein, dass Grundrechte und Grundfreiheiten nicht nur den Betroffenen, sondern – im nicht-öffentlichen Bereich – auch den Datenverarbeitern zustehen (insbesondere die Kommunikations- und die Berufsfreiheit). Beide Grundrechtspositionen können im Einzelfall miteinander kollidieren. Beide Grundrechtspositionen sind hierbei grundsätzlich von gleichem Gewicht und müssen im Einzelfall zu einem verhältnismäßigen Ausgleich gebracht werden („praktische Konkordanz"). Eine starre Verbotsregelung, die eine private Datenverarbeitung nur erlaubt, wenn hierfür ein Rechtfertigungsgrund besteht, ist mit den Erfordernissen des Grundrechtsschutzes zwar nicht per se unvereinbar. Eine gesetzliche Regelung, welche die Zulässigkeit der Datenverarbeitung stets unter den Vorbehalt der Einzelfallabwägung stellt, kann aber wegen der damit verbundenen Rechtsunsicherheit leicht in eine faktische Behinderung der Datenverarbeitung umschlagen, die durch die berechtigten Belange des Datenschutzes nicht mehr gerechtfertigt wäre. Es bedarf deshalb praktikabler **Abwägungsmechanismen** zur Herstellung einer solchen Konkordanz und zudem eines **effektiven Rechtsschutzes**.

II. Die „12 Anmerkungen" des DAV durch den Informationsrechtsausschuss

1. *Der Datenverkehr in der vernetzten Informationsgesellschaft führt zu **Risiken,** die in der Mitteilung „Gesamtkonzept für den Datenschutz in der Europäischen Union" eingehend analysiert werden. Dies gilt allerdings nicht nur für die private Datenspeicherung, sondern auch für die staatliche Überwachung. Dem Zugriff des Staates auf die „Spuren" der Kommunikationsbeziehungen müssen im Interesse der Bürgerrechte deutliche Schranken gesetzt werden.*

   Sachverhalte wie die Online-Durchsuchung und der staatliche Zugriff auf Kommunikationsdaten, die bei Telekommunikationsunternehmen gespeichert werden (Vorratsdatenspeicherung), zeigen, dass dem staatlichen Zugriff Schranken gesetzt werden müssen, ohne dass es auf einen **Personenbezug** einzelner Daten ankommt. Sobald Daten Personenbezug aufweisen, soll das gesamte Datenschutzrecht mit all seinen vielfältigen Instrumentarien auch weiterhin gelten. Wenn es dagegen an einem Personenbezug fehlt, soll das Datenschutzrecht – wie bisher – in toto nicht anwendbar sein. Dies bedeutet beispielsweise, dass es ohne Personenbezug auch weiterhin[7] keine Transparenzpflichten beim Umgang mit Daten geben soll (vgl. Art. 14 DS-GVO).

   Eines der Kernprobleme des **„Schwarz-Weiß-Prinzips"** ist die fehlende Trennschärfe des Begriffs der Personenbezogenheit. Je nachdem, ob man von einem „absoluten"[8] oder einem „relativen"[9] Begriffsverständnis ausgeht, gelangt man zu einem sehr weiten oder stark eingeschränkten Anwendungsbereich des Datenschutzrechts. Wie die hierzulande anhaltende Kontroverse um die Personenbezogenheit von IP-Adressen[10] zeigt, ist dies höchst unbefriedigend.

---

[7] Vgl. Härting, CR 2011, 169, 170 f.; Pahlen-Brandt, K&R 2008, 288.
[8] Vgl. Weichert in Däubler/Klebe/Wedde/Weichert, 3. Aufl. 2010, § 3 Rdnr. 3; Härting, BB 2012, 459, 463.
[9] Vgl. Dammann in Simitis, BDSG, 7. Aufl. 2011, § 3 Rdnr. 21.
[10] Vgl. Eckhardt, CR 2011, 339 ff.; Krüger/Maucher, MMR 2011, 433 ff.; Sachs, CR 2010, 547 ff.; Venzke, ZD 2011, 114 ff.; s.a. BVerfG v. 24. Januar 2012 - 1 BvR 1299/05 -.

Die Entwürfe lassen befürchten, dass sich die Kontroversen um den Anwendungsbereich des Datenschutzrechts fortsetzen werden.[11] Art. 4 Nr. 1 DS-GVO lässt es für die Bestimmbarkeit einer Person ausreichen, dass der Datenverarbeiter oder „jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach“ eine Zuordnung vornehmen kann. Dies legt die Deutung nahe, dass jede objektive Möglichkeit der Zuordnung für einen Personenbezug ausreichen soll („absoluter“ Begriff des Personenbezugs). Dieser Deutung steht jedoch Erwägungsgrund 24 entgegen. Dort heißt es, dass beispielsweise Kennnummern, Standortdaten und „Online-Kennungen“ (IP-Adressen) „nicht zwangsläufig und unter allen Umständen als personenbezogene Daten zu betrachten sind“. Dies würde bedeuten, dass die Feststellung eines Personenbezugs vom Verwendungskontext abhängt. Der genaue Anwendungsbereich des Datenschutzrechts wäre auch weiterhin unklar. Die neuen Formulierungen in Art. 4 Nr. 1 und Erwägungsgrund 24 DS-GVO würden die Unsicherheit sogar verstärken.

2. *Die vernetzte Kommunikation eröffnet auch **Chancen** für die ungehinderte Ausübung von Freiheitsrechten und ist daher ihrerseits schützenswert. Dies, insbes. die Informationsfreiheit als Gegengewicht, kommt in der Mitteilung „Gesamtkonzept für den Datenschutz in der Europäischen Union“ nicht hinreichend deutlich zum Ausdruck.*

Die Datenverarbeitung soll grundsätzlich verboten bleiben. Art. 6 DS-GVO hält an dem **Verbotsprinzip** fest. Es soll dabei bleiben, dass jede Art der datengestützten Kommunikation einer Rechtfertigung bedarf, sofern – wie regelmäßig – personenbezogene Daten genutzt werden. Die Information, Meinungsäußerung und Kommunikation im Netz sollen weiterhin – im Regelfall – nur zulässig sein, wenn ein gesetzlicher Rechtfertigungsgrund greift.

Die Kritik an einem prominenten Politiker, die in einem Blog oder auch per Twitter oder Facebook geäußert wird, steht aus Sicht des Entwurfs der DS-GVO auf einer Stufe mit der Erfassung von Adressdaten bei einem Versandhändler. Zwar sieht Art. 80 DS-GVO die Möglichkeit von Ausnahmen vom Verbotsprinzip für die journalistische Datenverarbeitung vor. Bezeichnenderweise findet sich diese Vorschrift jedoch in einem der Schlusskapitel ("besondere Datenverarbeitungssituationen"), und die Ausgestaltung von Ausnahmen soll vollständig dem nationalen Gesetzgeber überlassen bleiben. Ein und dieselbe Meinungsäußerung in einem Internetforum könnte somit nach deutschem Recht aufgrund einer Ausnahmenorm erlaubt und nach ungarischem Recht (mangels einer solchen Norm) verboten sein.[12]

Mit Art. 80 DS-GVO würde es bei einer Regelung bleiben, die dem **„Medienprivileg“** des Art. 9 DSRL entspricht. Die Reichweite des „Medienprivilegs“, das aus der Zeit vor dem Internet stammt, ist unsicher und streitig.[13] Praktikable Kriterien zur Abwägung zwischen schutzwürdigen Persönlichkeitsrechten und dem **Grundrecht auf freie Kommunikation** lassen sich Art. 80 DS-GVO ebenso wenig entnehmen wie Art. 9 DSRL.

---

[11] Härting, BB 2012, 459, 463; Hornung, ZD 2012, 99, 102.
[12] Vgl. Kuner, BNA 2012, 13 - „lack of harmonization“.
[13] Schneider/Härting, ZD 2011, 63, 66 f.

3. *Im nicht-öffentlichen Bereich ist das Verbot oder die Einschränkung der Datenverarbeitung im Normalfall mit einem Eingriff in **Freiheitsrechte** der datenverarbeitenden Person oder Stelle verbunden. Ein solcher Eingriff kann nur dann durch den Datenschutz legitimiert sein, wenn eine Abwägung der wechselseitigen Freiheitsrechte ergibt, dass der Datenschutz schwerer wiegt als die Freiheitsrechte der verarbeitenden Person oder Stelle. Dies gilt umso mehr, als der vernetzte Informationsaustausch es mit sich bringt, dass der Einzelne regelmäßig in eine **Doppelrolle** als Subjekt und Objekt der Datenverarbeitung gerät.*

   Im öffentlichen Bereich ist das Verbotsprinzip im Hinblick auf den Gesetzesvorbehalt konsequent und nicht zu beanstanden. Im nicht-öffentlichen Bereich geht es hingegen nicht um ein Eingriffsverhältnis, sondern im Regelfall um eine **mehrpolare Situation**, in der bei dem Betroffenen, aber auch bei Datenverarbeitern Grundrechtspositionen bestehen und abzuwägen sind. Beide Grundrechtspositionen sind hierbei grundsätzlich von gleichem Gewicht und müssen im Einzelfall zu einem verhältnismäßigen Ausgleich gebracht werden („praktische Konkordanz“).

   Das uneingeschränkte Festhalten am Verbotsprinzip im Bereich der nicht-öffentlichen Datenverarbeitung wird diesen mehrpolaren Sachverhalten nicht gerecht (oben I.7). Umgekehrt überzeugt es nicht, dass nach dem Entwurf der DS-GVO **„private“ Bereiche** der Grundrechtskollision vollständig aus der Anwendbarkeit des Datenschutzrechts ausklammert bleiben sollen. Nach Art. 2 Abs. 2 lit. d DS-GVO soll die Verordnung keine Anwendung finden auf eine Datenverarbeitung durch natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken „ohne jede Gewinnerzielungsabsicht“. Dies entspricht im wesentlichen Art. 3 Abs. 2, zweiter Spiegelstrich DSRL. Dies obwohl Blogs, Diskussionsforen und soziale Netzwerke Stoff für zahlreiche **Abgrenzungsfragen** liefern, die es zur Zeit des Inkrafttretens der DSRL noch nicht gab.

   In Art. 2 DS-GVO zeigt sich, dass die DS-GVO sich nur unzureichend mit der kommunikativen Dimension von Datenverarbeitung befasst. Für Online-Veröffentlichungen – beispielsweise in Blogs und sozialen Netzwerken – bedarf es einer klaren Regelung, ob und unter welchen Voraussetzungen die Schwelle zur **„Gewinnerzielungsabsicht“** somit zum Datenschutzrecht überschritten sein soll. Anderenfalls bleibt beispielsweise die problematische Deutung offen, dass ein und dieselbe Meinungsäußerung in einem privaten Blog zulässig und in einem kommerziellen sozialen Netzwerk unzulässig ist.

4. *Für den durch **Art. 10 EMRK** geschützten Informations- und Meinungsaustausch ist die vernetzte Kommunikation unverzichtbar. Das Recht auf freie Meinungsäußerung schließt nach Art. 10 Abs. 1 Satz 2 EMRK die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriff öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein. Jede Reglementierung des Meinungs- und Informationsflusses im nicht-öffentlichen Bereich birgt die Gefahr eines Eingriffs in Art. 10 EMRK. Dies gilt auch dann, wenn die Reglementierung aus Gründen des Datenschutzes erfolgt.*

Diese Anmerkung wendet sich gegen einen prinzipiellen Vorrang des Datenschutzes. Für den Bereich der privaten Datenverarbeitung gilt, dass sich sowohl der Datenschutz als auch die Datenverarbeitung auf grundrechtliche Schutzpositionen berufen kann. Beide Grundrechtspositionen sind hierbei grundsätzlich von gleichem Gewicht und müssen im Einzelfall zu einem verhältnismäßigen Ausgleich gebracht werden („praktische Konkordanz"). Weder der Datenschutz noch das Grundrecht auf Freiheit der Kommunikation genießt hierbei einen allgemeinen Vorrang.

Neben Art. 80 DS-GVO begegnet auch das undifferenzierte **„Right to be forgotten"** Einwänden mit Blick auf Art. 10 EMRK: Nach Art. 12 lit. b DSRL besteht derzeit ein Löschungsrecht des Betroffenen bei unvollständigen oder unrichtigen Daten und bei Daten, deren Verarbeitung aus anderen Gründen rechtswidrig ist. Im Zeichen der Einführung eines „Right to be forgotten"[14] weitet Art. 17 DS-GVO die Löschungsansprüche erheblich aus.

Art. 17 Abs. 1 DS-GVO unterscheidet zwischen vier Gründen für einen Löschungsanspruch. Während Art. 17 Abs. 1 lit. a DS-GVO noch an den Zweckbindungsgrundsatz anknüpft und somit im Kern Art. 12 lit. b DSRL entsprechen dürfte, führt Art. 17 Abs. 1 lit. b DS-GVO eine Löschungspflicht für den Fall ein, dass eine **„Speicherfrist"** abgelaufen ist oder dass der Betroffene eine Einwilligung widerruft. Da es in Art. 7 Abs. 3 DS-GVO an jedweder Einschränkung des Widerrufsrechts fehlt, muss der Datenverarbeiter in Zukunft damit rechnen, dass es weitgehend dem Belieben des Betroffenen überlassen ist, ob und wann eine (kraft Einwilligung) rechtmäßige Datenverarbeitung aufgrund eines Widerrufs rechtswidrig wird mit der Folge sofortiger Löschungspflichten.

Eine Löschungspflicht würde auch für literarische und andere urheberrechtlich geschützte Werke gelten. Der sich aufdrängende **Konflikt zum Urheberrecht** bleibt ungelöst.

Art. 17 Abs. 2 DS-GVO ist eine der wenigen Vorschriften, in denen einmal ausdrücklich auf eine **Veröffentlichung** Bezug genommen wird. Bei Veröffentlichungen stellt sich die Kommission vor, dass das „Recht auf Vergessenwerden" flankiert wird von erheblichen Handlungspflichten des Verarbeitenden: So soll ein Internetanbieter, der zu löschende Daten veröffentlicht hat, „alle vertretbaren Schritte, auch technischer Art" ergreifen, um Dritte von der Löschung zu informieren. Insbesondere soll er auf eine „Löschung aller Querverweise" und die Löschung von „Kopien oder Replikationen" hinwirken.

Wie angesichts der ständigen Vervielfältigungs- und Verknüpfungsvorgänge im Internet Art. 17 Abs. 2 DS-GVO umsetzbar sein soll, ist nicht ersichtlich. Aus Sicht desjenigen, der eine Veröffentlichung vornimmt, wird der Umgang mit personenbezogenen Daten zu einem **unüberschaubaren Risiko**. Denn der Anbieter muss jederzeit damit rechnen, dass der Betroffene sich auf ein Löschungsrecht gemäß Art. 17 Abs. 1 DS-GVO beruft und – gestützt auf Art. 17 Abs. 2 DS-GVO – von dem Anbieter eine Einwirkung auf Dritte verlangt mit einem Aufwand, der für den Anbieter nicht abzuschätzen ist. Unter dem Blickwinkel des Schutzes der freien

[14] Vgl. Nolte, ZRP 2011, 236 ff.

Kommunikation befördert Art. 17 Abs. 2 DS-GVO bei dem Internetakteur eine Selbstzensur im Sinne der **„Schere im Kopf“**.

Den Konflikt zur Kommunikationsfreiheit hat die Kommission nicht vollständig übersehen. Art. 17 Abs. 3 lit. a DS-GVO sieht eine Ausnahme von den Löschungspflichten vor für den Fall, dass die Datenspeicherung zur Ausübung des Rechts auf freie Meinungsäußerung gemäß Art. 80 DS-GVO „erforderlich“ ist. Schon das strenge Kriterium der „Erforderlichkeit“ belegt allerdings, dass der Regelung die Vorstellung zu Grunde liegt, dass die freie Kommunikation die Ausnahme darstellt und die DS-GVO nicht von einem **Gleichrang** des Schutzes der Privatsphäre und des Schutzes der Kommunikationsfreiheit ausgeht.

5. *Die latente Gefahr einer übermäßigen Einschränkung von Freiheitsrechten im Zeichen des Datenschutzes besteht ausschließlich im **nicht-öffentlichen Bereich** und stellt einen kardinalen Unterschied zum Datenschutz gegenüber staatlichen Stellen dar. Da der Schutz der Daten eines Bürgers im nicht-öffentlichen Bereich oft notwendig mit der Beschränkung von Freiheitsrechten verbunden ist, bedarf es klarer, praktikabler **Abwägungsregeln**.*

Die Entwertung der Einwilligung als Rechtsgrundlage für eine Datenverarbeitung (Art. 7 Abs. 4 DS-GVO) führt dazu, dass noch mehr als bisher **Einzelfallabwägungen** über die Rechtmäßigkeit der Datenverarbeitung entscheiden. Weitgehend unverändert (vgl. Art. 7 lit. f DSRL) heißt es in Art. 6 Abs. 1 lit. f DS-GVO, dass die Datenverarbeitung erlaubt ist zur Wahrung der berechtigten Interessen des Datenverarbeiters, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der Betroffenen überwiegen. Die Rechtmäßigkeitsprüfung wird noch viel deutlicher einer Einzelfallabwägung überlassen als bisher. Dies schafft ein Mehr an Rechtsunsicherheit an einer Stelle, an der das Bedürfnis nach Rechtssicherheit besonders evident[15] ist.

Berücksichtigt man die Entschlossenheit des Verordnungsgebers, staatliche Aufsichtsbefugnisse über die Datenverarbeitung zu verdichten, läuft ein verstärktes Erfordernis der Abwägung im Einzelfall auf eine Verstärkung **staatlicher Einflussnahme** auf die Datenverarbeitung hinaus. Dies kann sich zu einem Kommunikationshindernis und einer staatlichen Kontrolle von Kommunikation auswirken, die den freien Informationsaustausch in demokratisch organisierten Gesellschaften gefährdet. Wer bei der Kommunikation vor dem ständigen Erfordernis von Abwägungen steht, die einer staatlichen Kontrolle unterliegen, und für den Fall einer fehlerhaften Abwägung mit erheblichen Sanktionen rechnen muss, wird geneigt sein, sich Beschränkungen aufzuerlegen, die den Informationsfluss und den freien Meinungsaustausch in bedenklicher Weise einschränken.

Soll die Abwägung im Einzelfall gemäß Art. 6 Abs. 1 lit. f DS-GVO die wichtigste Weichenstellung bei der Beurteilung der Rechtmäßigkeit einer Datenverarbeitung sein, so stimmt es auch mehr als bedenklich, wenn Art. 6 Abs. 5 DS-GVO vorsieht, dass die Europäische Kommission ermächtigt werden soll, per „delegiertem Rechtsakt“[16] Maßgaben für die Abwägung zu erlassen. Hierdurch würde eine

[15] Schneider/Härting, ZD 2011, 63, 66.
[16] Vgl. Härting, BB 2012, 459, 460.

demokratisch nur sehr mittelbar legitimierte Stelle europaweit die Befugnis erhalten, Entscheidungen über die Rechtmäßigkeit von Datenverarbeitung zu treffen.

6. *Bei jedweder Abwägung ist zu berücksichtigen, dass eine Datenverarbeitung für den jeweils Betroffenen dann gefährlicher ist, wenn er in einem **Abhängigkeitsverhältnis** zu der Daten verarbeitenden Stelle steht. Im Verhältnis zwischen Arbeitgeber und Arbeitnehmer müssen für die Datenverarbeitung und -nutzung daher beispielsweise andere Regeln gelten als bei der Kommunikation unter Freunden und Bekannten in sozialen Netzwerken.*

   Art. 7 Abs. 4 DS-GVO sieht vor, dass bei einem **„erheblichen Ungleichgewicht“** zwischen Betroffenem und Datenverarbeiter die Einwilligung als Rechtsgrundlage für eine Datenverarbeitung von vornherein ausscheidet. Hieraus ergibt sich ein Gesamtbild, das die Einwilligung als Legitimation für eine Datenverarbeitung noch mehr als bisher[17] zur seltenen Ausnahme werden lässt. Dies läuft auf eine verstärkte **Bevormundung** des Betroffenen hinaus, dessen ausdrücklicher Wunsch einer Teilhabe am Datenverkehr von vornherein nicht respektiert wird.[18]

   Nimmt man das Individualrecht auf freie Entfaltung der Persönlichkeit ernst, so ist auch der großzügige, wenn nicht gar exhibitionistische Umgang mit Informationen über die eigene Person eine Ausübung von Grundfreiheiten, deren Einschränkung bedenklich stimmt. Die allzu paternalistischen Tendenzen werden in Art. 7 Abs. 4 DS-GVO besonders deutlich.[19] Je stärker auf der Basis des Verbotsprinzips die Betonung einer Verfügungsbefugnis des Einzelnen über Daten ist, desto weniger überzeugt es, wenn Einwilligungsbefugnisse weiter beschnitten werden sollen.

   Wenn sich ein Verbraucher und ein Unternehmen gegenübertreten, wird man stets von einem „Ungleichgewicht“ sprechen. Art. 7 Abs. 4 DS-GVO läuft somit darauf hinaus, Einwilligungen der Verbraucher in die Datenverarbeitung jegliche Rechtsbedeutung zu nehmen.[20] Aus Sicht der Unternehmen bedeutet dies, dass sie bei jeder Verarbeitung von personenbezogenen **Verbraucherdaten** darauf angewiesen sind, eine gemäß Art. 6 Abs. 1 lit. f DS-GVO „richtige“ Abwägung der Interessen vorzunehmen, wobei sie stets befürchten müssen, dass staatliche Aufsichtsbehörden die Abwägung überprüfen und zu abweichenden Ergebnissen gelangen.[21] Dies wird zu zunehmender Rechtsunsicherheit beim Datenverkehr und bei der Online-Kommunikation mit Verbrauchern führen.

7. *Jede staatliche Kontrolle der Datenverarbeitung kann im nicht-öffentlichen Bereich die Freiheitsrechte der Bürger gefährden. Dies gilt auch dann, wenn eine „unabhängige“ Stelle für die Kontrolle verantwortlich ist. Von einer Staatsferne bzw. **„Unabhängigkeit“** der Kontrollinstanz kann immer nur dann die Rede sein, wenn es um eine Kontrolle der staatlichen Datenverarbeitung geht. Wird dagegen einer*

---

[17] Vgl. Schneider/Härting, ZD 2011, 63, 65 f.; Wybitul/Fladung, BB 2012, 510.
[18] Auf die spezifisch deutsche Problematik, Einwilligungen nach AGB-Recht und im Verhältnis dazu auch nach UWG zu beurteilen, gehen wir hier nicht näher ein. S. etwa BGH v. 16.7.2008 – VIII ZR 348/06, NJW 2008, 3055 – payback - ; BGH v. 11.11.2009 – VIII ZR 12/09, NJW 2010, 864 – Happy Digits -.
[19] Härting, BB 2012, 459, 463.
[20] Kuner, BNA 2012, 6.
[21] Härting, BB 2012, 459, 463.

Behörde die Befugnis eingeräumt, gegenüber Bürgern bzw. privaten Unternehmen Kontrollmaßnahmen zu ergreifen, handelt es sich um ***hoheitliche Befugnisse****, die dieselben Fragen des Freiheitsschutzes aufwirft, die sich auch bei anderen staatlichen Maßnahmen stellen. Gegenüber dem Bürger ist der Staat stets Staat, auch wenn er sich in das Gewand einer „unabhängigen" Stelle kleidet.*

Zu den Bedenken gegen die Unabhängigkeit der Datenschutzbehörden im Bereich der privaten Datenverarbeitung im Allgemeinen und ihrer Ausgestaltung im Entwurf der Datenschutz-Grundverordnung im Besonderen verweisen wir auf die Ausführungen oben I.5.

Hinzuzufügen ist, dass die Unabhängigkeit der Datenschutzbehörde nicht zu Einschränkungen des Rechtsschutzes gegen deren Entscheidungen führen darf. Die Rechtsbehelfe gegen Entscheidungen der Aufsichtsbehörden sind in Art. 73 bis 76 DS-GVO geregelt. Art. 73 DS-GVO berechtigt Betroffene zur Beschwerde bei den Aufsichtsbehörden, wenn sie der Auffassung sind, dass Bestimmungen der DS-GVO oder – generell – „der Schutz personenbezogener Daten" (vgl. Art. 63 Abs. 3 DS-GVO) verletzt worden sind. Art. 74 Abs.1 DS-GVO regelt – in einem einzigen Satz – Rechtsbehelfe gegen eine Aufsichtsbehörde.

Art. 75 DS-GVO behandelt Klagerechte der Betroffenen gegen Datenverarbeiter. In Art. 76 DS-GVO finden sich Verfahrensvorschriften, die insbesondere einen einheitlichen Schutz personenbezogener Daten innerhalb der EU sicherstellen sollen (vgl. Art. 76 Abs. 2 DS-GVO). Insgesamt ist zu bemängeln, dass sich auf zwei Seiten mit Regelungen zu Rechtsbehelfen ein einziger Satz zu den Rechten findet, die ein Datenverarbeiter hat, der von einer **rechtswidrigen Maßnahme einer Aufsichtsbehörde** betroffen ist.

8. *Wegen der staatlichen Kontrolle bzw. Aufsicht, die mit Maßnahmen einer Datenschutzbehörde verbunden sind, gerät das* ***Anwaltsgeheimnis*** *in Gefahr, wenn Verpflichtungen des Anwalts zur* ***„Rechenschaft"*** *über den Umgang mit Daten erwogen werden. Die Kontrolle über den sorgsamen Umgang mit sensiblen Daten sollte Aufgabe der Stellen sein, die für die Überwachung pflichtgemäßen Handelns der Anwälte verantwortlich sind – in Deutschland die Anwaltskammern. Der Datenschutz legitimiert keine staatlichen Kontrollen der anwaltlichen Berufsausübung. Das Anwaltsgeheimnis schützt die Vertraulichkeit der Kommunikation zwischen Mandant und Anwalt, gehört nach deutschem Verfassungsrecht zu den Grundbedingungen des Rechtsstaates und muss daher von jedweder staatlichen Kontrolle und Einsichtnahme frei bleiben.*

Art. 84 DS-GVO stellt zwar klar, dass Informationen, die dem Anwaltsgeheimnis unterliegen, einer staatlichen Überwachung und Kontrolle entzogen sind. Offen bleibt jedoch das Verhältnis des materiellen Datenschutzrechts zu dem Geheimnisschutz. Hier muss das Anwaltsgeheimnis beispielsweise **Vorrang vor Informations- und Auskunftsrechten** Dritter haben. Es kann etwa nicht angehen, dass offen bleibt, ob sich Dritte auf ein „Right to be forgotten" berufen können, wenn der Mandant dem Anwalt Daten Dritter anvertraut hat. Ebenso wenig kann es beispielsweise richtig sein, dass ein Ehegatte vom Anwalt seiner scheidungswilligen Ehefrau Auskünfte über gespeicherte Daten verlangen kann. Noch gravierender ist die Verpflichtung,

schon bei einer Datenspeicherung im Zusammenhang mit einer reinen Beratung den Betroffenen zu unterrichten. Endet z.B. eine familienrechtliche Beratung mit der Entscheidung, die Ehe aufrechtzuerhalten, müsste der Rechtsanwalt den Ehepartner des Betroffenen etwa über die Speicherung von dessen Daten unterrichten, und zwar einschließlich des Zwecks der Speicherung (zur Berechnung des möglichen Trennungsunterhalts). Entsprechendes gilt hinsichtlich der Problematik bei vielen anderen Beratungen im Vorfeld eventueller Konflikte.

9. *Die vernetzte Kommunikation und die damit – jedenfalls theoretisch – oft mögliche Zusammenführung und Verknüpfung von Datenbeständen bringen es mit sich, dass ein großer Teil der im Internet verfügbaren Daten als* ***personenbezogen*** *angesehen werden kann, wenn man von einem weiten Begriff des Personenbezugs ausgeht. Je mehr Daten unter den Begriff fallen, desto mehr stellt sich die Frage, ob es nicht – im nicht-öffentlichen Bereich – einer stärkeren Differenzierung bedarf bei dem Schutz dieser Daten. Bei Gesundheitsdaten leuchtet es unmittelbar ein, dass diese Daten ohne Einwilligung des Betroffenen nur in eng zu definierenden Ausnahmefällen verarbeitet werden dürfen. Bei einer E-Mail-Adresse, die als personenbezogenes Datum anzusehen ist, fällt es dagegen schwer, einen einleuchtenden materiellen Grund zu benennen, weshalb der Adressinhaber gefragt werden muss, wenn die Adresse elektronisch gespeichert wird. Das* ***Einwilligungs-/Verbotsprinzip*** *gehört bei Daten, die ein selbstverständlicher Bestandteil der alltäglichen Kommunikation sind, abgeschafft.*

   Das Verbotsprinzip wird derzeit in Art. 7 DSRL geregelt. Es soll – wie bereits erwähnt – nicht gelockert, sondern – durch Art. 6 DS-GVO – verschärft werden. Angesichts der exponentiellen Zunahme der datengestützten Kommunikation ist dies ein **rückwärtsgewandter Ansatz**, der den Erfordernissen der Informationsgesellschaft nicht gerecht wird. Ohne eine Modifikation, wenn nicht gar Abschaffung des Verbotsprinzips, wird eine Modernisierung des Datenschutzrechts misslingen.[22]

10. *Das Einwilligungs-/Verbotsprinzip lässt sich keinesfalls damit legitimieren, dass man von einer Art (eigentumsähnlichen) absoluten Verfügungsrecht des Betroffenen ausgeht. Daten „gehören" einer Person nicht (allein), sie sind vielmehr (auch) ein* ***Abbild sozialer Realität*** *und als notwendiger Bestandteil der sozialen und gesellschaftlichen Interaktion schützenswert. Das Einwilligungs-/Verbotsprinzip darf nicht dazu führen, dass der soziale Interaktionsraum schleichend* ***„privatisiert"*** *und hierdurch die freie Kommunikation in einer demokratischen Gesellschaft behindert wird.*

    Dem Misstrauen des Verordnungsgebers gegen autonome Entscheidungen des Betroffenen entspricht es, wenn der Betroffene in Art. 7 Abs. 3 DS-GVO ein Recht zum jederzeitigen **Widerruf einer Einwilligung** erhalten soll. Dieses Widerrufsrecht soll an keinerlei Voraussetzungen gebunden sein und auch ohne weiteres (d.h. sofort) wirksam werden. Ein Internetanbieter, der personenbezogene Daten der Nutzer aufgrund deren Einwilligung zur Gestaltung seines Angebots einsetzt, müsste befürchten, die Legitimation für die Datennutzung jederzeit mit sofortiger Wirkung zu verlieren.[23]

---

[22] Vgl. Härting/Schneider, ZRP 2011, 233, 234; Peiffer, K&R 2011, 543 ff.
[23] Härting, BB 2012, 459, 463.

Bei Online-Publikationen und der Kommunikation im Netz – insbesondere auch innerhalb sozialer Netzwerke – kommt es zwangsläufig zu Konflikten zwischen Persönlichkeitsrechten und der Meinungs- und Informationsfreiheit.[24] Der Datenschutz hat in diesem Konfliktfeld die Aufgabe, die **Persönlichkeitsrechte** zu schützen. Ob E-Mail-Adresse, Gerätekennzeichen, Cookie oder IP-Adresse: Es gibt keinen plausiblen Grund, derartige Daten per se unter Schutz zu stellen. Von einem Datum als solchem geht keine Gefahr aus. Wenn die Daten jedoch – allein oder in Verbindung mit anderen Daten bzw. Informationen – Rückschlüsse darauf zulassen, dass ein bestimmter Internetnutzer sich auf Internetseiten mit pikantem Inhalt bewegt hat, ist die Privat- bzw. Intimsphäre des Nutzers berührt. Die Daten erlangen einen Informationswert, der die Persönlichkeitsrechte beeinträchtigen kann.[25]

Die DS-GVO hätte, basierend auf der EU-Grundrechtecharta, zwei Schutzgüter von Rang – „Privatsphäre“ und freie Kommunikation[26] – auszugestalten und abwägungsfähig ins Verhältnis zu setzen. Stattdessen stellt der Verordnungsentwurf nicht die Persönlichkeitsrechte in den Mittelpunkt, sondern erklärt in Art. 1 Abs. 2 DS-GVO den „Schutz personenbezogener Daten“ zum Anliegen der Verordnung. Art. 1 DS-GVO ist überschrieben „Gegenstand und Ziel“ und lädt zu dem Missverständnis ein, dass Daten um ihrer selbst willen zu schützen sind. Die für ein modernes Datenschutzrecht unverzichtbare **Differenzierung** zwischen Daten und persönlichkeitsrelevanten Informationen[27] geht in Art. 1 DS-GVO verloren. Gegenüber der DSRL ist dies ein Rückschritt, denn Art. 1 Abs. 1 DSRL bezeichnet den "Schutz der Privatsphäre" ausdrücklich als Schutzziel, während Art. 1 DS-GVO auf die Erwähnung der Privatsphäre gänzlich verzichtet.

11. *Das Einwilligungs-/Verbotsprinzip wird im Übrigen den Realitäten der Netzkommunikation nicht gerecht. Dies zeigt die Diskussion um die Anforderungen an einen **„informed consent“**: Kommunikation im Internet ist in weiten Bereichen Massenkommunikation. Wenn der Betreiber eines sozialen Netzwerks von einzelnen Nutzern Einwilligungserklärungen (benötigt und) verlangt, ist dies nicht anders realisierbar als durch vorgefertigte, standardisierte Erklärungen. Damit derartige Erklärungen noch den Sinn erfüllen können, dem Nutzer eine autonome Entscheidung zu ermöglichen, sind ausführliche und verständliche Erklärungen über die beabsichtigte Datennutzung unverzichtbar („informed consent“). Wenn der Nutzer in Kenntnis transparenter Erläuterungen die Plattform nutzt, ist die Autonomie seines Handelns gesichert. Dies dann mit vorgefertigten (formelhaften) Einwilligungserklärungen zu verbinden, ist entbehrlich. Verstärkte **Transparenzregeln** und gesetzlich genauer geregelte Anforderungen an Datenschutzbestimmungen sollten in weiten Bereichen an die Stelle des Einwilligungs-/Verbotsprinzip treten.*

---

[24] Vgl. *Härting*, AnwBl 2011, 246, 248 ff.; zum hohen Rang der Meinungsäußerungsfreiheit s. a. EMRG, Urteil der Großen Kammer v. 7.2.2012 in der Sache von Hannover gegen Deutschland Nr. 2 (Appl. nos. 40660/08 und 60641/08).

[25] *Schneider/Härting*, ZD 2011, 63, 64; *Schneider/Härting*, ZRP 2011, 233.

[26] Stattdessen besagt Art. 1 Abs. 1: *Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten*.

[27] *Schneider/Härting*, ZRP 2011, 233.

Das Datenschutzrecht setzt bislang sehr wenig auf die Information und Aufklärung des Betroffenen und hinkt damit der Entwicklung des **Verbraucherrechts** weit hinterher.[28] Nach Art. 10 und 11 DSRL beschränken sich die Informationspflichten des Datenverarbeiters auf allgemeine Angaben zur eigenen Identität, zu den Zwecken der Datenverarbeitung, zu den Empfängern von Daten sowie zu Auskunfts- und Beseitigungsrechten.

Art. 14 Abs. 1DS-GVO sieht eine Erweiterung der Informationspflichten aus Art. 10 und 11 DSRL vor. Weitgehend neu sind uneingeschränkte Belehrungspflichten zu der Person des Datenschutzbeauftragten, zu den Berichtigungs- und Widerspruchsrechten sowie zu dem Beschwerderecht bei der zuständigen Aufsichtsbehörde (Art. 14 Abs. 1 lit. a, d und e DS-GVO). Neu ist auch die Verpflichtung, über die Dauer der Speicherung personenbezogener Daten zu informieren (Art. 14 Abs. 1 lit. c DS-GVO). Diese Verpflichtung ist eng mit dem „Recht auf Vergessenwerden“ (Art. 17 DS-GVO)[29] verbunden. Dass sich eine solche Verpflichtung bei Internetangeboten anders in die Tat umsetzen lässt als durch **Allgemeinplätze** („solange gespeichert, wie die Profilseite besteht“), ist schwer vorstellbar.

Ein Teil der Belehrungspflichten ist für **Veröffentlichungen** schlechterdings untauglich. Wie soll man bei Daten, die im Internet veröffentlicht werden, die Verpflichtung verstehen, die Betroffenen über die „Empfänger“ der Daten zu unterrichten (Art. 14 Abs. 1 lit. f DS-GVO)? Und wie soll man bei einer Onlinepublikation die Verpflichtung verstehen, die Betroffenen über die „Übermittlung“ von Daten „an ein Drittland“ (Art. 14 Abs. 1 lit. g DS-GVO) zu verständigen?

Art. 14 DS-GVO bleibt auch im Übrigen stark dem Konzept der Offline-Verarbeitung verhaftet, das Art. 10 und 11 DSRL zugrunde liegt. Wenn Art. 14 Abs. 3 DS-GVO eine Information des Betroffenen über die **„Herkunft“** personenbezogener Daten vorschreibt, geht dies an den Gegebenheiten der Internetkommunikation vollständig vorbei. Dasselbe gilt für die Verpflichtung, den Betroffenen „innerhalb einer angemessenen Frist“ nach der Erhebung von Daten über die Datenerhebung zu informieren (Art. 14 Abs. 4 lit. b DS-GVO).

Art. 14 DS-GVO ist präzise bei der Verpflichtung des Datenverarbeiters zur Belehrung des Betroffenen über seine Rechte und Rechtsbehelfe. Zugleich bleibt die Norm vage bei den Informationen über die Datenverarbeitung selbst. Dies wird besonders deutlich in Art. 14 Abs. 1 lit. h DS-GVO. Dort wird dem Datenverarbeiter vorgeschrieben, dem Betroffenen „sonstige Informationen (mitzuteilen), die unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten“. Der Verzicht auf konkrete Vorgaben und der Rückgriff auf unbestimmte Begriffe („besondere Umstände“; „Treu und Glauben“) lassen erwarten, dass sich kaum **rechtssichere Aussagen** darüber treffen lassen, ob Datenschutzbestimmungen den Anforderungen des Art. 14 Abs. 1 DS-GVO genügen.

[28] Härting, CR 2011, 169 ff.; Schneider/Härting, ZD 2011, 63, 68.
[29] Vgl. Härting, BB 2012, 459, 464 f.; Hornung, ZD 2012, 103; Kuner, BNA 2012, 5.

Wesentliche Unzulänglichkeiten der bisherigen Transparenznormen[30] würden durch Art. 14 DS-GVO bestehen bleiben:

- Es ist nicht einsichtig, dass Informationspflichten nur bestehen sollen, wenn personenbezogene Daten verarbeitet werden. Insbesondere für das **Tracking** besteht ein Bedürfnis nach Transparenz, und zwar unabhängig davon, ob es sich bei dem Tracking um eine Verarbeitung von Daten mit Personenbezug handelt.

- Es gibt ein ersichtliches Interesse des Nutzers eines Internetangebots an Informationen über Maßnahmen, die gegen einen missbräuchlichen Datenzugriff durch Dritte getroffen werden. Art. 14 DS-GVO enthält dennoch keine Vorgaben für die Information des Nutzers über die **Datensicherheit**.

- Art. 11 Abs. 2 DS-GVO verpflichtet zwar zur Verwendung einer klaren, einfachen und adressatengerechten Sprache. Genauere **Standards** – wie etwa die Vorgabe separater „Datenschutzbestimmungen“ auf einer Internetseite – setzt die DS-GVO jedoch nicht. Die Setzung von Standards soll vielmehr – rechtsstaatlich bedenklich[31] – der Europäischen Kommission überlassen bleiben.

12. *Dass die 15 Jahre alte EU-Datenschutzrichtlinie den Herausforderungen des Internet nicht mehr in jeder Hinsicht gerecht wird, ist unbestritten. Dennoch sei abschließend darauf hingewiesen, dass es auch gute Gründe zu einer gewissen Zurückhaltung bei der Einführung neuer Regelungen geben mag. Dies betrifft die evtl. zu starke Berücksichtigung aktueller technischer und sozialer Phänomene. Insofern empfiehlt sich neben mehr abstrakter, genereller Regelung auch eine gewisse Zurückhaltung. Insbesondere unter jungen Menschen, die eine Welt ohne das Internet nicht mehr kennen, lässt sich beobachten, dass sich **Kommunikationsgewohnheiten** ändern; die wahrgenommenen Grenzen zwischen Privatem und Öffentlichem verschieben sich. Hinzu kommt die vielfach zu beobachtende Tendenz einer Minderheit von Internetnutzern, äußerst freigiebig, gelegentlich sogar **exhibitionistisch** sehr Persönliches in alle Welt zu verbreiten. Auch wenn dies den Mehrheitsgeschmack nicht trifft, ist auch unvernünftiges Verhalten durch die Freiheit der Entfaltung der Persönlichkeit geschützt. Neue Regelungen des Datenschutzes dürfen weder zu einer reglementierenden Bevormundung von Bürgern führen, die sich nach mehrheitlicher Auffassung unbesonnen oder geschmacklos verhalten. Eben so wenig sollte eine Neuregelung vorschnell tradierte Grenzen zwischen Privatem und Öffentlichem festschreiben, ohne den laufenden Wandel gesellschaftlicher Anschauungen abzuwarten und zu würdigen.*

    Da das materielle Datenschutzrecht in seiner Grundstruktur unverändert bleiben soll, verwundert es nicht, dass die DS-GVO Regelungen zum Interessenausgleich in **sozialen Netzwerken** und zur Grenzziehung zwischen schützenswerter privater Kommunikation und öffentlichem Diskurs vermissen lässt. Die Notwendigkeit, mutige Regelungen zu finden, die die Privatsphäre schützen, ohne **Kommunikationsräume** einzuengen, liegt indes auf der Hand.

[30] Schneider/Härting, ZD 2011, 63, 68.
[31] Vgl. Härting, BB 2012, 459, 460.

III. Einzelpunkte

1. Wie bereits oben I.3.b) bemerkt, begegnet es unter dem Gesichtspunkt des Subsidiaritätsprinzips Bedenken, dass die Datenverarbeitung durch Polizei und Justiz europaweit Beschränkungen unterworfen werden soll, ohne dass es darauf ankommt, ob die Datenverarbeitung auf innerstaatlicher Ebene oder grenzüberschreitend erfolgt. Zudem ist zweifelhaft, ob die DSRL-neu ihrem eigenen Anliegen in der vorliegenden Fassung gerecht werden kann. Dies gilt insbesondere im Hinblick auf Art. 7 DSRL-neu. Art. 7 DSRL-neu erklärt in generalklauselartigen Formulierungen die Datenverarbeitung schon dann für rechtmäßig, wenn sie – alternativ – zur „Wahrnehmung einer gesetzlichen Aufgabe“, zur „Erfüllung einer gesetzlichen Verpflichtung“, zur „Wahrung lebenswichtiger Interessen“ oder zur „Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit“ notwendig ist. Mit solchen Formulierungen würden der Datenverarbeitung durch Polizei und Justiz **keine spürbaren Grenzen** gesetzt.

2. Polizei und Justiz sind besonders grundrechtssensible Bereiche. Daher ist es unstimmig, wenn die Datenschutzkontrolle in der DSRL-neu zum Teil deutlich hinter der DS-GVO zurückbleibt. Dies gilt in besonderem Maße für die Befugnisse der Aufsichtsbehörden. Der Befugniskatalog des Art. 46 DSRL-neu bleibt deutlich hinter Art. 53 DS-GVO zurück. Die DSRL-neu verzichtet auf Sanktionsbefugnisse der Datenschutzbehörden und kann schon aus diesem Grund **keinen wirksamen Grundrechtsschutz** gegenüber Polizei und Justiz gewährleisten.

3. Die DS-GVO führt zu keiner Rechtssicherheit bei den Voraussetzungen einer **Profilbildung** im Netz. Denn angesichts der unklaren Definition des Begriffs der personenbezogenen Daten in Art. 4 Abs. 1 Nr. 1 und 2 DS-GVO würde es bei der bisherigen Unsicherheit bleiben, ob das Datenschutzrecht überhaupt anwendbar ist. Soweit man dies bejaht, bedarf es einer Regelung, die die Profilbildung unter bestimmten Voraussetzungen erlaubt (vgl. § 15 Abs. 3 TMG). Art. 20 Abs. 1 DS-GVO scheidet als Legitimationsnorm aus, da sie nicht als Ausnahme zum Verbotsprinzip formuliert ist, sondern das Vorliegen einer solchen Ausnahme voraussetzt und lediglich der Nutzung erlaubtermaßen erhobener und gespeicherter Daten Grenzen setzt.

4. Wir begrüßen es, dass der Verordnungsentwurf den in Deutschland bewährten **betrieblichen Datenschutzbeauftragten** europaweit anerkennt.

   Dennoch wirft die Regelung Zweifel auf. Zwar ist es sinnvoll, die Bestellung eines betrieblichen Datenschutzbeauftragten Betrieben nicht schon ab einer Größe von 10 Mitarbeitern aufzugeben. Denn die Grenze von 10 Mitarbeitern wird bei den Bedingungen moderner Datenverarbeitung von zu vielen Betrieben erreicht, als dass ernsthaft erwartet werden kann, dass all diese Betriebe betriebliche Datenschutzbeauftragte bestellen. Bei vielen kleinen Betrieben (z.B. Handwerksbetrieben) bestehen auch keine ernsthaften Gefahren für die Persönlichkeitsrechte, weil nur wenige personenbezogene Daten erhoben und diese Daten nur in seltenen Fällen weitergegeben werden.

Die Bestellung eines betrieblichen Datenschutzbeauftragten erst ab einer Größe von 250 Mitarbeitern vorzuschreiben, führt zu einer zu hohen und zu abstrakten Grenze, Die Grenze ist **zu hoch**, weil dadurch viele Betriebe nicht erfasst sind, die in großem Umfang personenbezogene Daten verarbeiten und bei denen ein hohes Gefährdungspotential besteht. Hier müsste ein betrieblicher Datenschutzbeauftragter schon bei einer niedrigeren Zahl von Mitarbeitern bestellt werden. Sinnvoll wäre u.U. eine Verpflichtung zur Stellung eines betrieblichen Datenschutzbeauftragten dann, wenn mindestens ein Schwerpunkt der betrieblichen Tätigkeit in der Verarbeitung personenbezogener Daten besteht. Dabei darf es nicht nur auf die **Beobachtung** betroffener Personen ankommen wie dies derzeit in Artikel 35 Abs. 1 c DS-GVO vorgesehen ist. Jede systematische Nutzung personenbezogener Daten reicht. Bei einer Reihe von kleinen Unternehmen (z.B. Detekteien, IT-Anbieter im Bereich SaaS, Managed Services u. ä. oder KMU im Bereich Online-Marketing) werden erhebliche Mengen an personenbezogenen, evtl. sogar sensiblen Daten erhoben, verarbeitet und genutzt.

Die Grenze ist auch **zu abstrakt**: Die Bestellung eines Datenschutzbeauftragten sollte beispielsweise davon abhängig gemacht werden, dass es in dem betreffenden Unternehmen eine eigenständige EDV-Abteilung mit mindestens einem Halbtagsbeschäftigten gibt. Dann ist neben einer „kritischen Mindestgröße“ auch sichergestellt, dass diese Person organisatorisch unabhängig ist und als Datenschutzbeauftragter über das erforderliche Fachwissen verfügt.

Darüber hinaus erscheint es verfehlt, dass für die Bestellung des Datenschutzbeauftragten sowohl der für die Verarbeitung Verantwortliche als auch der **Auftragsverarbeiter** in Betracht kommt. Dies führt zum einen dazu, dass bei einem Kleinunternehmen, das einen sehr großen Auftragsdatenverarbeiter beauftragt, das kleinere Unternehmen für die Bestellung eines Datenschutzbeauftragten beim großen Auftragsdatenverarbeiter verantwortlich sein kann. Hier müsste in Art. 35 Abs. 1 DS-GVO klargestellt werden, dass dann, wenn nur eines der beteiligten Unternehmen die maßgebliche Grenze zur Bestellung eines betrieblichen Datenschutzbeauftragten überschreitet, nur dieser für die Bestellung des betrieblichen Datenschutzbeauftragten verantwortlich ist.

Die vorgeschlagene Norm kann darüber hinaus auch so verstanden werden, dass ein **Kleinunternehmen**, das ein Großunternehmen als Auftragsdatenverarbeiter beschäftigt – eine Situation, die jedenfalls bei Cloud Computing und vergleichbaren Dienstleistungen häufiger auftritt – allein deswegen einen Datenschutzbeauftragten bestellen muss. Diese Konsequenz ist verfehlt. Auch insoweit sollte Art. 35 Abs. 1 DS-GVO klarer formuliert werden.

5. Zur **Auftragsdatenverarbeitung (Art. 26 DS-GVO)** ist festzustellen, dass die bisher nach deutschem Recht mit der Konstellation einer Auftragsdatenverarbeitung verbundene Privilegierung, wonach der Auftragnehmer nicht als „Dritter“ gilt und eine Datenweitergabe an ihn daher keine „Übermittlung“, sondern eine interne Nutzung ist, zumindest nicht explizit in der Regelung des Art. 26 DS-GVO zum Ausdruck kommt, sondern sich erst im Umkehrschluss aus Art. 26 Abs. 4 DS-GVO erschlossen werden muss. Da diese Wirkung aber die ganz maßgebliche Wirkung einer

Auftragsdatenverarbeitung ist, sollte diese Wirkung/Privilegierung ausdrücklich als Rechtsfolge einer ordnungsgemäßen Auftragsdatenverarbeitung genannt werden.

Die „insbesondere“-Formulierung in Art. 26 Abs. 2 lit. a DS-GVO kann ein Hinweis auf die Privilegierung sein. Allerdings bleibt offen, ob mit der „Übermittlung“ die Übermittlung von Daten vom Auftragnehmer an einen Drittempfänger gemeint ist oder die Übermittlung vom Auftraggeber an den Auftragnehmer.

Unklar ist in Art. 26 Abs. 4 DS-GVO geblieben, wie die Rechtslage sein soll, wenn die verantwortliche Stelle – aus welchen Gründen auch immer – einen Dienstleister einschaltet, dieser aufgrund der zivilrechtlichen Vertragsgestaltung aber kein klassischer Auftragsdatenverarbeiter ist, wie etwa ein Steuerberater. Denn dem Wortlaut des Art. 26 Abs. 1 in Verbindung mit Abs. 2 DS-GVO müsste man auch mit einem solchen Dienstleister einen Vertrag abschließen, der den Anforderungen einer Auftragsdatenverarbeitung entspricht und unter anderem die strenge Weisungsgebundenheit regelt. Eine solche wird aber bei vielen Dienstleistern nicht gegeben und nicht gewollt sein. Im Widerspruch dazu steht Art. 26 Abs. 4 DS-GVO, der dann doch auch andere Dienstleister als „Auftragsdatenverarbeiter“ zulässt, ohne dass die Restriktionen des Art. 26 Abs. 2 DS-GVO gelten. Um diese Unstimmigkeit auszuräumen, müsste zumindest in Art. 26 Abs. 1 DS-GVO auf die Ausnahmemöglichkeit nach Art. 26 Abs. 4 DS-GVO hingewiesen werden.

Die deutsche Fassung des Art. 26 Abs. 1 DS-GVO enthält einen **Übersetzungsfehler**: Der Begriff der „betreffenden“ technischen und organisatorischen Maßnahmen ist unklar, richtigerweise müsste es „angemessene“ oder „geeignete“ Maßnahmen heißen („**appropriate** technical and organisational measures“).

Unklar ist, was damit gemeint ist, dass diese Maßnahmen die „Rechte der betroffenen Person“ schützen sollen. Denn es geht dem Kontext nach um den Schutz von Daten und nicht von Rechten (zudem: welcher?).

Auf Bedenken stößt die Regelung des Art. 26 Abs. 5 DS-GVO, wonach die Kommission einmal mehr delegierte Rechtsakte erlassen und Kriterien und Anforderungen für die Verantwortlichkeiten, Pflichten und Aufgaben des Auftragnehmers festlegen soll, ebenso wie Bedingungen zur Verarbeitung von Daten in Unternehmensgruppen. Bereits der Rechtsicherheit und -klarheit wegen sollten dazu in der DS-GVO materielle Regelungen aufgenommen werden.

In diesem Zusammenhang ist zu betonen, dass Regelungen zum erleichterten Austausch von personenbezogenen Daten innerhalb eines Konzerns/einer Unternehmensgruppe, dringend nötig geworden sind (**„Konzernprivileg“**), insbesondere auch betreffend eines Datenaustausches über die Grenzen der EU hinweg. Es besteht ein starkes Regelungsbedürfnis. Schon wegen der praktischen Bedeutung der Datenverarbeitung im Konzern kann es nicht angehen, dass in der DS-GVO keinerlei Regelungen getroffen werden.

6. Zu begrüßen ist, dass in **Art. 30 DS-GVO (Datensicherheit)**am Grundsatz „Datenschutz durch Technik“ festgehalten und dieser besonders betont wird. Die Erfahrung zeigt, dass der technischen und organisatorischen Absicherung eine stark gestiegene Bedeutung zukommt, da selbst ein technologieneutrales Recht oft der technischen Realität hinterherhinkt **und** ein technischer Schutz dann umso wichtiger ist.

   Ebenso positiv ist, dass weiterhin die Angemessenheit von Maßnahmen betont wird, um einzelfallspezifisch entscheiden zu können. Gleiches gilt für den Begriff „Stand der Technik“, der technologieneutral und damit zukunftsfähig ist. In Deutschland wurden damit (siehe die Anlage zu § 9 BDSG) gute Erfahrungen gemacht.

   Auf Bedenken stoßen die Regelungen in Art. 30 Abs. 3 und 4 DS-GVO, wonach die Kommission durch delegierte Rechtsakte und Durchführungsbestimmungen u.a. die „Kriterien und Bedingungen“ für die technischen und organisatorischen Maßnahmen festlegen soll, ebenso wie den Stand der Technik. Es ist nicht die Aufgabe einer Behörde, den Stand der Technik festzulegen. Vielmehr ergibt sich dieser aus dem Markt und der Technik selbst, ist höchst volatil und zudem fallspezifisch. Er kann sich zudem binnen weniger Monate ändern. Es gibt auch nicht „den“ Stand der Technik, sondern dieser setzt sich aus einer Vielzahl von einzelnen Fragestellungen und Beurteilungen zusammen. Allenfalls könnte man sich vorstellen, dass die Kommission periodisch Erhebungen machen lässt, und den Stand der Technik als Orientierung (mehr nicht) in einer Mitteilung (mehr nicht) darstellt.

   Unklar ist das Verhältnis von Art. 30 DS-GVO zu Art. 23 Abs. 1 DS-GVO („Datenschutz durch Technik“). Insbesondere fehlt in Art. 23 Abs. 1 DS-GVO – anders als in Art. 30 DS-GVO – die Grenze der Verhältnismäßigkeit.

7. Das Anliegen des **Art. 18 DS-GVO („Recht auf Datenübertragbarkeit“)** ist es, Daten „portabel“ („übertragbar“) zu machen. Bei der Formulierung hat man ersichtlich vor allem an Facebook und andere soziale Netzwerke gedacht. Dem Facebook-Nutzer soll es durch „Portabilität“ erleichtert werden, zu einem anderen Anbieter von Netzwerken zu wechseln.

   Die in Art. 18 DS-GVO getroffene Regelung dient nicht dem Schutz der Privatsphäre. Es geht vielmehr um Verbraucherschutz in einem tendenziell monopolistisch strukturierten Markt. Und es kann nicht richtig sein, den Schutz der Privatsphäre zum Vorwand zu nehmen, um mit den Mitteln der Regulierung das Marktgeschehen zulasten einzelner Anbieter zu beeinflussen. Der Einfluss, den Anbieter wie Facebook oder auch Google aufgrund ihrer monopolistischen oder jedenfalls monopolähnlichen Stellung haben, mag das europäische Kartellrecht auf den Plan rufen. Es wäre eine problematische Entwicklung, wenn etwa der Europäische Datenschutzausschuss, zu dessen Aufgaben die Durchsetzung des Art. 18 DS-GVO zählen würden, zu einer umfassenden europäischen Regulierungsstelle ausgebaut würde, die über den Datenschutz hinaus in den (nicht nur) europäischen Datenverkehr eingreifen könnte, um Ungleichgewichten entgegenzuwirken.

   Nach Art. 18 Abs. 1 DS-GVO soll dem Betroffenen ein Recht auf Herausgabe „seiner“ elektronischen Daten in einem von ihm „weiter verwendbaren strukturierten gängigen

elektronischen Format“ zustehen. Als Begründung dazu findet sich in Erwägungsgrund Nr. 55 der Hinweis auf eine „bessere Kontrolle“ über die eigenen Daten und eine Verbesserung der Ausübung des Auskunftsrechts.

Auskunft und Herausgabe von Daten sind jedoch zwei gänzlich unterschiedliche Dinge: Eine Auskunft beinhaltet die – wie auch immer verkörperte – Information darüber, welche personenbezogenen Daten die verantwortliche Stelle vom Betroffenen hat, woher diese stammen, etc. Zweck ist also die Information des Betroffenen darüber, welche Daten die verantwortliche Stelle gespeichert hat. Eine solche Auskunft kann beispielsweise in Papierform erteilt werden, eine seit vielen Jahren in Deutschland etablierte Form der Auskunftserteilung.

Ein Herausgabeanspruch dagegen zielt auf etwas anderes ab, zudem dann, wenn – wie hier – die Herausgabe in einem bestimmten Format geschuldet ist. Denn dann geht es darum, den Empfänger durch eine mehr oder weniger aufwändige Aufbereitung der Daten in einem bestimmten Format selbst in die Lage zu setzen, mit den Daten möglichst einfach und ohne weiteren Aufwand weiter arbeiten zu können. Zweck der Herausgabe ist nicht die Information, denn diese kann er auch anders erlangen. Zweck ist vielmehr eine Arbeitserleichterung für den Empfänger.

Betrachtet man den Aufwand für die Unternehmen, der mit einer Datenaufbereitung zur Herausgabe nötig ist, etwa bei einem Kundenstamm mit mehreren Millionen Kunden und einer Vielzahl von Daten jedes einzelnen Kunden und langjährigen Geschäftsbeziehungen, schießt der Anspruch auf Datenherausgabe im Sinne einer bloßen Informationsverbesserung weit über das – gemäß den Erwägungsgründen verfolgte – Ziel hinaus.

Hinsichtlich des Formats muss zudem einerseits im Interesse einer Technologieneutralität mit unbestimmten Begriffen gearbeitet werden, sodass bereits jetzt Diskussionen dazu vorprogrammiert sind, welche Formate jeweils „gängig“ sind. Was soll passieren, wenn die verantwortliche Stelle zwar die Daten in einem „gängigen Format“ bereitstellt, der Betroffene aber die Daten – aus welchen Gründen auch immer – dennoch nicht „weiter verwenden“ kann? Zudem: Was soll ein „strukturiertes“ gängiges elektronisches Format sein? Sind elektronisch erfasste Daten nicht – denklogisch – immer „strukturiert“? Reicht eine Excel-Tabelle? Was, wenn die Software der verantwortlichen Stellen – etwa aus Datenschutz- und Sicherheitsgründen – gerade keinen solchen Export zulässt?

Insgesamt stößt auch die subjektive Komponente des Art. 18 Abs. 1 DS-GVO, wonach die Daten speziell vom Betroffenen weiter verwendet werden können müssen, auf große Bedenken.

Die (äußerst fragwürdige) Regelung in Art. 18 Abs. 3 DS-GVO, wonach die Kommission das Format „festlegen“ kann, lässt zudem die Frage aufkommen, warum dann in Art. 18 Abs. 1 DS-GVO von einem „gängigen“ Format die Rede ist.

Nachbesserung bedarf auch folgender Aspekt: Was genau sind die „verarbeiteten Daten“, von denen eine Kopie herauszugeben ist? Auch die Daten anderer Personen, die – etwa in Social Networks – mit den personenbezogenen Daten des Betroffenen

in Zusammenhang stehen? Warum aber soll die verantwortliche Stelle Aufwand haben, auch diese für den Betroffenen „fremden“ Daten für den Betroffenen in ein für diesen weiter verwendbares und daneben noch „strukturiertes gängiges elektronisches Format“ zu bringen?

Eine weitere offene Frage: In welchem Verarbeitungsstadium soll die Kopie der verarbeiteten Daten herausgegeben werden? In dem Stadium direkt nach der Erhebung? Nach der Hälfte der Verarbeitung? Was, wenn die Daten gleichzeitig in verschiedenen Verarbeitungsstadien vorliegen?

8. Bei **Art. 5 lit. e DS-GVO** gibt es in der deutschen **Übersetzung** einen sinnentstellenden Fehler, der bereits zu vielen Missverständnissen geführt hat. Die Übersetzung muss richtigerweise lauten, dass personenbezogene Daten nur so lange gespeichert werden **„dürfen“** (statt **„müssen“**) wie nötig. Die jetzige (deutsche) Formulierung statuiert eine (ungewollte) Identifizierungspflicht.