**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
17(4)584 B

**Stellungnahme für die Anhörung im Bundestags-Innenausschuss**
**am 22.10.2012**
**zur EU-Datenschutz-Grundverordnung / nichtöffentlicher Bereich**

Prof. Dr. Ralf B. Abel

1. Vorbemerkung

   a. Der Gegenstand der Anhörung ist zu umfangreich und komplex, um alle Aspekte hier ansprechen zu können. Die nachfolgende Stellungnahme befaßt sich daher vorrangig mit grundlegend konzeptionellen und verfassungsrechtlichen Gesichtspunkten.

   b. Ganz generell handelt es sich um ein Gesetzgebungsvorhaben von grundsätzlicher Bedeutung. Es hat weitreichenden Folgen für alle persönlichen und wirtschaftlichen Lebensbereiche und führt wegen seiner Breitenwirkung dazu, dass wesentliche und für die wirtschaftliche und gesellschaftliche Entwicklung in Deutschland grundlegende Bestimmungen der Gestaltungsmöglichkeit der deutschen Gesetzgeber (Bund und Länder) dauerhaft entzogen werden. Es bedarf daher einer besonders gründlichen Überprüfung der Konzeption und der einzelnen Regelungen des Entwurfs, da nach Inkrafttreten eine Veränderung durch deutsche Parlamente kaum noch möglich sein wird.

   c. Die Vereinheitlichung des Datenschutz- und des Informations-/ IT-Rechts in Europa ist in seiner Zielrichtung zu begrüßen. Die vorgeschlagene Datenschutz- Grundverordnung (zukünftig: GVO) ist in der vorliegenden Form jedoch nicht geeignet, die wünschenswerten und selbstgesteckten Ziele zu erreichen. Grund dafür sind eine unangemessene Regelungsstruktur (2), konzeptionell angelegte Systemfehler (3), verfassungsrechtlich bedenkliche wenn nicht sogar verfassungswidrige Bestimmungen (4) und eine Vielzahl schwer oder nicht umsetzbarer Einzelvorschriften (5).

2. Unangemessene Regelungsstruktur des Entwurfs

   Regelungsgegenstand der GVO ist eine elementare Funktion moderner Gesellschaften, nämlich die Nutzung von Information (dem „Öl der Wissensgesellschaft“)und die Generierung und Verwendung von Wissen. Daten sind dafür Mittel zum Zweck. Die GVO unterwirft diese zentralen Elemente der modernen Wissensgesellschaft pauschal und in toto einem strengen, unflexibel organisierten und bürokratisch überformten Regime. Es fehlt an einer sachangemessenen Differenzierung zwischen regulierungsbedürftigen Sachverhalten einerseits und an-

dererseits solchen, die die Persönlichkeitsrechte in geringerem Maße tangieren und in ihrer Wahrnehmung Ausprägung der Informations-, Kommunikations- und Berufsfreiheit sowie des Eigentumsgrundrechts sind.

Regulierungsbedürftig erscheinen Verarbeitungsvorgänge, die ihrem Wesen nach weltweit angeboten, global vermarktet und/oder durch monopolartige Unternehmensstrukturen, oft mit Sitz in Drittstaaten, vorgenommen werden. Das sind in erster Linie die sozialen Netzwerke und vergleichbare kommunikationstechnische Infrastrukturen. Für die „traditionellen" Formen der Gewinnung, Aufbewahrung und Nutzung von Wissen mit Hilfe IT-technischer Systeme müssen hingegen Regeln gelten, die auf einer Abwägung der jeweils tangierten Grundrechte im Sinne praktischer Konkordanz beruhen.

Zu wünschen ist daher für die GVO ein Allgemeiner Teil, der anerkannte Prinzipien bei der Informationsverarbeitung zur Wahrung der Persönlichkeitsrechte in allgemeiner und damit flexibler Form festlegt und bei Eingriffen namentlich in das Informationsgrundrecht dem Verhältnismäßigkeitsgrundsatz durch ein durchgängiges Abwägungsgebot Rechnung trägt.

Der in nichtöffentlichen Bereich geltende Freiheitsgrundsatz muß dabei den Regelfall bilden. Eingriffe in die Freiheitsrechte aus Art. 5, 12 und 14 GG müssen, wie z.B. beim Äußerungsrecht, die Ausnahme bleiben. Verarbeitungsformen wie z.B. soziale Netzwerke, Clouds oder vergleichbare Infrastrukturen, für die ein spezifischer Regelungsbedarf besteht, sollten in einem Besonderen Teil jeweils bereichsspezifisch normiert werden.

3. Konzeptionell angelegte Systemfehler

Die GVO leidet unter drei grundlegenden Systemfehlern. Diese falschen Weichenstellungen determinieren in der Konsequenz zahlreiche problematische Einzelbestimmungen.

a. Der Anwendungsbereich der GVO ist uferlos. Er umfasst nahezu die gesamte Datenverarbeitung. Grund dafür ist die äußerst weite Definition des personenbezogenen Datums in Artikel 4 Abs. 3. Berücksichtigt man die schon nach heutigem Recht sehr weite Auslegung dieses Begriffs durch die Gruppe 29, werden nahezu alle Daten als personenbezogen gelten können, da sie sich immer zumindest theoretisch irgendwie auf Personen beziehen lassen könnten. Das wäre auch im kommenden „Internet der Dinge" der Fall (Beispiel: Inhalt des Kühlschranks= personenbezogen, da es sich um den Kühlschrank be-

stimmter Personen handelt). Damit wird es zukünftig kaum noch Daten geben, die nicht unter das Regime der GVO fallen. Konsequenterweise enthält die GVO keine Sonderbestimmungen mehr über anonymisierte bzw. pseudonymisierte Daten, da auch diese zumindest theoretisch natürlichen Personen zugeordnet werden können und damit unter die Definition des Artikel 4 Abs.3 fallen. Damit erfaßt die GVO mit ihren engen und starren Regelungen faktisch die gesamte Informations- und Wissensverwendung im nichtöffentlichen Bereich.

Wünschenswert ist daher die Beschränkung des Anwendungsbereichs auf personenbezogene Daten im Sinne von § 3 Abs.1 BDSG in einer restriktiven Auslegung und die Fokussierung des Schutzbereichs auf die Verletzung von Persönlichkeitsrechten.

b. Die GVO missachtet die z.T. fundamentalen Unterschiede zwischen den verschiedenen Verarbeitungsformen von Information, indem sie – mit wenigen Ausnahmen in Art.80 bis 85 – den gesamten Umgang mit Information und Wissen schematisch gleich behandelt, unabhängig davon, ob es sich um weltweit verbreitete, monopolartige Strukturen wie etwa soziale Netzwerke oder ob es sich um die „traditionelle“ Verarbeitung von Daten durch Privatpersonen, Selbständige und Unternehmen handelt. Diese Gesetzgebung widerspricht damit dem Verhältnismäßigkeits- und dem Gleichbehandlungsgrundsatz (Artikel 2 und 5 Abs.4 EUV).

   Dadurch führen zahlreiche Einzelregelungen zu einer in vielen Bereichen unverhältnismäßigen Einschränkung der Informationsfreiheit des Art. 5 GG und der Grundrechte aus Art. 14, Art. 12 GG im deutschen Recht und der Rechte aus Art. 11, 15, 16 und 17 der europäischen Grundrechte-Charta.

   Wünschenswert wäre daher die Trennung in allgemeine und in bereichsspezifische Bestimmungen.

c. Ein weiterer Systemfehler liegt in der strikten Einführung und Festschreibung des Verbotsprinzips (Art. 6 i.V.m. Art. 5). Damit gemeint ist das generelle Verbot der Verarbeitung personenbezogener Date, es sei denn, es lägen Erlaubnistatbestände vor. Dieses Regelungsmodell entstammt dem öffentlichen Bereich, indem es aufgrund des Gesetzesvorbehalts für jeden Grundrechtseingriff und damit für jede staatliche Verarbeitung personenbezogener Daten eine Legitimationsgrundlage erfordert. Im Verhältnis zu Privaten hingegen bildet das Verbot mit Erlaubnisvorbehalt im deutschen (und europäischen) Rechtssystem die –seltene- Ausnahme, etwa beim Atom- oder Waffenrecht.

Weder im – bekanntlich gefahrgeneigten – Straßenverkehrsrecht noch im Presse- und Äußerungsrecht wäre ein derartiges Prinzip denkbar bzw. verfassungsgemäß.

Mit dem Verbotsprinzip soll nunmehr ein dem BDSG zugrundeliegendes öffentlich-rechtliches Regelungsmodell europaweit festgeschrieben und zementiert werden, obwohl gerade dieses Prinzip in Deutschland mittlerweile von Wissenschaft und Praxis immer stärker in Frage gestellt wird und – mit Ausnahme vor allem der öffentlichen Datenschutzbeauftragten – als sachlich unangemessen und als ein Entwicklungshemmnis für ein modernes Datenschutzrecht betrachtet wird.

Im nicht-öffentlichen Bereich bedeutet das Verbotsprinzip einen erheblichen Eingriff in das Grundrecht auf freie Beschaffung und kreative Nutzung von Information und Wissen und in die Freiheit der Netzkommunikation (Art.5 GG). Es beschränkt gleichermaßen die wirtschaftliche Betätigungsfreiheit (Art. 12, 14 GG).

In der vernetzten Informationsgesellschaft, in der die automatisierte (= computergestützte) Verarbeitung personenbezogener Daten zum ubiquitären Grundmuster des Alltagsverhaltens im wirtschaftlichen, nichtkommerziellen und im privaten Bereich geworden ist, bedeutet das geplante Verbotsprinzip somit einen massiven Grundrechtseingriff, dessen verfassungsrechtliche Legitimation dem strikten Verhältnismäßigkeitsgrundsatz unterliegt. Bislang fehlt es bereits an empirischen Belegen für die Geeignetheit und erst recht für die Erforderlichkeit einer derart weitgehenden, unterschiedslosen Freiheitseinschränkung.

Im Gegenteil erweist sich schon das im BDSG verankerte Verbotsprinzip immer weniger als praxistauglich, obwohl es wegen mancher Ausnahmeregelungen und mancher Möglichkeit zur Güterabwägung (z.B. in den §§ 28 bis 30 BDSG), die der GVO fehlen, milder ausgestaltet ist. Die Notwendigkeit, in den durchweg komplexen Verarbeitungsvorgängen für jeden einzelnen Verarbeitungsschritt eine verlässliche Rechtsgrundlage zu finden, stößt angesichts der Vielzahl der DV-technischen Prozesse, ihrer Verarbeitungsdichte und Verarbeitungstiefe schon jetzt und erst recht bei der Fortentwicklung zu einem ‚Internet der Dinge' an seine Grenzen. Ein Beispiel dafür ist die faktische Unmöglichkeit, DV-Vorgänge in der Cloud mit vertretbarem Aufwand konform mit deutschem Datenschutzrecht durchzuführen. Es sind private Vereinigungen, die über Gütesiegel und Transparenzregeln Datenschutz auf privatrechtlicher Ebene verbessern wollen (z.B. EuroCloud Deutschland_eco, Cloud Security

Alliance – CSA). Der Gesetzgeber wäre und ist damit überfordert.

Ein zukunftsweisendes und verfassungskonformes Informationsumgangsrecht für den nicht-öffentlichen Bereich muß daher vom überholten Konzept des Verbots mit Erlaubnisvorbehalt abgehen.

Gegenstand und Ziel der europäischen Gesetzgebung kann und darf somit nicht die kleinteilige und tiefgestaffelte Regelung technisch-organisatorischer Vorgänge sein. Vielmehr muß, ergebnisorientiert, der Schutz der Persönlichkeitsrechte Betroffener verbessert werden. Ob eine bestimmte Datenverarbeitung Persönlichkeitsrechte verletzt, ist freilich kontextabhängig und kann daher nicht, bezogen auf den technischen Vorgang „Datenverarbeitung", pauschal beurteilt und schematisch geregelt werden. So gelten bspw. Einkommensverhältnisse im Falle von Angestellten in der Privatwirtschaft in der Regel als besonders schutzwürdige Arbeitnehmerdaten, im Falle öffentlicher Bediensteter/Beamter dagegen sind deren Arbeitseinkommen öffentlich. Die Schutzwürdigkeit von Informationen hängt also nicht ab von der formalen Eingruppierung der Daten in eine bestimmte rechtliche Kategorie, sondern von ihrem jeweiligen Verwendungszusammenhang.

Ein zukunftsfähiges Datenschutzrecht darf sich daher nicht an einzelnen Verfahrensschritten abarbeiten, sondern muss sich daran orientieren, ob das Ergebnis eines Verarbeitungsvorgangs Persönlichkeitsrechte konkreter Betroffener verletzt oder nicht.

4. Verfassungsrechtlich bedenkliche Bestimmungen

a. Geplant ist die Einrichtung „völlig unabhängiger" Aufsichtsbehörden (Art. 47 f), deren Struktur und Aufgabenzuweisungen zu einem elementaren Verstoß gegen den Grundsatz der Gewaltenteilung führen:

Die Datenschutzaufsichtsbehörden sind, nicht anders als z.B. Gewerbeaufsichtsämter oder Ämter für die Lebensmittelüberwachung, Teile der vollziehenden Gewalt mit beträchtlichen Eingriffsbefugnissen (Art. 52 f, 79).

Gleichzeitig sollen sie - allein oder in interner Abstimmung – Einzelfragen klären, d. h. sie sind in der Konsequenz durch Überwachungs- und Genehmigungsermächtigungen befugt, die Verordnung verbindlich auszulegen und damit den materiellrechtlichen Gesetzesinhalt zu bestimmen (Art. 52, 53, 34). Sie erhalten damit faktisch die Stellung und Funktion eines Nebengesetzgebers.

Die Einhaltung der von ihnen für richtig gehaltenen Gesetzesinterpretation können und sollen durch abschreckende und empfindliche Sanktionen erzwungen werden können (Art. 78 Abs.1, 79).

Die Aufsichtsbehörden sind darüber hinaus berufen, neue Verarbeitungsformen bzw. Geschäftsmodelle, die sie für relevant halten, vorab zu genehmigen (Art. 34 i.V.m. Art 33). Damit wird es den Aufsichtsbehörden möglich, unmittelbaren Einfluss auf die inhaltliche Gestaltung von Datenverarbeitungsvorgängen bei Privaten zu nehmen und somit de facto eine zensurähnliche Funktion bei der IT- und netzgestützten Gewinnung und Nutzung von Information und Wissen im nahezu gesamten nichtöffentlichen Bereich auszuüben. Jede Kontrolle über die Inhalte von Daten- und Informationsverarbeitung durch staatliche Aufsichtsbehörden bedeutet in letzter Konsequenz eine moderne Form der Zensur, und zwar unabhängig davon, ob es um eine Überwachung der in soziale Netzwerke eingestellten Inhalte oder um die Kontrolle und Bewertung "klassischer" Datenverarbeitungsvorgänge im nichtöffentlichen Bereich geht.

Die Einstellung von Inhalten ins Netz fällt jedoch unter die Ausübung der Meinungsfreiheit. Die im Äußerungs- und Presserecht entwickelten Kriterien zeigen deren Grenzen auf. Sie sind technikneutral und können daher für das Internet gleichermaßen Geltung beanspruchen wie für den Offline-Bereich. Dabei kann es auch keine Rolle spielen, ob eine Veröffentlichung von einem marktmächtigen Presseorgan, einer kleineren Publikation oder von einem einzelnen Bürger stammt („Blogs"). Entscheidend ist das Grundrecht, seine Meinung frei zu äußern und sich frei zu informieren.

Ebenso verhält es sich, wenn Aufsichtsbehörden das Recht erhalten, DV-technische Anwendungen in Unternehmen umfassend zu bewerten und bestimmen zu dürfen, welche Daten und welche Verarbeitungsmethoden für welche Zwecke als erforderlich oder auch nicht anzusehen sind (Art. 34). Das wird am Beispiel der Nutzung mathematisch-statistischer Verfahren zur Informationsgewinnung und –bewertung, die meist mit den pauschalen Begriffen „Scoring" oder „Profiling" belegt und rechtspolitisch von vielen Verbraucherschützern und Aufsichtsbehörden abgelehnt werden, besonders augenfällig. Nach höchstrichterlicher Rechtsprechung in Deutschland fallen derartige und andere Bewertungen unter die Meinungsfreiheit, sei es die Bewertung der Qualität und/oder der persönlichen Eigenschaften einer Lehrperson („Spickmich.de") oder sei es die Bonitätseinschätzung potenzieller Vertragspartner. Dass es hier Transparenzansprüche und Korrekturmöglichkeiten für den Betroffenen geben muss, ist unstreitig und bereits im BDSG verankert, ändert aber nichts am Grund-

satz, dass keiner staatlichen Behörde das Recht zuerkannt werden darf, Art und Umfang der jeweiligen Datennutzung aus eigener Machtbefugnis festzulegen. Auch darin läge Zensur.

Gerichtlicher Rechtsschutz wird nur begrenzt möglich sein: Nur wenige Private oder Unternehmen werden nach den bisherigen Erfahrungen bereit und in der Lage sein, die Kosten und das Reputationsrisiko langwieriger gerichtliche Rechtsstreitigkeiten auf sich zu nehmen. Kein Unternehmen kann es sich angesichts der heute oft nur wenige Monate dauernden Innovations- und Entwicklungszyklen leisten, monate- oder jahrelange Abstimmungs- bzw. Genehmigungsprozeduren oder letztinstanzliche Gerichtsentscheidungen durch den EuGH abzuwarten.

b. Die „völlige Unabhängigkeit“ der Aufsichtsbehörden, wie sie den Entwurfsverfassern vorschwebt, würde einen ministerialfreien Raum in einem Bereich schaffen, der von grundsätzlicher Bedeutung mit weitreichenden Folgen für fast alle Lebensbereiche ist. Dies widerspräche eklatant fundamentalen deutschen Verwaltungsgrundsätzen und letztlich auch dem Demokratieprinzip, indem die Bindung des Exektivorgans Aufsichtsbehörde an demokratisch legitimierte und beeinflußbare Kontrollinstanzen vollständig beseitigt wird. Eine derartig weitgehende Unabhängigkeit läßt sich dem Primärrecht (Art. 8 GrdRCharta) nicht entnehmen; die vielfach als falsch und überzogen empfundene Rechtsprechung des EuGH zur „völligen Unabhängigkeit“ ließe sich durch den sprichwörtlichen „Federstrich des (EU-) Gesetzgebers anhand der Grundsätze des deutschen Staatsrechts korrigieren.

   Wünschenswert wäre daher zumindest die strikte Trennung von Aufsicht/ Kontrolle einerseits (nach dem Muster der Staatsanwaltschaften oder der Rechnungshöfe) und Eingriffsbefugnissen andererseits, die regulären Verwaltungsbehörden übertragen werden sollten. Wünschenswert wäre ferner die Rücknahme des ministerialfreien Raumes bei den Aufsichtsbehörden für den nichtöffentlichen Bereich. (Der öffentliche Bereich ist nicht Gegenstand dieser Stellungnahme).

c. Verfassungsrechtlich höchst bedenklich und daher abzulehnen ist die Fülle an Ermächtigungen, die es der Kommission gestatten, ohne Hinzuziehung des EP oder der nationalen Parlamente detaillierte Einzelregelungen zu schaffen. Durch derartige Einzelregelungen kann die Kommission das materielle Recht maßgeblich beeinflussen, etwa hinsichtlich der ins Auge gefassten Zertifizierungsverfahren. Damit lägen wesentliche Teile der Rechtsetzung allein in der Hand der Exekutive, denn Zertifizierungsverfahren sind geeignet, faktische Standards mit normativer Kraft zu setzen.

5. Einzelregelungen

a. Problematisch ist die faktische Abschaffung der in Deutschland bewährten Institution des betrieblichen Datenschutzbeauftragten durch die ausnahmslose Festsetzung einer Mindestschwelle von 250 Mitarbeitern. Es ist zwar nachvollziehbar, dass die obligatorische Einführung betrieblicher Datenschutzbeauftragter in anderen Ländern, die bisher kein derartiges Institut kennen, nur schrittweise durchgesetzt werden kann. Es gibt aber keinerlei Veranlassung, das bewährte deutsche Modell faktisch abzuschaffen. Es ist daher – so wie in anderen Bereichen auch, etwa dem Arbeitnehmerdatenschutz – eine nationale Öffnungsklausel erforderlich, die datenschutzreundlichere Regelungen gestattet.

b. Problematisch ist ferner die pauschale Übertragung von Bestimmungen, die gegenüber sozialen Netzwerken und bestimmten Erscheinungen des Internet Sinn machen, z. B. Löschungsansprüche („Recht auf Vergessen“) oder der Anspruch auf Übertragung der Daten auf einen anderen Anbieter („Recht auf Datenübertragbarkeit“), auf sämtliche Formen der Datenverarbeitung. Auch das extensiv ausgestattete Widerspruchsrecht (Art. 19) kann dort sinnvoll sein, wo der Betroffene in urheberähnlicher Weise selbst Informationen bereitstellt. Für die allgemeine Informationsverarbeitung bleibt die Feststellung des Bundesverfassungsgerichts im Volkszählungs-Urteil gültig, wonach der Mensch kein Robinson, sondern ein gemeinschaftsgebundenes Wesen ist und es daher kein Eigentumsrecht an den ihn betreffenden Datum gibt.

   Es muß daher sichergestellt werden, dass das Widerspruchsrecht ebenso wenig eine Handhabe für eine Verfälschung und Manipulation von Lebenssachverhalten gibt wie für die Unterdrückung von Transparenz und Meinungsfreiheit im Internet.

6. Mögliche Verbesserungen

   a. Rechtssystematisch bietet sich eine Kombination

      - unbestimmter Rechtsbegriffe mit positiv formulierten Rechtsansprüche des Betroffenen einerseits und
      - gesetzgeberischen Grenzziehungen andererseits an, wobei insbesondere das Lauterkeits- und das ABG-Recht als Strukturvorlage dienen können.

Ergänzend hierzu ist ein

- regulatorischer Rahmen

vorzuschlagen, der äußere Bedingungen für bestimmte Formen der Datenverarbeitung regelt, die zivilrechtlich oder über vertragliche Inhaltskontrolle nicht ausreichend geregelt werden können. Beispiele dafür finden sich bei der TK-Regulierung oder im Kartellrecht. Gerade gegenüber monopolartigen Strukturen und Oligopolen auf der Anbieterseite wäre beispielsweise über eine Versorgungspflicht ebenso wie eine striktere Erstreckung des Fernmeldegeheimnisses nachzudenken. Ob sich für eine gesetzestechnische Verortung das Datenschutzrecht anbietet, erscheint eher fraglich. Vielmehr ist auch eine Ankoppelung an das Telekommunikationsrecht erwägenswert.

b. Bei einer Verbesserung des zivilrechtlichen Persönlichkeitsschutzes, aber auch in Hinblick auf den Rechtsschutz aller Beteiligter im Rahmen der GVO bedarf es flankierender prozessrechtlicher Instrumente, die eine effektive und schnelle Rechtsdurchsetzung ermöglichen.