verbraucherzentrale Bundesverband

29. Februar 2012

Modernisierung des europäischen Datenschutzrechts

Stellungnahme des Verbraucherzentrale Bundesverbandes

zum Entwurf der EU-Kommission für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

Verbraucherzentrale Bundesverband e.V. – vzbv
Fachbereich Wirtschaft
Markgrafenstr. 66
10969 Berlin
wirtschaft@vzbv.de
www.vzbv.de

I. Einleitung

Der Verbraucherzentrale Bundesverband unterstützt die EU-Kommission in ihren Bestrebungen, für einen verbesserten, harmonisierten und modernen Datenschutz in Europa zu sorgen. Der Datenschutz ist vor allem durch die digitale Entwicklung zu einem immer wesentlicheren Teil des Verbraucherschutzes geworden. Eine Modernisierung ist dringend notwendig, um den Schutz der persönlichen Daten und die Privatsphäre der Verbraucher auch in Zukunft zu gewährleisten und gleichzeitig die Rechtssicherheit und Wettbewerbsfähigkeit der europäischen Unternehmen zu stärken.

Viele der in dem Kommissionsentwurf genannten Regelungsvorschläge greifen langjährige Forderungen des Verbraucherzentrale Bundesverbandes auf. Dies gilt insbesondere hinsichtlich der Transparenz der Verarbeitung von personenbezogenen Daten und der Einführung des Prinzips „data protection by default“. Auch begrüßt der Verbraucherzentrale Bundesverband, dass die Durchsetzung des geltenden europäischen Rechts gegenüber hier tätigen Unternehmen mit Sitz im außereuropäischen Ausland forciert werden soll.

Leider wurden jedoch in dem vorliegenden Entwurf bereits einige der guten Ansätze verwässert, die in vorher bekannt gewordenen Fassungen enthalten waren. So ist etwa die Notwendigkeit einer Einwilligung für die Nutzung von Daten zu Zwecken des Direktmarketings nicht mehr vorgesehen. Außerdem wurden die möglichen Sanktionen bei Missachtung der Verordnung entschärft. **Der Verbraucherzentrale Bundesverband spricht sich dafür aus,** diese Änderungen zu revidieren und im Laufe des Gesetzgebungsprozesses **von weiteren Verschlechterungen** der Vorschläge und des Datenschutzniveaus der Verbraucher **abzusehen. Die Regelungen der Verordnung dürfen auf keinen Fall hinter den bisher geltenden Gesetzen der Mitgliedsstaaten der Europäischen Union zurückbleiben.**

Kritisch betrachtet der Verbraucherzentrale Bundesverband insbesondere den Vorschlag, dass zukünftig nur der Datenschutzbeauftragte des Staates zuständig sein soll, in dem ein Unternehmen seine Hauptniederlassung hat, falls sich die Datenverarbeitung über mehrere EU-Mitgliedsstaaten erstreckt. **Der Bürokratieabbau bei den Unternehmen darf nicht zu einer Verschlechterung des Rechtsschutzes der Verbraucher führen.**

Der Verbraucherzentrale Bundesverband fordert die Institutionen der Europäischen Union auf, **die Rechte der einzelnen Verbraucher / Bürger konsequent ins Zentrum der Ausgestaltung der Datenschutz-Grundverordnung zu stellen** und nicht etwa das Interesse der Wirtschaft am „freien Verkehr personenbezogener Daten in der Union“. Ausgangspunkt der Betrachtungen und Ausgestaltung des Datenschutzes ist zwingend das Individuum und sein Recht auf Souveränität über seine Daten auch und gerade in der digitalen Welt.

Insgesamt sieht der Verbraucherzentrale Bundesverband die Kommission mit diesem Entwurf aber auf einem guten Weg, den Datenschutz in Europa auf ein zeitgemäßes Niveau zu hieven und den Schutz sowie die Rechte der Verbraucher zu stärken.

II. Die Positionen in der Zusammenfassung

1. Räumlicher Anwendungsbereich der Verordnung (Artikel 3)

Der Vorschlag der Kommission zum räumlichen Anwendungsbereich der Verordnung ist begrüßenswert. Eine solche Regelung kann allerdings nur wirksam sein, wenn es internationale Abkommen zur Rechtsdurchsetzung gibt. Daher muss die Europäische Union solche Abkommen zu ihrer Priorität machen.

2. Verarbeitung personenbezogener Daten eines Kindes (Artikel 4, Artikel 8)

Es ist zu begrüßen, dass nach dem Entwurf der EU-Kommission Kinder besonders geschützt werden sollen. Allerdings ist nicht verständlich, warum es außerhalb von „Diensten der Informationsgesellschaft“ keine Regelung zur Einwilligung durch Minderjährige geben soll.

Die Erhebung von Daten von Minderjährigen sollte darüber hinaus besonderen Restriktionen unterliegen, die auch nicht durch Einwilligungen aufgehoben werden können. Beispielsweise sollten Kinder vom Profiling / Scoring ausgeschlossen sein.

3. Einwilligung (Artikel 7)

Es ist ausdrücklich zu begrüßen, dass zukünftig eine Einwilligung einer „expliziten Willensbekundung“ bedarf, um gültig zu sein.

Bisher fehlen in dem Entwurf aber Regelungen zum Kopplungsverbot. Die Nutzung eines Dienstes darf nicht von der Einwilligung der Verbraucher zur Nutzung ihrer Daten - über das zur Diensterbringung notwendige Maß - abhängig gemacht werden.

Darüber hinaus sollte eine zeitliche Begrenzung von Einwilligungen, beispielsweise von zwei Jahren, eingeführt werden. Danach sollten die Daten entweder gelöscht oder eine neue Einwilligung beim Verbraucher eingeholt werden müssen.

4. Information der Nutzer / Transparenz (Artikel 11, Artikel 14)

Die Einführung eines allgemeinen Transparenzgrundsatzes für die Verarbeitung personenbezogener Daten verbunden mit Pflichten zur verbesserten Darstellung von datenschutzrelevanten Informationen wird unterstützt. Damit der Betroffene aber vor Erteilung einer Einwilligung die Folgen abschätzen kann, muss er auch über die Art und den Umfang der Datenverarbeitung informiert werden.

5. Recht auf Vergessenwerden und Löschung (Artikel 17)

Das „Recht auf Vergessenwerden“ ist zu begrüßen. Der Löschwunsch eines Verbrauchers sollte aber durch Unternehmen nicht nur dann an Dritte weitergegeben werden müssen, wenn Daten öffentlich gemacht , sondern auch immer dann, wenn Daten anderweitig an Dritte übermittelt wurden. Fraglich ist bisher jedoch, wie dieser Löschanspruch in der Praxis wirksam durchgesetzt werden soll.

6. Recht auf Datenübertragbarkeit (Artikel 18)

Die Regelung würde die Kontrolle der Verbraucher über ihre Daten stärken und marktbeherrschende Stellungen von Unternehmen verringern bzw. Wettbewerb ermöglichen. Damit das Recht nicht ins Leere läuft, müssen gemeinsame Datenstandards und Schnittstellen für die Datenportabilität zwischen den Unternehmen definiert werden. Außerdem dürfen anfallende Kosten nicht auf den Verbraucher abgewälzt werden .

7. Direktwerbung (Artikel 19 (2))

Der Verbraucherzentrale Bundesverband bedauert, dass eine Einwilligung für die Nutzung und Weitergabe der Daten zu Zwecken des Direktmarketing nicht mehr vorgesehen ist. Der aktuelle Vorschlag bleibt sogar weit hinter den in Deutschland geltenden Regelungen zurück.

8. Auf Profiling basierende Maßnahmen (Artikel 20 (3))

Sensitive Daten sollten nicht zum Zwecke des Profilings / Scorings verwendet werden dürfen.

Außerdem sollte Profiling / Scoring grundsätzlich nur mit Einwilligung des Betroffenen möglich sein und Minderjährige gänzlich ausgeschlossen werden.

9. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Artikel 23)

Der Vorschlag der Kommission ist zu begrüßen, allerdings sollten die Schutzziele dieses Artikels konkreter dargestellt werden. So sollte die explizite Verpflichtung eingeführt werden, anonyme und pseudonyme Nutzungsmöglichkeiten - insbesondere von Internetdiensten - anzubieten.

10. Benennung eines Datenschutzbeauftragten (Artikel 35 (1))

Die Verpflichtung, betriebliche Datenschutzbeauftragte erst ab 250 Beschäftigten bestellen zu müssen, ist deutlich zu niedrig. Die bisher in Deutschland geltende Schwelle von 10 Mitarbeitern hat sich bewährt und sollte beibehalten werden .

11. Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen (Artikel 40 ff)

Bisherige, ähnliche Regelungen gibt es bereits jetzt, allerdings sind diese in der Praxis höchst problematisch, wie beispielsweise das „Safe Harbor Abkommen“ zwischen der EU und den USA. Es ist zu bezweifeln, dass auch die neuen Regelungen einen ausreichenden Schutz der Verbraucher sicher stellen können.

12. Unabhängigkeit (Artikel 47) sowie Ausstattung der Datenschutzaufsichtsbehörden (Artikel 49) und Kohärenzverfahren (Artikel 57)

Damit die Datenschutzbeauftragten also ihre neu hinzukommenden Aufgaben erfüllen können, müssen ihre personellen und finanziellen Ressourcen deutlich aufgestockt werden.

Darüber hinaus muss die Unabhängigkeit der Datenschutzbeauftragten gewährleistet sein, besonders auch gegenüber der EU-Kommission, den anderen nationalen (Landes-)Datenschutzbeauftragten und denen der anderen EU-Mitgliedsstaaten.

13. „One-Stop-Shop"-Regelung (Artikel 51 (2))

Eine Harmonisierung des Datenschutzrechts kann aus Verbrauchersicht große Vorteile haben, aber dieses Recht ist weiterhin in den größeren Rechtsrahmen des jeweiligen Staates eingebunden. Auch die Ressourcen der Datenschutzbeauftragten sind in den EU-Mitgliedsstaaten verschieden. Unternehmen könnten sich daher gezielt in Ländern niederlassen, in denen der Rechtsrahmen oder die Ausstattung der Aufsichtsbehörden für sie günstig sind.

Der Bürokratieabbau bei den Unternehmen darf außerdem nicht zu einer Verschlechterung des Rechtsschutzes der Verbraucher führen, indem Dauer und Komplexität der entsprechenden Vorgänge zunehmen.

14. Verbandsklagerecht (Artikel 73 ff)

Der Entwurf in der vorliegenden Formulierung ändert nichts daran, dass der Verbraucherzentrale Bundesverband auch weiterhin nur höchst eingeschränkt für Verbraucher bei Fragen des Datenschutzes die Instrumente des kollektiven Rechtsschutzes nutzen können wird, da Verbraucherschutzorganisationen nicht als klagebefugt aufgeführt werden.

15. Haftung und Recht auf Schadenersatz (Artikel 77)

Es sollte ein pauschalisierter Schadensersatz - auch bei immateriellen Schäden – in Kombination mit einer Beweislastumkehr zu Gunsten der Verbraucher eingeführt werden. Nach einer rechtswidrigen Verwendung von personenbezogenen Daten müsste der Geschädigte nicht mehr grundsätzlich einen exakt bezifferten Schaden nachweisen, sondern nur noch, wenn dieser über die Pauschale hinaus gehen würde.

16. Verschärfte Sanktionen (Artikel 78, Artikel 79)

Der Verbraucherzentrale Bundesverband bedauert, dass der maximal mögliche Bußgeldrahmen im Vergleich zu vorherigen Versionen des Verordnungsentwurfs verringert wurde. Eine Regelung vergleichbar dem deutschen Bundesdatenschutzgesetzes, nach der die Bußgelder in Ausnahmenfällen auch überschritten werden können, ist nicht vorgesehen

III. Die Positionen im Einzelnen

1. Räumlicher Anwendungsbereich der Verordnung (Artikel 3)

Aus der Sicht des Verbraucherzentrale Bundesverbands besteht eine der größten Schwierigkeiten für europäische Verbraucher in der Durchsetzung ihrer Rechte gegenüber Unternehmen ohne Niederlassung in der Europäischen Union. Daher ist der Vorschlag der Kommission zum räumlichen Anwendungsbereich der Verordnung besonders begrüßenswert.

Diese Regelung schüfe dringend notwendige Klarheit, denn bisher ist oft nicht deutlich, welches Recht gegenüber einem internationalen Unternehmen anwendbar ist. Dies musste auch der Verbraucherzentrale Bundesverband in seinem laufenden Verfahren gegen Facebook[1] feststellen, wo lange unklar war, ob deutsches, europäisches oder irisches Datenschutzrecht einschlägig ist.

Eine solche Regelung **kann allerdings nur wirksam sein, wenn es internationale Abkommen zur Rechtsdurchsetzung gibt**. Ansonsten werden die angestrebten Regelungen in der Praxis oftmals keine Wirkung entfalten können. Daher muss die Europäische Union solche Abkommen zu ihrer **Priorität** machen.

2. Verarbeitung personenbezogener Daten eines Kindes (Artikel 4, Artikel 8)

Bei der Wahrnehmung der Datenschutzrechte handelt es sich um eine Grundrechtsausübung, für die es keine starre Altersregel gibt. Es ist daher zu begrüßen, dass Kinder, die jünger sind als 13 Jahre nicht selbst in die Datenverarbeitung durch „Dienste der Informationsgesellschaft“ einwilligen können sollen. **Allerdings ist nicht verständlich, warum es außerhalb dieser „Dienste der Informationsgesellschaft“ keine Regelung zur Einwilligung durch Minderjährige geben soll.**

Ferner fehlt es noch an klaren Regeln, ob und unter welchen Voraussetzungen und besonders in welchem Umfang Jugendliche zwischen 14 und 18 Jahren eigenständig einwilligen und ihre Betroffenenrechte wahrnehmen können.

Grundsätzlich sollte die Erhebung von Daten von Minderjährigen besonderen Restriktionen unterliegen, die auch nicht durch Einwilligungen aufgehoben werden können. Beispielsweise sollten Kinder vom Profiling / Scoring ausgeschlossen sein.

Diese Regelung dürfen jedoch in der Praxis nicht dazu führen, dass Altersverifikationen an Stellen eingerichtet werden müssen, wo sie bisher entbehrlich waren, beispielsweise wenn sich vereinzelt Kinder unter den Nutzern sein könnten, auch wenn sich das Angebot nicht an sie richtet. Dadurch könnten allein aus diesem Grund viele neue personenbezogene Daten erfasst und gespeichert werden, die sonst nicht notwendig wären. Für diese Grenzfälle müssen Regeln definiert werden.

[1] vzbv reicht Klage gegen Facebook ein http://www.vzbv.de/1484.htm

3. Einwilligung (Artikel 7)

Der Verbraucherzentrale Bundesverband begrüßt ausdrücklich, dass Einwilligungen zukünftig immer einer expliziten Willenserklärung bedürfen.

Ebenso ist es unerlässlich, dass diese ohne Zwang erfolgen müssen. Um dies zu präzisieren, **fehlen jedoch in dem Entwurf Regelungen zum Kopplungsverbot**. Kopplungsverbot bedeutet, dass die Nutzung eines Dienstes nicht von der Einwilligung der Verbraucher zur Nutzung ihrer Daten - über das zur Diensterbringung notwendige Maß - abhängig gemacht werden darf. **Jede Art der Koppelung läuft dem Grundsatz einer freiwilligen Einwilligung zuwider und muss verboten werden**.

Darüber hinaus sollte eine **zeitliche Begrenzung von Einwilligungen** eingeführt werden. Häufig kann der Verbraucher – auch trotz neuer Hinweis- und Dokumentationspflichten – nicht mehr nachvollziehen, wohin seine einst erteilte Einwilligung gewandert ist. Außerdem kann der Überblick über die oftmals sehr große Anzahl an Werbeeinwilligungen verloren gehen. **Daher sollte nach beispielsweise zwei Jahren eine Einwilligung ihre Wirksamkeit verlieren, mit der Folge, dass die Daten entweder gelöscht werden müssen oder eine neue Einwilligung beim Verbraucher eingeholt werden muss.**

4. Information der Nutzer / Transparenz (Artikel 11, Artikel 14)

Der Verbraucherzentrale Bundesverband stimmt zu, dass Transparenz eine Grundvoraussetzung für die Souveränität des Einzelnen über seine Daten und einen wirksamen Datenschutz ist. Daher unterstützt der Verbraucherzentrale Bundesverband die Einführung eines allgemeinen Transparenzgrundsatzes für die Verarbeitung personenbezogener Daten.

Damit der Betroffene aber vor Erteilung einer Einwilligung ihre Folgen abschätzen kann, muss er auch über die Art und den Umfang der Datenverarbeitung informiert werden[2]. Diese Angaben fehlen jedoch bisher im Informationskatalog des Artikels 14 der Verordnung.

5. Recht auf Vergessenwerden und Löschung (Artikel 17)

Der Verbraucherzentrale Bundesverband unterstützt die neue Bestimmung, die im Entwurf als „Recht auf Vergessenwerden“ bezeichnet wird. Wenn ein Verbraucher aber gegenüber einem Unternehmen seinen Löschwunsch äußert, sollte dieser Wunsch durch das Unternehmen **allerdings nicht nur dann an Dritte weitergegeben werden müssen, wenn es die Daten öffentlich gemacht** oder Dritten die Veröffentlichung personenbezogener Daten gestattet hat, **sondern auch immer dann, wenn es Daten unabhängig einer Veröffentlichung an Dritte übermittelt hat**. Der Verbraucher selbst kann oftmals gar nicht überblicken, an welche konkreten Dritten die Daten durch das Unternehmen weiter gegeben wurden.

Fraglich ist bisher zudem, wie dieser Löschanspruch in der Praxis wirksam durchgesetzt werden soll. Aus diesem Grund müssen Lösungsmöglichkeiten gemeinsam mit der Internetwirtschaft erarbeitet werden. Anderenfalls bleibt diese Regelung „ein zahnloserTiger“, ähnlich wie es der e-Privacy-Richtlinie bisher ergangen ist.

[2] Analog zu den bisherigen Regelungen des deutschen Telemediengesetzes

6. Recht auf Datenübertragbarkeit (Artikel 18)

Die neue Regelung ist zu begrüßen, denn durch sie würde die Kontrolle der Verbraucher über ihre Daten gestärkt und marktbeherrschende Stellungen von Unternehmen verringert bzw. Wettbewerb ermöglicht werden.

Es müssen aber **gemeinsame Datenstandards und Schnittstellen** für die Datenportabilität **zwischen den Unternehmen** definiert werden, damit das Recht auch bei der Übertragung von großen Datenmengen nicht ins Leere läuft und der Verbraucher nicht erst seine Daten auf seinen Computer herunterladen und zwischenspeichern muss. Außerdem **dürfen die anfallenden Kosten grundsätzlich nicht durch den Verbraucher getragen werden müssen**.

7. Direktwerbung (Artikel 19 (2))

Der Verbraucherzentrale Bundesverband bedauert zu tiefst, dass die das Direktmarketing betreffenden Regelungen im Vergleich zu früheren Entwürfen der Verordnung bereits verwässert wurden. **Eine Einwilligung für die Nutzung und Weitergabe der Daten zu diesen Zwecken ist leider nicht mehr vorgesehen**, sondern nur noch ein Widerspruchsverfahren.

Der aktuelle Vorschlag bleibt sogar weit hinter den in Deutschland geltenden Regelungen zurück: Bisher darf ein Anbieter zwar ohne Einwilligung des Nutzers die von ihm erhobenen Daten auch für eigene Werbung nutzen, solange der Betroffene dem nicht widerspricht. Doch eine Datenübermittlung an Dritte für Werbezwecke ohne Einwilligung des Nutzers ist „nur“ in den Fällen von listenmäßig zusammengefassten Daten zulässig. Bereits diese Regelung ist schon höchst unfreundlich für die Verbraucher!

Wenn die neue Regelung so in Kraft treten sollte, können die Verbraucher noch weniger als bisher Kontroll- und Steuerungsfunktion über die Verwendung ihrer Daten ausüben. Dies widerspräche dem der Verbraucherpolitik zu Grunde liegenden Leitbild des mündigen Verbrauchers, der selbst entscheiden kann, wem er welche seiner Daten zur Verfügung stellt. **Für die Nutzung von personenbezogenen Daten zu Werbezwecken sollte immer eine Einwilligung des Betroffenen eingeholt werden müssen.**

8. Auf Profiling basierende Maßnahmen (Artikel 20 (3))

Nach dem Verordnungsentwurf dürfte sich die Verarbeitung von personenbezogenen Daten zum Zwecke des Profilings / Scorings „nicht ausschließlich“ auf sensitive Daten[3] stützen**. Die geplante Regelung würde damit die bisher in Deutschland geltende Rechtslage für die Verbraucher verschlechtern.**

Derzeit dürfen in Deutschland nur Daten erhoben und gespeichert werden, soweit dies zur Erfüllung eines Vertragsverhältnisses erforderlich ist oder der Betroffene eingewilligt hat. Die Tatsache, dass ein Scoring- oder Profilingverfahren, beispielsweise durch Banken oder Werbetreibende durchgeführt wird, ändert daran nichts und erweitert nicht den Berechtigungsrahmen. Daher dürfen sensitive Daten, die normalerweise beim Scoring oder Profiling nicht zur Vertragserfüllung benötigt werden, bisher ohne eine explizite Einwilligung auch nicht zu diesen Zwecken genutzt werden.

[3] gemäß Artikel 9 der Verordnung

Schon beim „herkömmlichen“ Profiling / Scoring handelt es sich um einen kritischen, weitreichenden Eingriff in die Rechte der Verbraucher - und dies oft auf eine sehr intransparente und schwer nachvollziehbare Art und Weise. **Eine Profilbildung sollte im Gegensatz zur gegenwärtigen Praxis immer nur mit Einwilligung des Betroffenen möglich sein. Sensitive Daten sollten gar nicht zum Zwecke des Profilings / Scorings verwendet werden dürfen. Außerdem sollten Minderjährige grundsätzlich vom Profiling / Scoring ausgeschlossen werden.**

9. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Artikel 23)

Nach dem Vorschlag der Kommission soll das Prinzip „data protection by default“ in das Datenschutzrecht eingeführt werden. Allerdings **sollten die Schutzziele dieses Artikels konkreter dargestellt werden**. Die Anforderung Maßnahmen und Verfahren durchzuführen, „durch die sicher gestellt wird, dass die Verarbeitungen den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden“ reicht nicht aus, um sowohl den Verbraucher, als auch den Unternehmen Klarheit und Rechtssicherheit zu geben.

So sollte klar gestellt werden, dass alle Produkte und Dienste so voreingestellt sein müssen, dass so wenig personenbezogene Daten wie möglich erhoben oder verarbeitet werden. Im Januar 2012 appellierte der Verbraucherzentrale Bundesverband im Rahmen einer Petition an den Deutschen Bundestag „data protection by default“ gesetzlich einzuführen. Zuvor hatte der Verbraucherzentrale Bundesverband im Rahmen der Kampagne „Mehr Datenschutz – Weniger Stress“[4] öffentlich um die Unterstützung der Petition gebeten. Dieser Bitte folgten nahezu zwölftausend Verbraucher[5]. Außerdem sollte zusätzlich die explizite **Verpflichtung eingeführt werden, anonyme und pseudonyme Nutzungsmöglichkeiten** - insbesondere von Internetdiensten - **anzubieten[6]**.

10. Benennung eines Datenschutzbeauftragten (Artikel 35 (1))

Der Verbraucherzentrale Bundesverband betrachtet, wie auch die Kommission, betriebliche Datenschutzbeauftragte als wichtigen Baustein, die unternehmerische Eigenkontrolle zu stärken. Diese tragen somit zu einem verbesserten Datenschutzniveau bei und entlasten die Aufsichtsbehörden. Es ist positiv, dass die guten Erfahrungen aus Deutschland nun EU-weit ausgedehnt werden sollen.

Diesen Ansätzen widerspricht aber, dass **betriebliche Datenschutzbeauftragte künftig erst ab einer Schwelle von 250 Beschäftigten bestellt werden sollen. Dieser Wert ist deutlich zu niedrig.** Bisher mussten beispielsweise in Deutschland lediglich 10 Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sein, was sich in der Praxis bewährt hat.

Die neue Regelung könnte hingegen die Folge haben, dass ein Großteil der Unternehmen in Deutschland seine Aktivitäten im Bereich Datenschutz einstellen werden. Dadurch würde das Risiko von Datenschutzverletzungen für die Verbraucher

[4] http://www.vzbv.de/mediapics/datenschutz_voreinstellungen_hintergrundpapier_2011.pdf

[5] https://www.openpetition.de/petition/online/datenschutzfreundliche-voreinstellungen

[6] analog zum deutschen Telemediengesetz

deutlich zunehmen. Diese hätten – auch unabhängig von konkreten Verletzungen - in den Unternehmen keine direkten Ansprechpartner mehr für ihre Anliegen und müssten sich in vielen Fällen direkt an die Aufsichtsbehörden wenden. Diese müssten dann versuchen die Sachverhalte zeitnah aufzuklären, was zu einer deutlich höheren Belastung der staatlichen Datenschutzbeauftragten führen würde.

Unverständlich ist ferner die Formulierung, dass ein Datenschutzbeauftragter bestellt werden muss, wenn die Kerntätigkeiten eines Unternehmens in Datenverarbeitungen bestehen, die „auf Grund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen“[7]. Logisch wäre im Gegensatz dazu, **dass ein Datenschutzbeauftragter bestellt werden müsste, wenn die Art der Datenverarbeitung auf Grund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung dieser Datenverarbeitung** (und nicht etwa der Betroffenen) **erforderlich macht**.

11. Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen (Artikel 40 ff)

Ähnliche Regelungen zum Angemessenheitsbeschluss gibt es bereits jetzt, allerdings sind diese in der Praxis höchst problematisch, wie beispielsweise das „Safe Harbor Abkommen“ zwischen der EU und den USA zeigt. Dieses Abkommen würde voraussichtlich auch zukünftig als „internationale Verpflichtungen“ der USA bzw. der Unternehmen von der EU-Kommission anerkannt werden. Datenübermittlungen würden daraufhin keiner weiteren Genehmigung bedürfen. **Es ist zu bezweifeln, dass diese Regelungen einen ausreichenden Schutz der Verbraucher sicher stellen können**.

Wenn US-Unternehmen dem Safe Harbor beitreten, müssen sie sich auf dessen Grundsätze verpflichten und auf eine Liste des Handelsministeriums der USA eintragen lassen. Eine Studie des US-Beratungsunternehmens Galexia aus dem Jahr 2008 zeigte jedoch gewaltige Defizite bei der Umsetzung auf[8]. Von nahezu 1600 Unternehmen auf der Liste hatten lediglich 348 Unternehmen größte Teile der Mindestvoraussetzungen des Abkommens erfüllt. Über 200 Unternehmen behaupteten darüber hinaus fälschlicherweise, Mitglieder des Abkommens zu sein. Dennoch wurden bisher keinerlei Sanktionen gegenüber Unternehmen ausgesprochen.

Hat die Kommission keinen Angemessenheitsbeschluss getroffen, soll nach dem Entwurf die grenzüberschreitende Verarbeitung personenbezogener Daten durch verbindliche Unternehmensregeln oder durch (Standard-) Vertragsklauseln ermöglicht werden, die durch die Aufsichtsbehörden zu genehmigen sind. Die Datenschutzbeauftragten werden hierbei nicht nur im Genehmigungsverfahren, sondern auch bei der Überprüfung der Maßnahmen eine wichtige Rollen spielen und müssen dementsprechend über die angemessenen Ressourcen verfügen.

[7] Im Original: “The controller and the processor shall designate a data protection officer in any case where the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.”

[8] http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

12. Unabhängigkeit (Artikel 47) sowie Ausstattung der Datenschutzaufsichtsbehörden (Artikel 49) und Kohärenzverfahren (Artikel 57)

Durch die neue Verordnung sollen die Datenschutzaufsichtsbehörden zahlreiche erweiterte Aufgaben und Funktionen erhalten, beispielsweise bei der Überprüfung der verbindlichen Unternehmensregeln oder im Rahmen der „One-Stop-Shop“ Regelung (siehe auch Punkt 14). Außerdem müsste die Reduzierung der betrieblichen Datenschutzbeauftragten kompensiert werden, damit überhaupt eine nennenswerte Kontrolle der Unternehmen stattfinden würde. Ist eine solche Kontrolle nicht vorhanden, laufen die Bestimmungen dieser Verordnung ins Leere.

Doch schon bereits heute sind die Aufsichtsbehörden nach eigenen Angaben nicht ausreichend ausgestattet, um ihre Funktionen angemessen wahrnehmen zu können[9]. **Damit diese also ihre neu hinzukommenden Aufgaben erfüllen können, müssen ihre personellen und finanziellen Ressourcen deutlich aufgestockt werden.** Dies gilt auch insbesondere für kleine Mitgliedsstaaten der Europäischen Union, in denen sich viele große oder besonders aufsichtsbedürftige Unternehmen niederlassen.

Darüber hinaus muss die Unabhängigkeit der Beauftragten für den Datenschutz gewährleistet sein – und dies nicht nur gegenüber der Wirtschaft und der nationalen Politik, sondern auch gegenüber der EU-Kommission, den anderen nationalen (Landes-) Datenschutzbeauftragten und denen der anderen EU-Mitgliedsstaaten. Dem Verbraucherzentrale Bundesverband ist bisher nicht klar, wie diese Unabhängigkeit vor allem im Rahmen des Kohärenzverfahrens beibehalten werden könnte, das für einheitliche Positionen der Datenschutzbeauftragten der EU-Staaten sorgen soll. Gleiches gilt für die Abstimmungen zwischen den Aufsichtsbehörden, die durch die One-Stop-Shop Regelung notwendig werden.

13. „One-Stop-Shop“-Regelung (Artikel 51 (2))

Zwar stimmt der Verbraucherzentrale Bundesverband der EU-Kommission zu, dass eine europaweite Harmonisierung des Datenschutzrechts auch aus Verbrauchersicht große Vorteile haben kann. Doch auch wenn das Datenschutzrecht harmonisiert ist, steht es doch nicht alleine, sondern ist in einen größeren Rechtsrahmen eingebunden, der von Staat zu Staat verschieden ist und beispielsweise das Verhältnis zur Meinungsfreiheit definiert. Ebenso ist die Kapazität und die Ausstattung der Datenschutzbeauftragten in den EU-Mitgliedsstaaten unterschiedlich.

Der Verbraucherzentrale Bundesverband befürchtet daher, dass diese Regelung zum so genannten "Forum-Shopping" führen könnte. Dies bedeutet, dass Unternehmen sich gezielt in Ländern niederlassen könnten, in denen der Rechtsrahmen für sie günstig ist. Außerdem könnten besonders in kleinen Mitgliedsstaaten die ebenso kleinen Aufsichtsbehörden überlastet sein, wenn sich dort eine hohe Anzahl an großen Konzernen niederlassen würde.

Der Bürokratieabbau bei den Unternehmen darf darüber hinaus nicht zu einer Verschlechterung des Rechtsschutzes der Verbraucher führen: Wendet sich beispielsweise ein Verbraucher zukünftig an seinen Landesdatenschutzbeauftragten, weil seine Daten auf nationaler Ebene von einem international agierenden

[9] Nach Berechnungen der Xamit Bewertungsgesellschaft stehen derzeit bundesweit für die Datenschutzaufsicht nur ca. 3,6 Stellen auf 100.000 Unternehmen zur Verfügung http://www.xamit-leistungen.de/downloads/Files.php?f=XamitDatenschutzbarometer2011.pdf

Unternehmen mit Sitz im Ausland unrechtmäßig verarbeitet wurden, wird dieser Landesdatenschutzbeauftragte seine Anfrage an die dortige Aufsichtsbehörde weitergeben müssen. Diese Aufsichtsbehörde würde sich wiederum an den Landesdatenschutzbeauftragten wenden, damit dieser vor Ort den Sachverhalt klären dürfte. Der Landesdatenschutzbeauftragte wäre allerdings nicht befugt Sanktionen auszusprechen, wenn er Mängel aufdecken sollte. Dies obläge wieder der Aufsichtsbehörde am Sitz des Unternehmens, die ihn wiederum mit der Vollstreckung beauftragen müsste.

Von der Dauer und Komplexität des Vorgangs abgesehen könnte eine Vielzahl von den praktischen Problemen auftreten, wie beispielsweise die notwendige Erstellung von Übersetzungen, bei denen nicht klar ist, wer diese verfassen soll. Auf diese Weise könnten die Verfahren oft deutlich erschwert und verlängert werden – zu Lasten der Verbraucher.

14. Verbandsklagerecht (Artikel 73 ff)

Es ist zu begrüßen, dass Datenschutzorganisationen zukünftig mit dem Recht ausgestattet sein sollen, gegen Datenschutzverstöße zu klagen. Dies entlastet die Aufsichtsbehörden und stärkt die Rechtsdurchsetzung der Verbraucher. **Es müssen aber auch dringend Verbraucherschutzorganisationen,** neben den Datenschutzorganisationen, **in diesem Artikel als klagebefugt aufgeführt werden.**

Da Verbraucherschutzorganisationen nicht explizit in der neuen Regelung genannt werden, werden auch weiterhin beispielsweise dem Verbraucherzentrale Bundesverband im Bereich des Datenschutzes die Hände gebunden sein. Der Datenschutz ist in Deutschland nicht explizit als verbraucherschützende Norm festgelegt, weshalb diesbezügliche Klagen durch Verbraucherorganisationen von den Gerichten nicht anerkannt werden. Die langjähigen Erfahrungen der Rechtsdurchsetzung die in anderen Bereichen gesammelt wurden, können daher beim Datenschutz nicht eingesetzt werden. Gesetzeswidriges Verhalten wird demnach häufig ohne Konsequenzen und Sanktionen bleiben.

15. Haftung und Recht auf Schadenersatz (Artikel 77)

Derzeit erstreckt sich ein möglicher Schadensersatz auf alle erlittenen materiellen Schäden. Immaterielle Schäden sind von der Ersatzpflicht ausgeschlossen. Der entstandene Schaden muss darüber hinaus durch den Betroffenen nachgewiesen und beziffert werden.

Gerade im Bereich des Datenschutzes ist dies allerdings häufig sehr schwierig, da der Schaden teilweise erst Jahre später auftritt[10]. Immaterielle Schäden, wie Rufschädigungen, sind meist gar nicht zu beziffern. Der Betroffene hat somit nicht nur den Schaden zu tragen, sondern muss auch den Ärger und Aufwand auf sich nehmen, um den Schaden zu minimieren. Somit werden in der Praxis auch bei massiven und massenhaften Verstößen oder fahrlässigen Praktiken durch Unternehmen die Verbraucher nahezu nie entschädigt.

[10] Beispielsweise wurden dem Unterhaltungskonzern Sony im Frühjahr 2011 ca. 100 Millionen Kundendatensätze, teilweise mit Kreditkartendaten gestohlen http://heise.de/-1236269 . Wenn die Kreditkartendaten erst Jahre später missbraucht werden, hat der Verbraucher keine Chance, den Schaden auf diesen Vorfall zurück zu führen.

Daher sollte ein pauschalisierter Schadensersatz - auch bei immateriellen Schäden – in Kombination mit einer Beweislastumkehr zu Gunsten der Verbraucher eingeführt werden. Nach einer rechtswidrigen Verwendung von personenbezogenen Daten müsste der Geschädigte nicht mehr grundsätzlich einen exakt bezifferten Schaden nachweisen, sondern nur noch, wenn dieser über die Pauschale hinaus gehen würde. Das Unternehmen müsste dann nachweisen, dass es den Schaden nicht verschuldet hat oder dieser Schaden überhaupt nicht erfolgt ist.

Dies wäre ein starkes Instrument für die Verbraucher sich gegen unrechtmäßige Datenverwendungen und mangelnde Datensicherheit zur Wehr zu setzen. Gleichzeitig könnten so die bisherigen Vollzugsdefizite teilweise ausgeglichen werden.

16. Verschärfte Sanktionen (Artikel 78, Artikel 79)

Der Verbraucherzentrale Bundesverband bedauert, dass der maximal mögliche Bußgeldrahmen im Vergleich zu vorherigen Versionen des Verordnungsentwurfs verringert wurde. Ursprünglich waren Maximalstrafen von bis zu fünf Prozent des weltweiten Jahresumsatzes geplant. Auch ist eine Regelung vergleichbar dem deutschen Bundesdatenschutzgesetz nicht vorhergesehen, nach dem die Bußgelder in Ausnahmenfällen auch überschritten werden können[11].

Datenschutzverstöße können auf der einen Seite massive Schäden und Beeinträchtigungen für eine große Anzahl von Verbrauchern zur Folge haben. Auf der anderen Seite können sich unseriöse Unternehmen durch ein systematisches Missachten von Datenschutzvorgaben einen signifikanten Wettbewerbsvorteil verschaffen[12]. **Aus diesen Gründen muss es auch bei den Sanktionen einen Spielraum nach oben geben, analog den Bestimmungen des deutschen Bundesdatenschutzgesetzes.**

[11] Bisher sind im deutschen Bundesdatenschutzgesetz Strafen bei Datenschutzverstößen von bis zu 300.000 Euro vorgesehen, allerdings mussten wegen Datenschutzverstößen Lidl im Jahr 2008 ein Bußgeld von 1.462 Millionen Euro https://www.datenschutzzentrum.de/presse/20080911-bw-lidl-bussgeldverfahren.pdf und die Deutsche Bahn AG im Jahr 2009 ein Bußgeld von 1.12 Millionen Euro http://heise.de/-837477 bezahlen

[12] Die Xamit Bewertungsgesellschaft geht davon aus, dass sich alleine in Deutschland der wirtschaftliche Vorteil für die Wirtschaft durch Datenschutzverletzungen über 7,5 Mrd. Euro beträgt http://www.xamit-leistungen.de/downloads/Files.php?f=XamitDatenschutzbarometer2011.pdf

IV. Weitere Anmerkungen

1. Kompetenzen der Kommission

Mit Sorge nimmt der Verbraucherzentrale Bundesverband zur Kenntnis, dass sich die EU-Kommission in äußerst vielen Fällen Befugnisse für delegierte Rechtsakte und Durchführungsrechtsakte einräumt. Bei 26 Artikeln soll die Kommission weitergehende Regelungen erlassen, sowie im Nachhinein Umsetzungsmodalitäten bestimmen können.

Somit sind die konkreten Inhalte und praktischen Bedeutungen dieser Artikel gänzlich unklar, womit die Reichweite der Verordnung kaum abzuschätzen ist. Dies führt zu einer bedeutenden Rechtsunsicherheit – sowohl was die grundsätzliche Beurteilung der Verordnung, als auch ihre spätere Anwendung angeht.

2. Richtlinie oder Verordnung

Vor allem in Deutschland wird derzeit eine hitzige Diskussion geführt, ob eine Verordnung tatsächlich der richtige Weg zur Verbesserung des Datenschutzes wäre. Unbestreitbar würde eine europäische Harmonisierung viele Vorteile für Unternehmen, aber auch für Verbraucher bieten.

Auf der anderen Seite befürchtet beispielsweise der Verfassungsrechtler und Mitglied des Bundesverfassungsgerichtes Johannes Masing[13], dass das deutsche Grundrecht auf informationelle Selbstbestimmung praktisch hinfällig werden könnte. Die Anwendung und Auslegung der Verordnung wäre auf Grund ihrer Vorrangigkeit gegenüber dem Grundgesetz nicht mehr am Maßstab deutscher Grundrechte überprüfbar, sondern müsste sich an der EU-Grundrechtecharta und der Europäischen Menschenrechtskonvention messen. Masing sieht darin jedoch nicht ansatzweise einen Ersatz. Einzelpersonen könnten sich nicht mit Verfassungsbeschwerden an den Europäischen Gerichtshof wenden und der Europäische Gerichtshof für Menschenrechte sei schon kapazitätsmäßig kein Äquivalent zum Bundesverfassungsgericht.

Der Deutsche Richterbund hingegen begrüßt die angestrebte Vollharmonisierung des Europäischen Datenschutzes im Rahmen einer Verordnung. Sichergestellt werden müsse aber dabei, dass der Europäische Gerichtshof der künftigen Aufgabe gerecht werden könne, die Rechtsprechung zum europäischen Datenschutz maßgeblich zu prägen. Dies könne durch die Einrichtung einer spezialisierten Datenschutzkammer erreicht werden[14].

[13] in der Süddeutschen Zeitung vom 09.01.2012

[14] http://www.drb.de/cms/index.php?id=756