

04. Januar 2013

Modernisierung des europäischen Datenschutzrechts

Änderungsvorschläge 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)

Einleitung

Der Datenschutz ist vor allem durch die digitale Entwicklung zu einem immer wesentlicheren Teil des Verbraucherschutzes geworden. Eine Modernisierung der gesetzlichen Regelungen ist daher 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.

Der Verbraucherzentrale Bundesverband (vzbv) unterstützt daher die EU-Kommission in ihren Bestrebungen, für einen verbesserten, harmonisierten und modernen Datenschutz in Europa zu sorgen¹. Dies umso mehr, als viele der im Kommissionsentwurf genannten Regelungsvorschläge langjährige Forderungen des Verbraucherzentrale Bundesverbandes aufgreifen. Doch trotz der grundsätzlichen Zustimmung zu den vorgeschlagenen Regelungen gibt es aus Verbrauchersicht noch weitreichenden Verbesserungsbedarf und Optimierungsmöglichkeiten. Die Rechte der einzelnen Verbraucher müssen dabei konsequent ins Zentrum der Ausgestaltung der Datenschutz-Grundverordnung gerückt werden. 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 auf einem guten Weg, den Datenschutz in Europa auf ein zeitgemäßes Niveau zu heben. Nun müssen sich auch das Europäische Parlament und der Rat der Europäischen Union diesem Weg folgen, den Schutz sowie die Rechte der Verbraucher stärken und Verwässerungen der Verordnung verhindern.

Die Kernpositionen des Verbraucherzentrale Bundesverbands

Allgemein: Der Verbraucherzentrale Bundesverband begrüßt mit Nachdruck die Pläne der EU-Kommission, das bestehende Datenschutzrecht gemäß der derzeit angewandten und etablierten Grundprinzipien fortzuentwickeln, insbesondere hinsichtlich der weiten Definition personenbezogener Daten und des Verbotsprinzips mit Einwilligungsvorbehalt. Den in die Diskussion eingebrachten Überlegungen, diese Prinzipien aufzuweichen, erteilt der Verbraucherzentrale Bundesverband eine deutliche Absage.

¹ Siehe auch 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) vom 29. Februar 2012
http://www.vzbv.de/cps/rde/xbcr/vzbv/EU-Datenschutz-Grundverordnung_Stellungnahme-vzbv_2012-02-29.pdf

Räumlicher Anwendungsbereich der Verordnung: Der Vorschlag der Kommission zum räumlichen Anwendungsbereich der Verordnung ist begrüßenswert, auch wenn einzelne Begrifflichkeiten noch klarer definiert werden müssen. So muss zum Beispiel in der Verordnung deutlich werden, dass „Waren und Dienstleistungen“ auch Dienste mit einschließen, bei denen der Nutzer keine finanziellen Kosten trägt. Außerdem können die Regelungen nur dann wirksam sein, wenn es internationale Abkommen zur Rechtsdurchsetzung gibt. Daher muss die Europäische Union solche Abkommen zu ihrer Priorität machen.

Personenbezogene Daten: Um die Rechte der Verbraucher angemessen zu schützen, sollte explizit klar gestellt werden, dass Kennnummern, Standortdaten, Online-Kennungen oder sonstige vergleichbare Elemente immer personenbezogene Daten sind, wenn mit ihrer Hilfe eine Person bestimmbar ist.

„Berechtigtes Interesse“ als rechtliche Grundlage der Verarbeitung: Es fehlt eine klare Definition des „berechtigten Interesses“ als rechtliche Basis für eine Datenverarbeitung. Es sollten Fälle genannt werden, die eindeutig unter ein berechtigtes Interesse fallen bzw. eindeutig nicht darunter fallen. Insbesondere sollte klar gestellt werden, dass das Geschäftsmodell von Unternehmen nicht per se als berechtigtes Interesse gilt (insb. im Falle von Direktwerbung).

Zweckbindung: Das Prinzip der Zweckbindung sollte beibehalten und gestärkt werden. Eine Weiterverarbeitung der Daten zu einem Zweck, der mit dem Zweck zu dem sie erhoben wurden nicht vereinbar ist, muss ausgeschlossen werden.

Einwilligung: 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 Dienstleistung notwendige Maß hinaus - abhängig gemacht werden.

Transparenz: Die Einführung eines allgemeinen Transparenzgrundsatzes für die Verarbeitung personenbezogener Daten verbunden mit Pflichten zur verbesserten Darstellung von datenschutzrelevanten Informationen wird unterstützt. Allerdings muss dieser Grundsatz weiter gestärkt werden, denn in vielen Punkten ist die Art der vorgesehenen Informationen nicht angemessen. Damit der Betroffene aber vor Erteilung einer Einwilligung die Folgen abschätzen kann, muss er beispielsweise auch über die Art und den Umfang der Datenverarbeitung informiert werden.

Profilbildung: Der Verbraucherzentrale Bundesverband sieht mit Sorge die zunehmende Profilbildung der Verbraucher. Daher begrüßt der vzbv zwar entsprechende Regelungen, diese müssen allerdings dringend weiter geschärft werden. Die bisherigen Formulierungen und Regelungen reichen bei Weitem nicht aus, um dem Gefahrenpotential der Profilbildung angemessen gerecht zu werden. Wichtig ist, dass Unterschiede bei der Profilbildung in den verschiedenen Wirtschaftssektoren oder rechtlichen Beziehungen berücksichtigt werden. Beispielsweise müssen sowohl die

Profilbildung im Internet, aber auch in Offline-Umgebungen, wie beim Kreditscoring, ausreichend eingeschlossen werden.

Datenschutz durch Technik /datenschutzfreundliche Voreinstellung: 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 Internet- und Zahlungsdiensten - anzubieten.

Recht auf Beschwerde und gerichtlichen Rechtsbehelf: Der Entwurf in der vorliegenden Formulierung ändert nichts daran, dass Verbraucherschutzorganisationen auch weiterhin nur höchst eingeschränkt für Verbraucher bei Fragen des Datenschutzes die Instrumente des kollektiven Rechtsschutzes nutzen können. Auch qualifizierte Verbraucherschutzorganisationen sollten daher als klagebefugt aufgeführt werden.

Die Änderungsvorschläge des Verbraucherzentrale Bundesverbands

Vorschlag der Kommission	vzbv Änderungsvorschlag
<p><i>Artikel 3 – Räumlicher Anwendungsbereich</i></p> <p>[...]</p> <p>2. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung</p> <p>a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, oder</p> <p>b) der Beobachtung ihres Verhaltens dient.</p> <p>[...]</p>	<p><i>Artikel 3 – Räumlicher Anwendungsbereich</i></p> <p>[...]</p> <p>2. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung</p> <p>a) dazu dient, diesen Personen entgeltlich oder unentgeltlich in der Union Waren oder Dienstleistungen anzubieten, oder</p> <p>b) der Beobachtung ihres Verhaltens dient.</p> <p>[...]</p>
<p><i>Begründung</i></p> <p><i>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 schuf dringend notwendige Klarheit, denn bisher ist oft nicht deutlich, welches Recht gegenüber einem internationalen Unternehmen anwendbar ist.</i></p> <p><i>Es muss aber in der Verordnung deutlich werden, dass „Waren und Dienstleistungen“ auch Dienste mit einschließen, bei denen der Nutzer keine finanziellen Kosten trägt.</i></p> <p><i>Der Begriff der „Beobachtung“ zielt nach Erwägungsgrund 21 auf eine Profilbildung im Internet ab. Es muss aber sicher gestellt sein, dass jede Beobachtung, Analyse oder Vorhersage des Verhaltens der Verbraucher und darauf folgende Entscheidungen eingeschlossen sein müssen, auch wenn keine Profile erstellt werden und auch wenn diese Beobachtung offline erfolgt.</i></p>	
<p><i>Artikel 4 – Begriffsbestimmung</i></p> <p>Im Sinne dieser Verordnung bezeichnet der Ausdruck</p> <p>(1) „betroffene Person“ eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche oder jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren be-</p>	<p><i>Artikel 4 – Begriffsbestimmung</i></p> <p>Im Sinne dieser Verordnung bezeichnet der Ausdruck</p> <p>(1) „betroffene Person“ eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche oder jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren be-</p>

<p>sonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;</p> <p>[...]</p> <p>(8) "Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;</p> <p>[...]</p>	<p>sonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;</p> <p>[...]</p> <p>(4a) „Sperren“ das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung einzuschränken</p> <p>(8) "Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in vorheriger Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen, durch die datenverarbeitende Stelle nachweisbaren Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;</p> <p>[...]</p> <p>(19a) „Anonymisieren“ das Verändern personenbezogener Daten nach dem aktuellen Stand der Technik derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.</p> <p>(19b) „Pseudonymisieren“ das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen wesentlich zu erschweren.</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Um die Rechte der Verbraucher angemessen zu schützen, sollte im Einklang mit Artikel 4 Nummer 1 im Erwägungsgrund 24 klar gestellt werden, dass Kennnummern, Standortdaten, Online-Kennungen oder sonstige vergleichbare Element immer personenbezogene Daten sind, wenn mit ihrer Hilfe eine Person bestimmbar sein kann. Erwägungsgrund 24 sollte ferner technikneutral gehalten und nicht auf Online-Dienste und -Kennungen begrenzt werden, um beispielsweise auch Offline-Techniken wie den Einsatz von RFID-Technologie im Endkundenbereich mit einzuschließen.</i></p> <p><i>Der Vorgang des Sperrens sollte in die Verordnung mit aufgenommen und dementsprechend definiert werden.</i></p> <p><i>Der Verbraucherzentrale Bundesverband begrüßt ausdrücklich, dass stillschweigende Einwilligungen ohne Zutun der betroffenen Person zukünftig ausgeschlossen werden und damit die Stärkung der Einwilligung als eine Bedingung für die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten. Um diese Stärkung zu verdeutlichen, sollten im Erwägungsgrund 25 Beispiele für Fälle aufgeführt werden, die nicht als „Zutun der betroffenen Person“ gelten, wie beispielsweise der reine Besuch einer Internetseite oder ein bereits „angeklicktes“ Kästchen. Die Lösung, eine Einwilligung zur Werbeprofilerstellung beispielsweise über die Einstellungen in Webbrowsern auszudrücken ist denkbar: Allerdings müssen dafür die Webbrowser bei Auslieferung so voreingestellt sein, dass sie standardmäßig keine Einwilligung ausdrücken.</i></p>	

Eine Einwilligung muss außerdem immer nach vorheriger Information, bewusst und auf den konkreten Fall bezogen vor der Datenverarbeitung abgegeben werden. Dass dabei die Beweislast beim für die Verarbeitung Verantwortlichen liegt, sollte aber auch in der Definition wiederspiegelt werden.

Es fehlt eine Definition der Begriffe „Anonymisieren“ und „Pseudonymisieren“, um klar zu stellen, dass eine Anonymisierung nur dann erfolgt ist, wenn sich vormals personenbezogene Daten in Zukunft nicht mehr einer Person zuzuordnen lassen. Daher muss die Anonymisierung ständig dem Stand der Technik angepasst werden, da sich auch die Möglichkeiten der De-Anonymisierung kontinuierlich weiter entwickeln. Daten, die nur mit einem großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können, sind als pseudonymisiert zu betrachten.

Sind Daten vollständig anonymisiert, sollten Sie nicht unter den Geltungsbereich der Verordnung fallen. Sind Daten pseudonymisiert kann ihre Schutzwürdigkeit - beispielsweise im Rahmen einer Interessenabwägung nach Artikel 6 Absatz 1 Buchstabe f oder bei der Datenschutz-Folgeabschätzung – anders beurteilt werden, als bei unpseudonymisierten Daten, da die Eingriffstiefe in die schutzwürdige Interessen der betroffenen Person geringer ist.

Artikel 6 – Rechtmäßigkeit der Verarbeitung	Artikel 6 – Rechtmäßigkeit der Verarbeitung
<p>1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:</p> <p>[...]</p> <p>f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dieser gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.</p> <p>[...]</p> <p>4. Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e genannten Gründe zutreffen. Dies gilt insbesondere bei Änderungen von Geschäfts- und allgemeinen Vertragsbedingungen.</p> <p>5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Anwendung von Absatz 1 Buchstabe f für verschiedene Bereiche und Verarbeitungssituationen einschließlich Situationen, die die Verarbeitung personenbezogener Daten von Kindern betreffen, näher zu regeln.</p>	<p>1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:</p> <p>[...]</p> <p>f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dieser Rechtsgrund gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Er gilt auch nicht, wenn die Verarbeitung auf Basis einer der in Absatz 1 Buchstaben a bis e genannten Bedingungen erfolgen kann.</p> <p>[...]</p> <p>4. Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e genannten Gründe zutreffen. Dies gilt insbesondere bei Änderungen von Geschäfts- und allgemeinen Vertragsbedingungen.</p> <p>5. Der europäische Datenschutzausschuss erlässt Richtlinien, unter deren Maßgabe Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Anwendung von Absatz 1 Buchstabe f für verschiedene Bereiche und Verarbeitungssituationen einschließlich Situationen, die die Verarbeitung</p>

	personenbezogener Daten von Kindern betreffen, näher zu regeln als Rechtsgrundlage einer Verarbeitung von personenbezogenen Daten ermöglicht wird und erstellt Kriterien, anhand derer beurteilt werden kann, ob die berechtigten Interessen des für die Verarbeitung Verantwortlichen gegenüber den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person überwiegen.
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Die Bestimmung des „berechtigten Interesses“ als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten ist derzeit zu vage gehaltenen. Es gibt keine Hinweise darauf, welche Arten von Datenverarbeitungen zulässig sind, die sich aber nicht durch einen der anderen Rechtsgründe begründen lassen. Artikel 6 Absatz 1 Buchstabe f darf kein Auffangtatbestand für Verarbeitungen sein, die der für die Verarbeitung Verantwortliche nicht auf eine der in Artikel 6 Absatz 1 Buchstaben a bis e genannten Rechtsgrundlagen stellen möchte. Dementsprechend sollte eine Datenverarbeitung auf Grundlage einer Interessenabwägung nur erlaubt sein, wenn diese Verarbeitung aus objektiven Gründen nicht auf einer der in Artikel 6 Absatz 1 Buchstaben a bis e begründet werden kann.</i></p> <p><i>Um diese Gründe dazulegen fehlt es an einer klaren Definition des „berechtigten Interesses“ bzw. an entsprechenden objektiven Kriterien, die durch den europäischen Datenschutzausschuss aufgestellt werden sollten. Eine fehlende klare Definition könnte zu einer Rechtsunsicherheit bei den Unternehmen und zu unterschiedlichen Auslegungen in den Mitgliedsstaaten führen. Es sollten daher zum Beispiel in den Erwägungsgründen Fälle genannt werden, die eindeutig unter ein berechtigtes Interesse fallen bzw. eindeutig nicht darunter fallen. Beispielsweise sollte klar gestellt werden, dass allein ein von der Rechtsordnung gebilligtes Interesse oder lediglich ein Hinweis auf die Geschäftszwecke eines Unternehmens nicht ausreichen, um ein berechtigtes Interesse zu begründen. Insbesondere sollte Direktwerbung nicht auf Grundlage des Artikel 6 Absatz 1 Buchstabe f, sondern nur mit Einwilligung des Betroffenen möglich sein.</i></p> <p><i>Auf keinen Fall darf die Entscheidung, ob das Interesse der datenverarbeitenden Stelle gegenüber den Interessen der betroffenen Person überwiegt, auf der einen Seite von der verantwortlichen Stelle ohne eine nachweisbar gewissenhafte Abwägung frei getroffen werden und auf der anderen Seite lediglich in den Fällen hinterfragt werden, in denen die betroffene Person rechtlich gegen die Datenverarbeitung vor geht. Damit sicher gestellt wird, dass die Interessenabwägung gewissenhaft durchgeführt wird, sollte sie im Rahmen einer im Rahmen einer Datenschutz-Folgeabschätzung erfolgen müssen [s.a. Artikel 33]. Im Rahmen seiner Informationspflichten [s.a. Artikel 14], sollte der für die Verarbeitung Verantwortliche gegenüber der betroffenen Person das Ergebnis begründen müssen. Außerdem sollte die betroffene Person Datenverarbeitungen nach Artikel 6 Absatz 1 Buchstabe f widersprechen können und vor Beginn der erstmaligen Verarbeitung ausdrücklich in einer verständlichen und von anderen Informationen klar abgegrenzten Form auf dieses Recht hingewiesen werden [s.a. Artikel 19].</i></p> <p><i>Das Prinzip der Zweckbindung sollte beibehalten und gestärkt werden. Artikel 6 Absatz 4 untergräbt jedoch dieses das Prinzip und steht in eklatantem Widerspruch zu Artikel 5 Buchstabe b. Eine Weiterverarbeitung der Daten zu einem Zweck, der mit dem Zweck zu dem sie erhoben wurden nicht vereinbar ist, muss ausgeschlossen werden. Daher sollte Artikel 6 Absatz 4 gestrichen werden.</i></p>	
<p style="text-align: center;"><i>Artikel 7 – Einwilligung</i></p> <p>[...]</p> <p>2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, die noch einen anderen Sachverhalt betrifft, muss das Erfordernis der</p>	<p style="text-align: center;"><i>Artikel 7 – Einwilligung</i></p> <p>[...]</p> <p>2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, die noch einen anderen Sachverhalt betrifft, muss das Erfordernis der</p>

<p>Einwilligung äußerlich erkennbar von dem anderen Sachverhalt getrennt werden.</p> <p>[...]</p>	<p>Einwilligung äußerlich erkennbar von dem anderen Sachverhalt getrennt werden.</p> <p>[...]</p> <p>4a. Eine verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung der betroffenen Person abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.</p> <p>4b. Nach einer vorherig festgelegten Frist oder nach maximal zwei Jahren, wenn keine Frist definiert wurde, verliert eine Einwilligung ihre Wirksamkeit. In Folge müssen die Daten entweder gelöscht oder eine neue Einwilligung beim Verbraucher eingeholt werden.</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Eine Hervorhebung der Einwilligung sollte nicht nur bei „schriftlichen“ Erklärungen (i.S.v. § 126 BGB) notwendig sein, wenn die Erklärung noch weitere Sachverhalte betrifft, sondern beispielsweise auch bei Einwilligungen, die auf elektronischem Weg abgegeben werden.</i></p> <p><i>Es ist unerlässlich, dass Einwilligungen 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 Dienstleistung notwendige Maß - abhängig gemacht werden darf, wenn dem Nutzer ein anderer Zugang zu gleichwertigen Leistungen ohne die Einwilligung nicht möglich ist. Diese Art der Koppelung läuft dem Grundsatz einer freiwilligen Einwilligung zuwider und muss verboten werden.</i></p> <p><i>Darüber hinaus sollte eine zeitliche Begrenzung von Einwilligungen eingeführt werden. In der Praxis werden Einwilligungen oftmals unwirksam erhoben, zu ausufernden Zwecken verwendet und an Dritte weiter gegeben und verkauft. Häufig kann der Verbraucher – auch trotz neuer Hinweis- und Dokumentationspflichten – nicht mehr nachvollziehen, wohin seine einst erteilte Einwilligung gewandert ist. 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.</i></p>	
<p>Artikel 8 – Verarbeitung personenbezogener Daten eines Kindes</p> <p>1. Für die Zwecke dieser Verordnung ist die Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten dreizehnten Lebensjahr, dem direkt Dienste der Informationsgesellschaft angeboten werden, nur rechtmäßig, wenn und insoweit die Einwilligung hierzu durch die Eltern oder den Vormund des Kindes oder mit deren Zustimmung erteilt wird. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen, um eine nachprüfbare Einwilligung zu erhalten.</p>	<p>Artikel 8 – Verarbeitung personenbezogener Daten eines Kindes</p> <p>1. Für die Zwecke dieser Verordnung ist dieDie Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten dreizehnten Lebensjahr, dem direkt Dienste der Informationsgesellschaft angeboten werden, ist nur rechtmäßig, wenn und insoweit die Einwilligung hierzu durch die Eltern oder den Vormund des Kindes oder mit deren Zustimmung erteilt wird. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen, um eine nachprüfbare Einwilligung zu erhalten.</p>

<p>[...]</p> <p>3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten und Anforderungen in Bezug auf die Art der Erlangung einer nachprüfaren Einwilligung gemäß Absatz 1 näher zu regeln. Dabei zieht die Kommission spezifische Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen in Betracht.</p> <p>[...]</p>	<p>[...]</p> <p>3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten und Anforderungen in Bezug auf die Art der Erlangung einer nachprüfaren Einwilligung gemäß Absatz 1 näher zu regeln. Dabei zieht die Kommission spezifische Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen in Betracht.</p> <p>[...]</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Es ist 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.</i></p> <p><i>Da Kinder besonders schutzbedürftig sind, sollte die Erhebung von Daten von Minderjährigen besonderen Restriktionen unterliegen, die auch nicht durch Einwilligungen aufgehoben werden können. Beispielsweise sollten Kinder immer vom Profiling ausgeschlossen sein.</i></p> <p><i>Die genannten Regelungen 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 eines Dienstes sein könnten, auch wenn sich das Angebot nicht an sie richtet. Denn sonst müssten allein aus diesem Grund viele neue personenbezogene Daten erfasst und gespeichert werden, die sonst nicht notwendig wären. Es sollte daher, beispielsweise in den Erwägungsgründen, betont werden, dass die Prinzipien des „Privacy by Design“, der Datensparsamkeit und der Zweckbindung streng zu beachten sind. Anonyme Altersverifikationen sind zu entwickeln und zu bevorzugen (ähnlich der Altersverifikationsfunktion des deutschen elektronischen Personalausweises).</i></p> <p><i>Da bereits klare Anforderungen an die verantwortliche Stelle bestehen, eine unter Berücksichtigung der vorhandenen Technologie nachprüfbare Einwilligung zu erhalten, besteht keine Notwendigkeit eines delegierten Rechtsaktes. Ausnahmen für KMUs wären gerade im Hinblick auf das Schutzziel des Artikels nicht nachvollziehbar.</i></p>	
<p><i>Artikel 13 – Rechte gegenüber Empfängern</i></p> <p>Der für die Verarbeitung Verantwortliche teilt allen Empfängern, an die Daten weitergegeben wurden, jede Berichtigung oder Löschung, die aufgrund von Artikel 16 beziehungsweise 17 vorgenommen wird, mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.</p>	<p><i>Artikel 13 – Rechte gegenüber Empfängern</i> Benachrichtigungspflicht bei Berichtigungen und Löschungen</p> <p>Der für die Verarbeitung Verantwortliche teilt allen Empfängern, an die Daten weitergegeben wurden, jede Berichtigung oder , Löschung oder Sperrung, die aufgrund von Artikel 16 beziehungsweise 17 vorgenommen wird, sowie Widersprüche der Betroffenen aufgrund von Artikel 19 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Eine Pflicht der verantwortlichen Stelle, bei Berichtigungen und Löschungen die Empfänger von</i></p>	

Daten zu benachrichtigen, ist zu begrüßen. Da der Artikel jedoch keine Rechte gegenüber den Empfängern enthält, sollte er in „Benachrichtigungspflicht bei Berichtigungen und Löschungen“ umbenannt werden.

Ferner sollte die Benachrichtigungspflicht auch die Mitteilung von Sperrungen, sowie von Widersprüchen nach Artikel 19 mit einschließen.

Darüber hinaus sollte – beispielsweise in den Erwägungsgründen - klar gestellt werden, was unter einem „unverhältnismäßigen Aufwand“ zu verstehen ist, der die verantwortliche Stelle von den Benachrichtigungspflichten entbindet. Dabei ist der „unverhältnismäßigen Aufwand“ möglichst eng zu definieren. Wenn schon die Weitergabe der Daten möglich war, sollte in den meisten Fällen auch eine Weitergabe des Löschwunsches auf dem gleichen Weg eingerichtet werden können.

Artikel 14 – Information der betroffenen Person	Artikel 14 - Information der betroffenen Person
<p>1. Einer Person, von der personenbezogene Daten erhoben werden, teilt der für die Verarbeitung Verantwortliche zumindest Folgendes mit:</p> <p>[...]</p> <p>b) die Zwecke, für die Daten verarbeitet werden, einschließlich der Geschäfts- und allgemeinen Vertragsbedingungen, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe b gründet, beziehungsweise die von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen, wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht,</p> <p>[...]</p>	<p>1. Einer Person, von der personenbezogene Daten erhoben werden, teilt der für die Verarbeitung Verantwortliche zumindest Folgendes mit:</p> <p>[...]</p> <p>a1) Art und Umfang der personenbezogenen Daten, die verarbeitet werden</p> <p>b) die spezifischen Zwecke, für die Daten verarbeitet werden, einschließlich der Geschäfts- und allgemeinen Vertragsbedingungen, sowie Informationen hinsichtlich der konkreten Verarbeitung falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe b gründet, beziehungsweise die von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen, sowie die Begründung, warum der für die Verarbeitung Verantwortliche zu dem Ergebnis kommt, dass seine berechtigten Interessen gegenüber den Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht,</p> <p>[...]</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>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. Um diesem Ziel jedoch gerecht zu werden, sind Konkretisierungen notwendig.</i></p> <p><i>Damit der Betroffene vor Erteilung einer Einwilligung ihre Folgen abschätzen kann, muss er über die Art und den Umfang der Datenverarbeitung informiert werden. Diese Angaben fehlen jedoch bisher im Informationskatalog des Artikels 14 der Verordnung.</i></p> <p><i>Auf die Angabe zu Geschäfts- und allgemeinen Vertragsbedingungen kann verzichtet werden,</i></p>	

wenn diese nicht datenschutzrelevant sind, da ihre Angabe bereits anderen rechtlichen Vorgaben unterliegt. Eine erneute Angabe würde Menge der Informationen aufblähen, ohne einen Mehrwert zu bilden.

Wenn eine datenverarbeitende Stelle die Datenverarbeitung auf der rechtlichen Basis des „berechtigten Interesses“ nach Artikel 6 Absatz 1 Buchstabe f vornimmt, muss sie nicht nur die Pflicht haben, diese berechtigten Interessen dar zu legen, sondern auch zu begründen, warum ihre berechtigten Interessen gegenüber den schutzwürdigen Interessen der betroffenen Person überwiegen.

Besonders im Internet muss die bisherige Praxis aufgebrochen werden, dass dem Betroffenen nur Informationen hinsichtlich der Datenverarbeitungen zur Verfügung gestellt werden, die in Zusammenhang mit dem Betrieb der entsprechenden Webseite stehen. Der Betroffene muss hingegen auch über alle weiteren Verarbeitungen der verantwortlichen Stelle informiert werden, bei denen Daten zu seiner Person verarbeitet werden.

Artikel 15 – Auskunftsrecht der betroffenen Person

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen jederzeit eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht. Werden personenbezogene Daten verarbeitet, teilt der für die Verarbeitung Verantwortliche Folgendes mit:

[...]

b) die Kategorien personenbezogener Daten, die verarbeitet werden,

c) die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben werden müssen oder weitergegeben worden sind, speziell bei Empfängern in Drittländern,

[...]

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchsrechts gegen die Verarbeitung dieser Daten,

[...]

g) diejenigen personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten,

h) die Tragweite der Verarbeitung und die mit ihr angestrebten Auswirkungen, zumindest im Fall der Maßnahmen gemäß Artikel 20.

Artikel 15 – Auskunftsrecht der betroffenen Person

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen jederzeit eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht. Werden personenbezogene Daten verarbeitet, teilt der für die Verarbeitung Verantwortliche Folgendes mit:

[...]

b) **die personenbezogenen Daten, die verarbeitet werden, sowie alle Informationen über die Herkunft der Daten**, ~~die Kategorien personenbezogener Daten, die verarbeitet werden,~~

c) ~~die Empfänger oder Kategorien von Empfängern~~, an die die personenbezogenen Daten weitergegeben werden ~~müssen~~ oder weitergegeben worden sind, speziell bei Empfängern in Drittländern,

[...]

e) das Bestehen eines Rechts auf Berichtigung ~~oder~~, Löschung **oder Sperrung** der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchsrechts gegen die Verarbeitung dieser Daten,

[...]

g) ~~diejenigen personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten,~~

h) die **Bedeutung und** Tragweite der Verarbeitung und die mit ihr angestrebten Auswirkungen, ~~zumindest~~ **insbesondere** im

<p>[...]</p> <p>3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten zu den Kriterien und Anforderungen in Bezug auf die Mitteilung über den Inhalt der personenbezogenen Daten gemäß Absatz 1 Buchstabe g an die betroffene Person festzulegen.</p>	<p>Fall der Maßnahmen gemäß des Artikel 20. Im Falle einer Verarbeitung für die unter Artikel 20 Absatz 1 genannten Zwecke ferner die konkreten, der Auswertung zu Grunde liegenden Daten und ihre Gewichtung in einer nachvollziehbaren Form.</p> <p>h1) die Ergebnisse der Datenschutzfolgeabschätzung gemäß Artikel 33 Absatz 3.</p> <p>[...]</p> <p>3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten zu den Kriterien und Anforderungen in Bezug auf die Mitteilung über den Inhalt der personenbezogenen Daten gemäß Absatz 1 Buchstabe g an die betroffene Person festzulegen.</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Analog zu Artikel 14 trägt Artikel 15 zur Transparenz der Verarbeitung bei und gibt der betroffenen Person die Möglichkeit, weiterführende Informationen zu dieser Verarbeitung zu erhalten. Transparenz ist aber nur möglich, wenn die Informationen konkret sind. Daher sollte im Gegensatz zu den allgemeinen Informationen in Artikel 14 nicht nur über die Kategorien der verarbeiteten Daten bzw. über die Kategorien der Empfänger von personenbezogenen Daten informiert werden, sondern es sollten immer die konkreten Daten und ihre Herkunft, sowie die konkreten Empfänger der Daten benannt werden müssen. Nur so ist es der betroffenen Person möglich, auch bei diesen Empfängern ihre Rechte wahr zu nehmen.</i></p> <p><i>Da Verarbeitungen nach Artikel 20 Absatz 1 eine besondere Eingriffstiefe in die Persönlichkeitsrechte der betroffenen Person innehaben, muss die datenverarbeitende Stelle die mit diesen Verarbeitungen angestrebten Auswirkungen gegenüber der betroffenen Person darlegen. Um Kontroll- und Korrekturmöglichkeiten der Verarbeitung auch durch die betroffene Person zu ermöglichen, muss die datenverarbeitende Stelle ferner die der Auswertung zugrunde liegenden Daten, sowie ihre Gewichtung bei der Berechnung konkret in einer nachvollziehbaren Form offenlegen.</i></p> <p><i>Die Datenschutz-Folgenabschätzung trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen Rechnung. In den Fällen in denen eine Datenschutz-Folgeabschätzung vorgenommen werden muss sollten daher die betroffenen Personen auch auf Anfrage eine allgemeine Beschreibung der Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren erhalten, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden.</i></p>	
<p style="text-align: center;"><i>Artikel 16 – Recht auf Berichtigung</i></p> <p>Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Berichtigung von unzutreffenden personenbezogenen Daten zu verlangen. Die betroffene Person hat das Recht, die Vervollständigung unvollständiger personenbezogener Daten, auch in Form eines Korrigendums, zu verlangen.</p>	<p style="text-align: center;"><i>Artikel 16 – Recht auf Berichtigung</i></p> <p>Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Berichtigung von unzutreffenden personenbezogenen Daten zu verlangen Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Die betroffene Person hat das Recht, die Vervollständigung unvollständiger personenbezogener Daten, auch in Form eines Korrigendums, zu verlangen.</p>

<i>Begründung</i>	
<i>Die Korrektur von unzutreffenden personenbezogenen Daten sollte nicht von einem Verlangen der betroffenen Person abhängen, sondern immer dann durchzuführen sein, wenn der für die Verarbeitung Verantwortliche davon Kenntnis erhält.</i>	
<p>Artikel 17 – Recht auf Vergessenwerden und auf Löschung</p> <p>1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten zu verlangen, speziell wenn es sich um personenbezogene Daten handelt, die die betroffene Person im Kindesalter öffentlich gemacht hat, sofern einer der folgenden Gründe zutrifft:</p> <p>[...]</p> <p>2. Hat der in Absatz 1 genannte für die Verarbeitung Verantwortliche die personenbezogenen Daten öffentlich gemacht, unternimmt er in Bezug auf die Daten, für deren Veröffentlichung er verantwortlich zeichnet, alle vertretbaren Schritte, auch technischer Art, um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt. Hat der für die Verarbeitung Verantwortliche einem Dritten die Veröffentlichung personenbezogener Daten gestattet, liegt die Verantwortung dafür bei dem für die Verarbeitung Verantwortlichen.</p> <p>[...]</p> <p>4. Anstatt die personenbezogenen Daten zu löschen, kann der für die Verarbeitung Verantwortliche deren Verarbeitung beschränken, wenn</p> <p>[...]</p> <p>9. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten festzulegen in Bezug auf</p> <p>[...]</p> <p>b) die Bedingungen für die Löschung gemäß Absatz 2 von Internet-Links, Kopien oder Replikationen von personenbezogenen Daten aus</p>	<p>Artikel 17 – Recht auf Vergessenwerden und auf Löschung</p> <p>1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die auf Löschung oder Sperrung von der sie betreffenden personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten durch den für die Verarbeitung Verantwortlichen zu verlangen, speziell wenn es sich um personenbezogene Daten handelt, die die betroffene Person im Kindesalter öffentlich gemacht hat, sofern einer der folgenden Gründe zutrifft:</p> <p>[...]</p> <p>2. Hat der in Absatz 1 genannte für die Verarbeitung Verantwortliche die personenbezogenen Daten öffentlich gemacht, unternimmt er in Bezug auf die Daten, für deren Veröffentlichung er verantwortlich zeichnet, alle vertretbaren Schritte, auch technischer Art, um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt. Hat der für die Verarbeitung Verantwortliche einem Dritten die Veröffentlichung personenbezogener Daten gestattet, liegt die Verantwortung dafür bei dem für die Verarbeitung Verantwortlichen.</p> <p>[...]</p> <p>4. Anstatt die personenbezogenen Daten zu löschen, kann der für die Verarbeitung Verantwortliche deren Verarbeitung beschränken diese Daten sperren, wenn</p> <p>[...]</p> <p>9. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten festzulegen in Bezug auf</p> <p>[...]</p> <p>b) die Bedingungen für die Löschung gemäß Absatz 2 von Internet-Links, Kopien oder Replikationen von personenbezogenen Daten aus</p>

öffentlich zugänglichen Kommunikationsdiensten, [...]	öffentlich zugänglichen Kommunikationsdiensten, [...]
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Der Verbraucherzentrale Bundesverband begrüßt grundsätzlich eine Stärkung des Rechts der betroffenen Person auf die Löschung ihrer Daten bei der verantwortlichen Stelle. Der Titel des Artikels führt jedoch in die Irre und sollte daher entsprechend geändert werden.</i></p> <p><i>Das Recht auf Löschung sollte allen Betroffenen gleichermaßen zur Verfügung stehen, und daher nicht durch eine Betonung dieses Rechtsanspruchs für Kinder unnötig relativiert werden.</i></p> <p><i>Absatz 2 des Artikels sollte gelöscht werden. Fraglich ist, wie er in der Praxis durchgesetzt werden sollte. Es ist beispielsweise nicht klar, was „vertretbare Schritte“ sind, durch die die verantwortliche Stelle die Benachrichtigung Dritter vor nehmen soll. Darüber hinaus wird es dem Verarbeitung Verantwortlichen oftmals gar nicht möglich sein, eine Benachrichtigung von dritten Stellen vor zu nehmen – kann er ja gar nicht wissen, welche Stellen dies sind. Ferner ist es nicht klar, wie diese Regelungen außerhalb des Internet angewendet werden sollen.</i></p> <p><i>In seiner bisherigen Form ist der Artikel nicht nur viel zu unbestimmt und praxisfern, seine Durchsetzung könnte darüber hinaus schwerwiegende Folgen nach sich ziehen. Allein der Versuch dieser Regelung nach zu kommen, beispielsweise durch das Löschen lassen von Internet-Links, könnte tief in die Meinungsfreiheit eingreifen.</i></p> <p><i>Wichtiger und auch sinnvoller ist, dass (wie in Artikel 13 der Verordnung bereits vor gesehen) wenn ein Verbraucher gegenüber einem Unternehmen einen Löschwunsch äußert, dieser Wunsch durch das Unternehmen immer dann an Dritte weiter geleitet werden muss, wenn es diesen die Daten übermittelt hat, unabhängig von einer Veröffentlichung.</i></p>	
<p style="text-align: center;"><i>Artikel 18 – Recht auf Datenübertragbarkeit</i></p> <p>1. Werden personenbezogene Daten elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet, hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten Daten in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format zu verlangen.</p> <p>2. Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und basiert die Verarbeitung auf einer Einwilligung oder einem Vertrag, hat die betroffene Person das Recht, diese personenbezogenen Daten sowie etwaige sonstige von ihr zur Verfügung gestellte Informationen, die in einem automatisierten Verarbeitungssystem gespeichert sind, in einem gängigen elektronischen Format in ein anderes System zu überführen, ohne dabei von dem für die Verarbeitung Verantwortlichen, dem die personenbezogenen Daten entzogen werden, behindert zu werden.</p> <p>[...]</p>	<p style="text-align: center;"><i>Artikel 18 – Recht auf Datenübertragbarkeit</i></p> <p>1. Werden personenbezogene Daten elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet, hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten Daten in einem von ihr weiter verwendbaren interoperablen, strukturierten, gängigen elektronischen Format zu verlangen.</p> <p>2. Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und basiert die Verarbeitung auf einer Einwilligung oder einem Vertrag, hat die betroffene Person hat das Recht, diese personenbezogenen Daten sowie etwaige sonstige von ihr zur Verfügung gestellte Informationen, die in einem automatisierten Verarbeitungssystem gespeichert sind, in einem gängigen elektronischen Format unentgeltlich in ein anderes System zu überführen, ohne dabei von dem für die Verarbeitung Verantwortlichen, dem die personenbezogenen Daten entzogen werden, behindert zu werden.</p> <p>[...]</p>

<p style="text-align: center;"><i>Begründung</i></p> <p><i>Die neue Regelung ist zu begrüßen, denn durch sie würde die Kontrolle der Verbraucher über ihre Daten gestärkt, der Markt geöffnet und somit marktbeherrschende Stellungen von Unternehmen verringert werden. Je leichter Verbraucher einen Anbieter wechseln können, umso weniger werden sie sich an diesen Anbieter gebunden fühlen, insbesondere wenn sie mit diesem Anbieter unzufrieden sind oder sich bei Veränderungen der Allgemeinen Geschäftsbedingungen oder Datenschutzrichtlinien neuen Regeln unterwerfen müssten. Datenschutz könnte so zu einem echten Wettbewerbsfaktor werden, durch den sich Unternehmen profilieren können, ohne durch Netzwerkeffekte ausgebremst zu werden.</i></p> <p><i>Allerdings sollte das Recht auf Datenübertragbarkeit nicht beschränkt werden auf Daten, die der verantwortlichen Stelle in einem „strukturierten gängigen“ Format vor liegen. So könnten sich datenverarbeitenden Stellen aus der Verantwortung stehlen, indem sie unübliche Formate verwenden. Auf der anderen Seite sollte dem Artikel zur Klarstellung hinzugefügt werden, dass die Daten, die dem Betroffenen zur Verfügung gestellt werden, interoperabel sein müssen, beispielsweise durch die Verwendung von quelloffenen Formaten.</i></p> <p><i>Auch muss der Fokus des Artikels auch auf Datenverarbeitungen ausgeweitet werden, die nicht auf Basis der Einwilligung oder vertraglicher Verpflichtungen vorgenommen werden. Eine Begrenzung des Rechts auf Datenübertragbarkeit auf diese Fälle ist nicht einleuchtend.</i></p> <p><i>Die Ausübung des Rechts darf ferner nicht dadurch ausgehebelt werden, dass die betroffene Person die anfallenden Kosten für die Übertragung übernehmen muss. Außerdem darf der Nutzer durch den für die Verarbeitung Verantwortlichen nicht dadurch behindert werden, dass dieser keine (technischen) Möglichkeiten der Überführung anbietet.</i></p> <p><i>Darüber hinaus sollte, beispielsweise in den Erwägungsgründen, nochmals betont werden, dass die Daten beim für die Verarbeitung Verantwortlichen gelöscht werden müssen, wenn der Zweck der Speicherung durch die Übertragung der Daten entfällt.</i></p>	
<p style="text-align: center;"><i>Artikel 19 – Widerspruchsrecht</i></p> <p>1. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben d, e und f erfolgt, Widerspruch einzulegen, sofern der für die Verarbeitung Verantwortliche nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.</p> <p>2. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, hat die betroffene Person das Recht, dagegen unentgeltlich Widerspruch einzulegen. Die betroffene Person muss ausdrücklich in einer verständlichen und von anderen Informationen klar abgegrenzten Form auf dieses Recht hingewiesen werden.</p> <p>[...]</p>	<p style="text-align: center;"><i>Artikel 19 – Widerspruchsrecht</i></p> <p>1. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben d, und e und f erfolgt, Widerspruch einzulegen, sofern der für die Verarbeitung Verantwortliche nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.</p> <p>2. Werden personenbezogene Daten aufgrund von Artikel 6 Absatz 1 Buchstabe f verarbeitet, um Direktwerbung zu betreiben, hat die betroffene Person das Recht, dagegen unentgeltlich Widerspruch einzulegen. Die betroffene Person muss vor Beginn der erstmaligen Verarbeitung ausdrücklich in einer verständlichen und von anderen Informationen klar abgegrenzten Form auf dieses Recht hingewiesen werden.</p> <p>[...]</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Das Widerspruchsrecht in Artikel 19 Absatz 2 lässt vermuten, dass Direktwerbung auf Basis des</i></p>	

Artikels 6 Absatz 1 Buchstabe f möglich sein soll. Dies ist abzulehnen. Eine Nutzung von personenbezogenen Daten zu Zwecken des Direktmarketings sollte – auch in Einklang mit der Richtlinie 2002/58/EG - nur mit Einwilligung der betroffenen Person möglich sein.

Hingegen sollten die in Absatz 2 aufgeführten Rechte der betroffenen Person und die Verpflichtungen der datenverarbeitenden Stelle, für alle Fälle bestehen, wenn Daten auf Basis des Artikels 6 Absatz 1 Buchstabe f verarbeitet werden. Damit die betroffene Person auch rechtzeitig von ihrem Widerspruchsrecht Gebrauch machen kann, sollte sie bereits vor Beginn der Verarbeitung über dieses Recht aufgeklärt werden.

Artikel 20 – Auf Profiling basierende Maßnahmen

1. Eine natürliche Person hat das Recht, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage etwa ihrer beruflichen Leistungsfähigkeit, ihrer wirtschaftlichen Situation, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens besteht.

2. Unbeschadet der sonstigen Bestimmungen dieser Verordnung darf eine Person einer Maßnahme nach Absatz 1 nur unterworfen werden, wenn die Verarbeitung

a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags vorgenommen wird und der Abschluss oder die Erfüllung des Vertrags auf Wunsch der betroffenen Person erfolgt ist oder geeignete Maßnahmen ergriffen wurden, um die berechtigten Interessen der betroffenen Person zu wahren, beispielsweise durch das Recht auf direkten persönlichen Kontakt, oder

[...]

Artikel 20 – Profiling und Auf Profiling basierende Maßnahmen

1. Eine natürliche Person hat das Recht, nicht ~~einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme~~ unterworfen zu werden, ~~die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage etwa ihrer beruflichen Leistungsfähigkeit, ihrer wirtschaftlichen Situation, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens besteht.~~ **die darin besteht, ihr einen Datensatz zuzuordnen, der eine bestimmte Gruppe von Menschen charakterisiert („Profil“), um insbesondere Entscheidungen in Bezug auf ihre Person zu treffen oder um ihre wirtschaftlichen Situation, ihren Aufenthaltsorts, ihren Gesundheitszustand, ihre Zuverlässigkeit, ihre persönlichen Vorlieben, Verhaltensweisen und Einstellungen zu analysieren oder vorherzusagen.**

2. Unbeschadet der sonstigen Bestimmungen dieser Verordnung darf eine Person einer Maßnahme nach Absatz 1 nur unterworfen werden, wenn die Verarbeitung

a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags vorgenommen wird und der Abschluss oder die Erfüllung des Vertrags auf Wunsch der betroffenen Person erfolgt ist oder geeignete Maßnahmen ergriffen wurden, um die berechtigten Interessen der betroffenen Person zu wahren, ~~beispielsweise indem~~ **Maßnahmen nach Absatz 1 nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden** ~~durch das Recht auf direkten persönlichen Kontakt, oder~~

[...]

2a. Absatz 2 gilt nicht, wenn die Datenverarbeitung ein Kind betreffen würde.

<p>3. Die automatisierte Verarbeitung personenbezogener Daten zum Zwecke der Auswertung bestimmter persönlicher Merkmale einer natürlichen Person darf sich nicht ausschließlich auf die in Artikel 9 genannten besonderen Kategorien personenbezogener Daten stützen.</p> <p>4. In Fällen gemäß Absatz 2 müssen die von dem für die Verarbeitung Verantwortlichen gemäß Artikel 14 erteilten Auskünfte auch Angaben zu einer etwaigen Verarbeitung für die unter Absatz 1 beschriebenen Zwecke und die damit angestrebten Auswirkungen auf die betroffene Person beinhalten.</p> <p>5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen, die für geeignete Maßnahmen zur Wahrung der berechtigten Interessen gemäß Absatz 2 gelten sollen, näher zu regeln.</p>	<p>[...]</p> <p>3. Die automatisierte Verarbeitung personenbezogener Daten zum Zwecke der Auswertung bestimmter persönlicher Merkmale einer natürlichen Person darf sich nicht ausschließlich auf die in Artikel 9 genannten besonderen Kategorien personenbezogener Daten stützen, es sei denn, sie sind unter den Maßgaben von Artikel 9 Absatz 2 erforderlich.</p> <p>3a. Ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen darf nur erhoben oder verwendet werden, wenn die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines anerkannten mathematisch-statistischen Verfahrens, dessen Prognosefähigkeit wissenschaftlich nachgewiesen werden kann, für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind.</p> <p>3b. Daten, die zum Zwecke des Profilings verarbeitet werden, dürfen nur an Dritte übermittelt werden, wenn diese Daten zum jeweiligen Zweck geeignet sind und keine Möglichkeiten der Fehlinterpretation lassen.</p> <p>4. In Fällen gemäß Absatz 2 müssen die von dem für die Verarbeitung Verantwortlichen gemäß Artikel 14 erteilten Auskünfte auch Angaben zu einer etwaigen Verarbeitung für die unter Absatz 1 beschriebenen Zwecke und die damit angestrebten Auswirkungen auf die betroffene Person beinhalten sowie die der Auswertung zugrunde liegenden Daten und ihre Gewichtung in einer nachvollziehbaren Form offen legen.</p> <p>5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen, die für geeignete Maßnahmen zur Wahrung der berechtigten Interessen gemäß Absatz 2 gelten sollen, näher zu regeln.</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Der Verbraucherzentrale Bundesverband sieht mit Sorge die zunehmende Bildung von Profilen der Verbraucher. Daher begrüßt der vzbv zwar entsprechende Regelungen, diese müssen allerdings dringend weiter geschärft werden. Die bisherigen Formulierungen werden nicht im Ansatz dem Gefahrenpotential der Profilbildung gerecht. Wichtig ist, dass Unterschiede bei der Profilbildung in den verschiedenen Wirtschaftssektoren oder rechtlichen Beziehungen berücksichtigt werden. Beispielsweise müssen sowohl die Profilbildung im Internet, aber auch in Offline-Umgebungen, wie beim Kredit scoring, ausreichend eingeschlossen werden.</i></p> <p><i>Derzeit werden von Artikel 20 nur Maßnahmen erfasst, die auf der Profilbildung basieren, nicht aber die Profilbildung selbst. Da aber schon die reine Bildung eines Profils in die Rechte der</i></p>	

betroffenen Person eingreift, sollte auch sie reglementiert werden. Dafür könnte die Definition des „Profiling“ aus der aus Europaratsempfehlung CM/Rec(2010)13 vom 23. November 2010 übernommen werden.

Weil Bewertungssysteme nur statistische Vergleiche mit Verhaltensweisen anderer Verbraucher anstellen können, sind die Fehler bei der konkreten Bewertung groß. Wird die Profilbildung Rahmen des Abschlusses oder der Erfüllung eines Vertrags vorgenommen, sollte daher die betroffene Person immer die Möglichkeit erhalten, vorgeblich erkannte statistisch Ergebnisse zu kommentieren, um eine akkurate, faire und nicht zu Unrecht schädigende Bewertung zu erhalten. Dabei reicht es nicht aus, das nur ein Gespräch mit einem Vertreter des Unternehmens geführt werden kann, dieser muss auch die Entscheidungsgewalt haben, automatisiert getroffene Bewertungen zu korrigieren.

Da Kinder besonders schutzbedürftig sind, sollte die Erhebung von Daten von Minderjährigen besonderen Restriktionen unterliegen, die auch nicht durch Einwilligungen aufgehoben werden können. Daher sollten Kinder immer von der Profilbildung ausgeschlossen werden. Dies ist zwar im Erwägungsgrund 58 vorgesehen, spiegelt sich aber bisher nicht im Regelungstext wieder.

Die Verarbeitung von den in Artikel 9 genannten besonderen Kategorien personenbezogener Daten ist gerade in Hinblick auf die Profilbildung besonders kritisch. Daher sollte die Nutzung dieser Daten für die Profilbildung ausgeschlossen werden, es sei denn diese Profilbildung ist unter den in Artikel 9 Absatz 2 genannten Maßgaben unbedingt erforderlich.

Besonders im Bereich des Kreditscorings gibt es in einigen Märkten, wie beispielsweise in Deutschland, oft als Betriebsgeheimnisse verborgene Bewertungskriterien, die nicht nachvollziehbare oder sachgerechte Ergebnisse aus Sicht der betroffenen Person liefern. So werden Schätzungen über die Kreditwürdigkeit auch jenseits harter Fakten angestellt. Daher sollten nachweisbar ausschließlich wissenschaftlich anerkannte mathematisch-statistischen Verfahren zur Berechnung eines Wahrscheinlichkeitswerts für ein zukünftiges Verhalten des Betroffenen verwendet werden dürfen. Die Prognose-tauglichkeit der Verfahren sollten durch eine unabhängige noch zu bestimmende (wie z.B. die Finanzdienstleistungsaufsicht) oder zu schaffende Stelle überprüft werden.

Ferner ist die Qualität der Daten besonders beim internationalen Austausch zu regulieren. Wer beim Kreditscoring in einem Land als besonders ausfallgefährdet betrachtet wird, ist nach bisherigen Erkenntnissen durchaus unterschiedlich. Beispielsweise sind es mal ledige Personen, mal Familien. Daher sollten nur die und solche Daten ausgetauscht werden dürfen, die zum jeweiligen Zweck geeignet sind und keine Möglichkeiten der Fehlinterpretation zu lassen.

Um Kontroll- und Korrekturmöglichkeiten der Verarbeitung auch durch die betroffene Person zu ermöglichen, muss die datenverarbeitende Stelle ferner die der Auswertung zugrunde liegenden Daten und ihre Gewichtung bei der Berechnung konkret in einer nachvollziehbaren Form offenlegen. Denn ist es der betroffenen Person nicht ersichtlich, aufgrund welcher Auswertungsverfahren eine sie betreffende Entscheidung zustande gekommen ist, kann sie weder Fehler oder Missverständnisse korrigieren noch ihre Interessen vertreten.

Artikel 22 – Pflichten des für die Verarbeitung Verantwortlichen	Artikel 22 – Pflichten des für die Verarbeitung Verantwortlichen
<p>1. Der für die Verarbeitung Verantwortliche stellt durch geeignete Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann.</p> <p>2. Die in Absatz 1 genannten Maßnahmen umfassen insbesondere</p>	<p>1. Der für die Verarbeitung Verantwortliche stellt durch die Umsetzung geeigneter Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann.</p> <p>2. Die in Absatz 1 genannten Maßnahmen umfassen insbesondere</p> <p>a1) die Gewährleistung der Rechte der Be-</p>

<p>[...]</p> <p>4. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere, in Absatz 2 nicht genannte Kriterien und Anforderungen für die in Absatz 1 genannten Maßnahmen, die Bedingungen für die in Absatz 3 genannten Überprüfungs- und Auditverfahren und die Kriterien für die in Absatz 3 angesprochene Angemessenheitsprüfung festzulegen und spezifische Maßnahmen für Kleinst-, Klein- und mittlere Unternehmen zu prüfen.</p>	<p>troffenen nach Kapitel III dieser Verordnung;</p> <p>[...]</p> <p>4. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere, in Absatz 2 nicht genannte Kriterien und Anforderungen für die in Absatz 1 genannten Maßnahmen, die Bedingungen für die in Absatz 3 genannten Überprüfungs- und Auditverfahren und die Kriterien für die in Absatz 3 angesprochene Angemessenheitsprüfung festzulegen und spezifische Maßnahmen für Kleinst-, Klein- und mittlere Unternehmen zu prüfen</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>Allein Strategien reichen nicht aus um sicher zu stellen, dass personenbezogene Daten nur in Übereinstimmung mit dieser Verordnung verarbeitet werden. Diese Strategien müssen auch praktisch umgesetzt werden.</i></p> <p><i>Die in diesem Artikel geforderten Maßnahmen sollten auch explizit die Gewährleistung der Rechte der Betroffenen nach Kapitel III der Verordnung beinhalten.</i></p> <p><i>Absatz 2 des Artikels beschreibt bereits ausreichend Kriterien und Anforderungen an geeignete Maßnahmen. Daher besteht keine Notwendigkeit an einem delegierten Rechtsakt.</i></p>	
<p><i>Artikel 23 – Datenschutz durch Technik und datenschutzfreundliche Voreinstellung</i></p> <p>1. Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung technische und organisatorische Maßnahmen und Verfahren durch, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden.</p> <p>2. Der für die Verarbeitung Verantwortliche setzt Verfahren ein, die sicherstellen, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung benötigt werden, und dass vor allem nicht mehr personenbezogene Daten zusammengetragen oder vorgehalten werden als für diese Zwecke unbedingt nötig ist und diese Daten auch nicht länger als für diese Zwecke unbedingt erforderlich gespeichert werden. Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht</p>	<p><i>Artikel 23 – Datenschutz durch Technik und datenschutzfreundliche Voreinstellung</i></p> <p>1. Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung technische und organisatorische Maßnahmen und Verfahren durch, die geeignet sind ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist und durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden.</p> <p>2. Der für die Verarbeitung Verantwortliche setzt Verfahren und Maßnahmen ein, die sicherstellen, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung benötigt werden, und dass vor allem nicht mehr personenbezogene Daten zusammengetragen oder vorgehalten werden als für diese Zwecke unbedingt nötig ist und diese Daten auch nicht länger als für diese Zwecke unbedingt erforderlich gespeichert werden. Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten</p>

<p>einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.</p>	<p>grundsätzlich nur den von der betroffenen Person zu bestimmenden Personen nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Insbesondere sind personenbezogene Daten und Profile zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen unverhältnismäßigen Aufwand erfordert.</p> <p>2a. Betreiber von Diensten der Informationsgesellschaft müssen Maßnahmen ergreifen, die die Nutzung dieser Dienste, ihre Bezahlung und die Möglichkeiten der betroffenen Person ihre Rechte wahr zu nehmen anonym oder pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist. Die betroffene Person ist über diese Möglichkeit zu informieren.</p> <p>2b. Die technische Gestaltung und Auswahl von Datenverarbeitungssystemen sollten unter den Gesichtspunkten der Absätze 1 bis 2 erfolgen. Darüber hinaus sollten Produkte und Dienste so voreingestellt sein, dass so wenig personenbezogene Daten wie möglich erhoben oder verarbeitet werden und dass personenbezogene Daten nur vom Betroffenen zu bestimmenden natürlichen Personen zugänglich gemacht werden.</p>
<p>3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Absätzen 1 und 2 genannten Maßnahmen und Verfahren festzulegen, speziell was die Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen betrifft.</p> <p>[...]</p>	<p>3. Der europäische Datenschutzausschuss erstellt Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Absätzen 1 und 2 genannten Maßnahmen und Verfahren festzulegen, speziell was die Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen betrifft.</p> <p>[...]</p>
<p align="center"><i>Begründung</i></p> <p>Nach dem Vorschlag der Kommission sollen die Prinzipien „data protection by design“ „data protection by default“ in das Datenschutzrecht eingeführt werden. Dies begrüßt der Verbraucherzentrale Bundesverband deutlich.</p> <p>Allerdings sollten die Schutzziele dieses Artikels im Erwägungsgrund 61 konkreter dargestellt werden. Hinsichtlich der Auswahl und Gestaltung von Datenverarbeitungssystemen müssen die Schutzziele der Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Nichtverkettbarkeit von personenbezogenen Daten und der Interventionsfähigkeit (i.S.v. technischen Möglichkeiten zur Ausübung von Betroffenenrechten) verfolgt werden. Allein 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.</p>	

<p><i>Konkrete Maßnahmen und Verfahren, wie Anonymisierung und Pseudonymisierung von personenbezogenen Daten, müssen gefordert werden. Außerdem sollte die explizite Verpflichtung von Unternehmen eingeführt werden, anonyme und pseudonyme Nutzungsmöglichkeiten - insbesondere von Internetdiensten - anzubieten.</i></p> <p><i>So sollte auch klar gestellt werden, dass alle Produkte und Dienste von Beginn an so voreingestellt sein müssen, dass sie den der Datenschutz-Grundverordnung zugrunde liegenden Prinzipien – wie Datenvermeidung und Zweckbindung - gerecht werden. Die betroffene Person sollte selbst die aktive Wahl haben, ob und wem ihre personenbezogenen Daten zugänglich gemacht werden.</i></p>	
<p><i>Artikel 33 – Datenschutz-Folgeabschätzung</i></p> <p>1. Bei Verarbeitungsvorgängen, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen, führt der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.</p> <p>[...]</p>	<p><i>Artikel 33 – Datenschutz-Folgeabschätzung</i></p> <p>1. Bei Verarbeitungsvorgängen, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen oder die auf Grundlage von Artikel 6 Absatz 1 Buchstabe f vorgenommen werden, führt der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.</p> <p>[...]</p>
<p><i>Begründung</i></p> <p><i>Siehe Begründung zu Artikel 6 Absatz 1 Buchstabe f</i></p>	
<p><i>Artikel 35 - Benennung eines Datenschutzbeauftragten</i></p> <p>1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls</p> <p>a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder</p> <p>b) die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder</p> <p>c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.</p>	<p><i>Artikel 35 - Benennung eines Datenschutzbeauftragten</i></p> <p>1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls</p> <p>a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder</p> <p>b) die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder</p> <p>e) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.</p> <p>1a. Die Pflicht zur Benennung gilt uneingeschränkt für Unternehmen, deren Haupttätigkeit die Verarbeitung personenbezogener Daten ist.</p>

[...]	<p>1b. Unternehmen, die personenbezogene Daten als Hilfstätigkeit zur Haupttätigkeit verarbeiten, sind von der Pflicht zur Bestellung eines Datenschutzbeauftragten ausgenommen, sofern</p> <p>a) der Umfang der Verarbeitung personenbezogener Daten, oder</p> <p>b) die Art der verarbeiteten personenbezogener Daten, oder</p> <p>c) die Art der Verarbeitung personenbezogener Daten, oder</p> <p>d) eine Kombination der vorgenannten Aspekte</p> <p>die Bestellung eines Datenschutzbeauftragten nicht erforderlich macht.</p> <p>1c. Unternehmen mit drei oder mehr Tätigen zeigen binnen Monatsfrist die Benennung eines Datenschutzbeauftragten oder den Grund für Ausnahme von der Bestellung gegenüber der Datenschutzaufsichtsbehörde an.</p> <p>[...]</p>
<p style="text-align: center;"><i>Begründung</i></p> <p><i>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.</i></p> <p><i>Diesen Ansätzen widerspricht aber, dass betriebliche Datenschutzbeauftragte künftig erst ab einer Schwelle von 250 Beschäftigten bestellt werden sollen. Dieser Wert ist deutlich zu hoch. Bisher mussten beispielsweise in Deutschland lediglich 10 Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sein. Die neue Regelung könnte daher zur Folge haben, dass ein Großteil der Unternehmen in Deutschland seine Aktivitäten im Bereich Datenschutz einstellt. Dadurch würde das Risiko von Datenschutzverletzungen für die Verbraucher 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. Die Aufsichtsbehörden müssten dann versuchen die Sachverhalte zeitnah aufzuklären, was zu einer deutlich höheren Belastung der staatlichen Datenschutzbeauftragten führen würde.</i></p> <p><i>Der Verbraucherzentrale Bundesverband plädiert daher für einen risikobasierten Ansatz, um die Notwendigkeit eines Datenschutzbeauftragten zu bestimmen. So sollte jedes Unternehmen, dessen Kerntätigkeit in der Verarbeitung personenbezogener Daten besteht, einen Datenschutzbeauftragten bestellen müssen. Dem gegenüber sollten Unternehmen, bei denen die Datenverarbeitung lediglich einen Hilfstätigkeit zur Haupttätigkeit darstellt von dieser Pflicht ausgenommen werden, es sei denn dass der Umfang, die Art der Daten, die Art der Verarbeitung oder eine Kombination dieser Aspekte die Bestellung eines Datenschutzbeauftragten erforderlich macht.</i></p>	

<p align="center"><i>Artikel 51 – Zuständigkeit</i></p> <p>[...]</p> <p>2. Findet die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten der Niederlassung eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der Union statt, wobei der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, so ist die Aufsichtsbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters befindet, unbeschadet der Bestimmungen von Kapitel VII dieser Verordnung für die Aufsicht über dessen Verarbeitungstätigkeit in allen Mitgliedstaaten zuständig.</p> <p>[...]</p>	<p align="center"><i>Artikel 51 – Zuständigkeit</i></p> <p>[...]</p> <p>2. Findet die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten der Niederlassung eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der Union statt, wobei der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, so ist die Aufsichtsbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters befindet, unbeschadet der Bestimmungen von Kapitel VII dieser Verordnung für die Aufsicht über dessen Verarbeitungstätigkeit in allen Mitgliedstaaten federführend zuständig.</p> <p>[...]</p>
<p align="center"><i>Begründung</i></p> <p><i>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 aber nicht zu einer Verschlechterung des Rechtsschutzes der Verbraucher führen. Daher sollte die Zuständigkeit der Aufsichtsbehörden vor Ort, keine absolute, sondern lediglich eine federführende sein.</i></p>	
<p align="center"><i>Artikel 73 – Recht auf Beschwerde bei einer Aufsichtsbehörde</i></p> <p>[...]</p> <p>2. Einrichtungen, Organisationen oder Verbände, die sich den Schutz der Rechte und Interessen der betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, haben das Recht, im Namen einer oder mehrerer betroffenen Personen Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde zu erheben, wenn sie der Ansicht sind, dass die einer betroffenen Person aufgrund dieser Verordnung zustehenden Rechte infolge der Verarbeitung personenbezogener Daten verletzt wurden.</p> <p>[...]</p>	<p align="center"><i>Artikel 73 – Recht auf Beschwerde bei einer Aufsichtsbehörde</i></p> <p>[...]</p> <p>2. Einrichtungen, Organisationen oder Verbände, die sich den Schutz der Rechte und Interessen der betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten oder den Schutz von Verbrauchern vor unlauteren Geschäftspraktiken zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, haben das Recht, im Namen einer oder mehrerer betroffenen Personen Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde zu erheben, wenn sie der Ansicht sind, dass die einer betroffenen Person aufgrund dieser Verordnung zustehenden Rechte infolge der Verarbeitung personenbezogener Daten verletzt wurden.</p> <p>[...]</p>
<p align="center"><i>Begründung</i></p> <p><i>Es ist zu begrüßen, dass Datenschutzorganisationen zukünftig mit dem Recht ausgestattet sein</i></p>	

sollen, bei einer Aufsichtsbehörde Beschwerde gegen Datenschutzverstöße einzulegen bzw. nach Artikel 75 Klage zu erheben. 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. Ansonsten werden diesen auch weiterhin im Bereich des Datenschutzes die Hände gebunden sein. Beispielsweise in Deutschland ist der Datenschutz nicht als verbraucherschützende Norm anerkannt, weshalb diesbezügliche Klagen durch Verbraucherorganisationen von den Gerichten scheitern. Die langjährigen Erfahrungen der Rechtsdurchsetzung, die in anderen Bereichen gesammelt wurden, können daher beim Datenschutz nicht eingesetzt werden. Gesetzeswidriges Verhalten bleibt demnach häufig ohne Konsequenzen und Sanktionen.

Artikel 78 (neu) – Recht auf Schmerzensgeld

1. Wegen eines Schadens, der nicht Vermögensschaden ist, kann nach Maßgabe von Artikel 77 über die dort geregelten Ansprüche hinaus eine billige Entschädigung in Geld gefordert werden.

2. Ist unter den Parteien streitig, ob ein Schaden entstanden sei und wie hoch sich der Schaden belaufe, so entscheidet hierüber das Gericht unter Würdigung aller Umstände nach freier Überzeugung.

Begründung

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. 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.

Daher sollte ein Schadensersatz für immaterielle Schäden eingeführt und die Beweislast für geschädigte Verbraucher verringert werden.