Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)593

Stellungnahme

zum Vorschlag der Europäischen Kommission für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25. Januar 2012 (KOM 2012/0011)

Kontakt:
Dr. Christian Koch
Telefon: +49 30 2021-2321
E-Mail: c.koch@bvr.de

Berlin, 18. Mai 2012

Registriernummer der Deutschen Kreditwirtschaft im Transparenzregister der Europäischen Union: 52646912360-95

Federführer:
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Schellingstraße 4 | 10785 Berlin
Telefon: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

Stellungnahme zum Vorschlag einer EU-Datenschutz-Grundverordnung

Die Europäische Kommission hat am 25. Januar 2012 ihren Vorschlag für eine Datenschutz-Grundverordnung vorgelegt, die die bisherige EU-Datenschutzrichtlinie aus dem Jahr 1995 ersetzen soll. Die Deutsche Kreditwirtschaft unterstützt grundsätzlich die damit beabsichtigte Modernisierung des Datenschutzrechts. Es gilt, hierbei einen angemessenen Schutz der Persönlichkeitsrechte der EU-Bürger unter Berücksichtigung der technischen Entwicklungen gerade im Bereich der modernen Informationstechnologien zu finden. Insbesondere begrüßen wir das Ziel, das Datenschutzrecht weiter zu vereinheitlichen, um im EU-Binnenmarkt ein „einheitliches Spielfeld" für alle Wirtschaftsunternehmen zu schaffen, Hindernisse im EU-Binnenmarkt zu beseitigen und Wettbewerbsverzerrungen zu vermeiden. Ebenso halten wir das Bestreben der Europäischen Kommission für sehr wichtig, bürokratische Regelungen abzubauen und das Datenschutzrecht zu vereinfachen.

Gleichwohl sehen wir noch erheblichen Verbesserungsbedarf im vorgeschlagenen Verordnungstext. Insbesondere erscheinen uns etliche Regelungen zu sehr als Reaktion auf die Wahrung des Datenschutzes im Internet, insbesondere in sozialen Netzwerken, gestaltet. Für konventionelle Datenverarbeitungen von Kundendaten in Unternehmen, wie u. a. in Kreditinstituten, führen diese durch das Internet ausgelösten Regelungen oftmals zu nicht sachgerechten Ergebnissen. Auch haben wir den Eindruck, dass etliche Regelungen (z. B. zu Informations- und Dokumentationspflichten, zur Folgenabschätzung) den formalen Aufwand für datenverarbeitende Unternehmen eher erhöhen als abbauen. Des Weiteren ist die äußerst extensive Nutzung des Instruments des „delegierten Rechtsakts" sowohl aus rechtsstaatlichen als auch inhaltlichen Gründen nicht akzeptabel: Die Unbestimmtheit etlicher Regelungen im Verordnungstext darf nicht durch delegierte Rechtsakte kompensiert werden, das Datenschutzrecht darf keine Dauerbaustelle sein. Überdies wird das für Kreditinstitute besonders wichtige Thema des Gleichklangs von datenschutz- und bankaufsichtsrechtlichen Anforderungen nicht ausreichend im Verordnungsvorschlag berücksichtigt. Auch fehlt es an einer Verbesserung der Rahmenbedingungen für die in einer arbeitsteiligen Wirtschaft immanente Datenverarbeitung im Konzern bzw. in Unternehmensverbünden.

Wir möchten daher die Gelegenheit nutzen, nachfolgend unsere wesentlichen Kernanliegen darzustellen. Unsere Anmerkungen und Änderungsvorschläge zu den einzelnen Vorschriften des Verordnungsvorschlags können der als Anlage beigefügten Synopse entnommen werden.

I. Grundsätzliche Themen

1. Verhältnis der Verordnung zu bestehenden Regelungen mit Datenschutzrelevanz klären

Eine Harmonisierung des Datenschutzrechts in der Europäischen Union und die Beseitigung von EU-Binnenmarkthindernissen unterstützen wir (s. o.). Das Instrument der Verordnung ist gerade für grenzüberschreitende Sachverhalte sehr sinnvoll. In Bezug auf rein nationale Sachverhalte ist allerdings nicht zu verkennen, dass die Verordnung weitgehend bewährte Datenschutzregelungen in den jeweiligen EU-Mitgliedstaaten beseitigen würde, die den dortigen nationalen Besonderheiten (z. B. nationale Kreditauskunfteien, gesetzliches Bankgeheimnis, Bankaufsichtsrecht) Rechnung tragen. Bei einer Weiterverfolgung des Verordnungsansatzes müssen daher gerade aus Sicht der Kreditwirtschaft folgende Spannungsfelder angemessen geklärt werden:

- Verhältnis zu bestehenden Datenschutzregelungen in anderen EU-Rechtsakten (z. B. in der EU-Verbraucherkreditrichtlinie),

- Möglichkeit der Konkretisierung der Verordnung durch nationale Rechtsvorschriften bzw. Fortbestand nationaler Spezialvorschriften (z. B. Vorschriften für Kreditauskunfteien, bankaufsichtsrechtliche Normen zur Geldwäsche-, Korruptions- und Betrugsbekämpfung, bankaufsichtsrechtliche Regeln zum Scoring, datenschutzrelevante Vorschriften im Wertpapierhandelsrecht, Datenschutzvorschriften im Telemediengesetz),
- Verhältnis zu den in einigen EU-Mitgliedstaaten geltenden gesetzlichen Regelungen zum Bankgeheimnis.

2. Widersprüche zum Bankaufsichtsrecht und zu bankspezifischen Zivilrechtsvorschriften vermeiden

Die Kreditwirtschaft wird bereits durch das Bankaufsichtsrecht streng reguliert. So müssen die Institute nach Artikel 22 der RICHTLINIE 2006/48/EG vom 14. Juni 2006 „über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute" über geeignete Organisations-, Steuerungs- und Risikokontrollinstrumente verfügen. Die Organisationsvorgaben zum Datenschutzmanagement im Unternehmen in der Verordnung (u. a. Artikel 22) würden sich mit diesen bankaufsichtsrechtlichen Pflichten überlappen und unnötigen Bürokratieaufwand für Banken hervorrufen. Zudem sind Kreditinstitute aufgrund bankaufsichtsrechtlicher Vorgaben zu umfangreichen Maßnahmen auf dem Gebiet der Betrugs-, Korruptions- und Geldwäschebekämpfung sowie der Risikokontrolle verpflichtet, die auch die Verarbeitung personenbezogener Daten betreffen und legitimieren.

Deshalb gilt es, bei der EU-Datenschutz-Grundverordnung Doppelregulierungen und Widersprüche zum EU-Bankaufsichtsrecht und den nationalen Bankaufsichtsvorschriften zu vermeiden. Hierzu sollte in der Verordnung festgelegt werden, dass eine Bank, die bereits ihre bankaufsichtsrechtlichen Pflichten zur Unternehmensführung erfüllt, damit auch vergleichbare datenschutzrechtliche Vorgaben erfüllt. Ordnen bankaufsichtsrechtliche Normen die Verarbeitung personenbezogener Daten an oder erlauben sie diese, muss die Verordnung das Bankaufsichtsrecht als spezialgesetzliche Regelung akzeptieren.

Überdies kollidieren einige Vorgaben der Verordnung mit zivilrechtlichen Regelungen für Kreditinstitute im EU-Recht, wie der EU-Verbraucherkredit- und EU-Zahlungsdiensterichtlinie. Auch hier gilt es, ein geeignetes Zusammenspiel der Normen in der Art zu finden, dass die Verordnung bankfachliche Vorschriften mit Datenschutzrelevanz akzeptiert.

3. Keine Übertragung von Gesetzgebungskompetenzen von Rat und Parlament auf die Europäische Kommission

Der Europäischen Kommission soll an 26 Stellen der Verordnung (vgl. Artikel 86) die Kompetenz zum Erlass von die Verordnung ergänzenden Vorschriften gegeben werden. Hierbei werden die in Artikel 290 des „Vertrages über die Arbeitsweise der Europäischen Union" (AEUV) gesetzten Grenzen für sog. „delegierte Rechtsakte" deutlich überschritten. Zwar sind die in Artikel 289 ff. AEUV genannten inhaltlichen oder formalen Anforderungen für delegierte Rechtsakte weit gefasst. Aus dem Zusammenspiel der Artikel 289 und 290 AEUV ergibt sich aber, dass eine Verordnung als Basisrechtsakt die wesentlichen materiellen Festlegungen nicht auf den abgeleiteten Rechtsakt übertragen darf. Dagegen beschränkt sich die Rechtsetzungsermächtigung des Verordnungsvorschlags vielfach nicht auf die Übertragung einer solchen „Konkretisierungskompetenz", sondern überlässt der Kommission weitgehend die Befugnis, den Regelungsgehalt eigenständig festzulegen. Damit erhält die Kommission die Befugnis, im Bereich des Datenschutzes

die Normen, deren einheitliche Anwendung sie nach der bisherigen Konzeption des Entwurfs überwachen soll, weitestgehend eigenständig zu schaffen. In dieser Kumulation von Rechtsetzungskompetenz und Verwaltungshandeln liegt aus unserer Sicht eine Durchbrechung des Gewaltenteilungsprinzips, die erheblichen rechtsstaatlichen Bedenken begegnet.

Überdies führt die angestrebte Befugnis zur Präzisierung strafbewehrter Vorschriften mittels delegiertem Rechtsakt, wie etwa die Sanktionierung eines Verstoßes gegen das Einwilligungserfordernis nach Artikel 79 Absatz 6 lit. l) i.V.m. Artikel 6 Absatz 1 lit. f) und Absatz 5, zu einem Konflikt mit dem strafrechtlichen Grundsatz des „nulla poena sine lege" nach Artikel 7 Absatz 1 EMRK. Dieser setzt voraus, dass eine anzuwendende Strafnorm bereits durch den Normgeber selber hinreichend bestimmt gefasst sein muss. Gegen den Charakter als Strafnorm spricht auch nicht, dass der Verordnungsentwurf die gesetzlichen Maßnahmen als „Verwaltungssanktionen" klassifiziert. De facto handelt es sich jedenfalls um die Einführung von Ordnungswidrigkeitstatbeständen, die gleichermaßen den strafrechtlichen Grundsätzen unterliegen.

Zudem befürchten wir, dass das Datenschutzrecht zur Dauerbaustelle wird und Unternehmen laufend neuen rechtlichen Anforderungen ausgesetzt werden. Dies wäre für die Rechtssicherheit und die Umsetzbarkeit des Datenschutzrechts kontraproduktiv. Soweit einzelne Regelungen derzeit noch der weiteren Konkretisierung bedürfen, sind diese möglichst sogleich in der Verordnung selbst vorzunehmen oder in der Verordnung müsste festgelegt werden, welche Themen späteren, gesonderten Rechtsakten vorbehalten sein sollen, die dann aber der Gesetzgebungskompetenz von Rat und Parlament unterliegen sollten.

Abzulehnen ist letztlich auch die in der Verordnung vorgesehene Delegierung hinsichtlich der Vorgaben für Datenformate (z. B. Artikel 18 Absatz 3) und Muster für die Erfüllung von Transparenzpflichten (z. B. Artikel 14 Absatz 8). Angesichts der bereits zitierten Vielzahl datenverarbeitender Sachverhalte erscheint eine einheitliche Vorgabe von Mustern und Dateiformaten kaum sinnvoll, um der jeweiligen individuellen Unternehmenssituation Rechnung zu tragen.

4. Vorschriften anlassbezogen ausgestalten und konventionelle Datenverarbeitungen nicht weiter erschweren

Der Verordnungsvorschlag ist vor allem dadurch motiviert, geeignete Antworten auf den Datenschutz im Internet, insbesondere in sozialen Netzwerken, zu finden. Gleichwohl beschränken sich die dazu vorgeschlagenen Normen nicht auf dieses Regelungsziel, sondern gelten allgemein, obwohl sie für „konventionelle Datenverarbeitungen" in Unternehmen nicht immer sachgerecht sind. „Konventionelle Datenverarbeitungen" in Unternehmen, wie z. B. in Kreditinstituten, würden damit unnötig bürokratisiert, eingeschränkt und/oder beeinträchtigt. Auch muss der organisatorische Aufwand, den Unternehmen zum Schutz der Daten zu treffen haben, in angemessenem Verhältnis zur Gefährdungslage stehen. Die Datenverarbeitungen in sozialen Netzwerken können naturgemäß angesichts der Art und des Umfangs der offenbarten privaten Daten (bis hin zur künftig möglichen chronologischen Darstellung ganzer Lebensläufe) für den Betroffenen ein erheblich höheres Risiko in sich bergen, als dies etwa bei der Verarbeitung von Daten im gewöhnlichen Geschäftsverkehr des dienstleistenden Gewerbes und insbesondere der Kreditwirtschaft der Fall ist. Gerade in der Kreditwirtschaft ist das Schutzniveau für das Persönlichkeitsrecht des Kunden aufgrund des parallel bestehenden Bankgeheimnisses besonders hoch. Daraus folgt, dass nicht jede durch die Herausforderungen des Internet motivierte Verschärfung des Datenschutzrechts zu pari für „konventionelle" Datenverarbeitungen übernommen werden darf.

Die aufgezeigten Probleme treten insbesondere auf bei den – in der „virtuellen Welt" des Internet durchaus nachvollziehbaren und ausweislich der Erwägungsgründe 52, 54 sowie 55 auch auf Online-Sachverhalte zugeschnittenen – Rechten des Betroffenen auf „elektronische Auskunftserteilung" (Artikel 15 Absatz 2), auf „Vergessenwerden" (Artikel 17 Absatz 2) und „Datenportabilität" (Artikel 18). Diese Vorschriften sollten sich auf internetbezogene Anwendungen beschränken.

5. Rechte datenverarbeitender Unternehmen angemessen berücksichtigen

Im Verordnungsvorschlag werden die nach deutschem Recht verfassungsmäßig geschützten Rechte und berechtigten Interessen datenverarbeitender Unternehmen nicht immer angemessen berücksichtigt. Das informationelle Selbstbestimmungsrecht des Betroffenen steht verfassungsrechtlich nicht isoliert, sondern bei der Schaffung gesetzlicher Regelungen sind auch die verfassungsmäßig garantierten Grundrechte der datenverarbeitenden Unternehmen zu berücksichtigen, wie insbesondere das in den Artikeln 2, 12 und 14 des Grundgesetzes garantierte Recht am eingerichteten und ausgeübten Gewerbebetrieb oder Grundrechte im Verwaltungs- und Gerichtsverfahren. Überdies sind auch die sonstigen berechtigten Interessen der datenverarbeitenden Unternehmen bei der Bestimmung der Reichweite der Schutzpflichten des Staates zur Wahrung des Rechts des Bürgers auf informationelle Selbstbestimmung in die Betrachtung mit einzubeziehen. Insgesamt gilt es, einen angemessenen Ausgleich zwischen den verfassungsrechtlich geschützten Rechtspositionen von Bürgern und Unternehmen zu finden.

Besonders deutlich wird dieser aktuell fehlende Interessenausgleich beim Recht des Betroffenen auf Herausgabe der über ihn gespeicherten Daten in Artikel 18 (Recht auf Datenübertragbarkeit). Es wird verkannt, dass es sich bei den – außerhalb von sozialen Netzwerken, Online-Datenbanken oder „Cloud"-Anwendungen – in „konventionellen" unternehmensinternen Datenbanken gespeicherten Kundendaten nicht um ausschließlich im „Eigentum" des Betroffenen stehende Daten („seine" Daten) handelt, die er selber dort eingestellt hat. Vielmehr handelt es sich um eine unternehmensinterne „elektronische Kundenakte", die bei Kreditinstituten zur Erfüllung vertraglicher Pflichten (z. B. Zahlungsdiensterahmenvertrag, Kreditvertrag) und gesetzlicher Pflichten (z. B. Handels- und Steuerrecht, Bankaufsichtsrecht) geführt wird. Überdies wird in Dauerschuldverhältnissen (z. B. Kontovertrag zwischen Kunde und Bank) damit ein Erfahrungswissen des Unternehmens über die Geschäftsbeziehung angesammelt, das für das Unternehmen einen besonderen wirtschaftlichen Wert bildet. Diese Informationen sind folglich ein Gut des Unternehmens, über das der Kunde kein alleiniges Verfügungsrecht in Gestalt eines Herausgabeanspruchs haben kann. Seinem Datenschutzinteresse wird bereits durch sein Recht auf Auskunft, Berichtigung und Löschung bzw. Sperrung ausreichend Rechnung getragen. Konsequenz des Rechts auf Datenportabilität wäre auch, dass andere Unternehmen – als Wettbewerber – das Erfahrungswissen beispielsweise einer Bank aus einer langjährigen Geschäftsbeziehung ohne Vergütung dessen Werts einfach „geschenkt" bekämen. Damit würde die aus einer bilateralen Vertragsbeziehung stammende „elektronische Kundenakte" zu einem frei verfügbaren Handelsgut. Eine solche Entwicklung dürfte auch eine massive Belastung für den gesamten Wirtschaftsstandort Deutschland darstellen, da gewachsene Kundenbeziehungen im internationalen Wettbewerb häufig der Grund dafür sind, dass sich deutsche Unternehmen gegen die Konkurrenz aus Staaten mit niedrigerem Lohnniveau durchsetzen können.

Weiter sind auch verfassungsmäßig geschützte Rechte von Unternehmen im Verwaltungs- und Strafrechtsverfahren zu berücksichtigen. Eine in einigen Regelungen anklingende Umkehr der Beweislast würde übermäßig die Rechte von Unternehmen im Verwaltungs- und Strafverfahren einschränken.

6. Übermäßige Formalisierung und Bürokratisierung vermeiden

Zu begrüßen ist, dass die Kommission mit dem Verordnungsvorschlag zugleich das Ziel verfolgt, den Datenschutz durch Vereinheitlichung nicht nur effektiver, sondern zugleich auch so zu gestalten, dass Unternehmen von überflüssigen Formalien entlastet werden. Der konkrete Verordnungstext vermittelt aber einen anderen Eindruck. Datenverarbeitende Unternehmen werden künftig – selbst im Vergleich zum allgemein als besonders hoch angesehenen deutschen Datenschutzniveau – durch eine Vielzahl weiterer Informations- und Dokumentationspflichten sowie Pflichten zur Erstellung von Folgenabschätzungen und Verbandskonsultationen belastet, ohne dass hierbei nach der konkreten Gefährdungssituation für die Betroffenen differenziert wird. Es sollte daher jede formale Anforderung einer Aufwand-Nutzen-Prüfung unterzogen und sodann bei der jeweiligen Anforderung eine Differenzierung nach Gefährdungslagen für die Persönlichkeitsrechte der Betroffenen vorgenommen werden.

II. Anwendungsbereich der Verordnung

1. Keine Erweiterung des Begriffs der „personenbezogenen Daten" (Artikel 4 Absätze 1 und 2), Förderung von Pseudonymisierungs- und Verschlüsselungsmaßnahmen

Der Anwendungsbereich der Datenschutzverordnung hängt maßgeblich von den Begriffsbestimmungen in Artikel 4 der „betroffenen Person" und der „personenbezogenen Daten" ab. Im Vergleich zur Definition in Artikel 2 Absatz a der EU-Datenschutzrichtlinie von 1995 erscheint die Begriffsbestimmung in Artikel 4 Absätze 1 und 2 weiter gefasst, weil nicht mehr alleine auf die Bestimmbarkeit des Personenbezugs durch die jeweils verarbeitende Stelle (subjektive Perspektive) abgestellt wird, sondern auch eine Bestimmbarkeit des Personenbezugs durch irgendeine Stelle ausreichen soll. Der datenschutzrechtlich negative Effekt ist, dass damit bisher bestehende Anreize zur Pseudonymisierung von Daten und zum Einsatz von Verschlüsselungstechniken beseitigt werden. Mit der Pseudonymisierung von Daten wird erreicht, dass andere Stellen, außer der die Pseudonymisierung vornehmenden Stelle, mangels des für die Entschlüsselung der Daten erforderlichen Zusatzwissens keinen Personenbezug herstellen können. Wenn Daten durch Pseudonymisierung bzw. Verschlüsselung besonders geschützt werden, dann sollte dies im Datenschutzrecht als datenschutzfreundliche Maßnahme gewürdigt werden. Dazu sollte die bisherige Definition aus der Richtlinie weiterverwendet und eine Differenzierung zwischen für jedermann personenbeziehbare Daten, pseudonymisierte Daten und anonymisierte Daten (diese fallen nicht in den Anwendungsbereich des Datenschutzrechts) vorgenommen werden. Gerade bei der zukunftsträchtigen Cloud-Technologie dürfte ein Anreiz zur Verschlüsselung der in die Cloud verlagerten Daten ein ganz erheblicher Fortschritt für den Datenschutz sein. Außer dem Cloud-Nutzer, d. h. der Stelle, die die Daten in der Cloud verarbeiten lässt, kann kein anderer einen Personenbezug aus den verschlüsselten Daten herleiten.

2. Bei Anwendung der Verordnung auf Verarbeiter in Drittstaaten Rechtskollisionen lösen (Artikel 3 Absatz 2)

Zielrichtung der neuen Regelung in Artikel 3 Absatz 2 ist die Erfassung von Internet-Anbietern in Drittstaaten, die Daten von EU-Bürgern verarbeiten. Diese Ausdehnung der Schutzwirkung des EU-Datenschutzrechts ist grundsätzlich nachvollziehbar und zur Vermeidung einer Flucht aus dem EU-Datenschutzrecht durch Off-Shore-Anbieter zu begrüßen. Jedoch ist zu bedenken, dass die Exterritorialitätsvorschrift auch für Töchter deutscher Kreditinstitute in Drittstaaten relevant (z. B. Bank in den

USA) sein würde, die in der EU ansässige Kunden haben. Somit stellt sich die Frage, wie eine etwaige Kollision von EU-Datenschutzrecht und ggf. zuwiderlaufenden Rechtsvorschriften im Drittstaat gelöst werden soll. Zumindest bei hoheitlichen Akten in dem Drittstaat (z. B. Beschlagnahme von Daten durch staatliche Behörden) sollte das Drittstaatrecht beachtet werden. So sollte – in Artikel 25 – eine Regelung geschaffen werden, die den Konflikt löst, wenn die Bank im Drittstaat besonderen aufsichtsrechtlichen Vorgaben oder hoheitlichen Eingriffen (z. B. strafrechtlichen Beschlagnahmen) unterliegt.

III. Rechtmäßigkeit der Datenverarbeitung

1. Funktionsweise von Kreditauskunfteien durch Beibehaltung der Datenverarbeitung im Drittinteresse erhalten (Artikel 6)

Artikel 6 des Verordnungsvorschlags stellt einen Katalog von alternativ erforderlichen Voraussetzungen für eine zulässige Datenverarbeitung auf. Artikel 6 Absatz 1 lit. f) des Verordnungstextes erlaubt entsprechend Artikel 7 lit. f) der Richtlinie 95/46/EG zwar die Datenverarbeitung insbesondere auch dann, wenn diese zur Wahrung berechtigter Interessen erforderlich ist. Anders als in der Richtlinie 95/46/EG reicht aber im Verordnungstext das Interesse eines Dritten, dem die Daten übermittelt werden, nicht zur Legitimation des Vorgangs aus. Die Einbeziehung des Drittinteresses in den Zulässigkeitstatbestand ist aber für die Datenübermittlung vom Kreditgeber an eine Kreditauskunftei zur Weiterleitung an andere dem System angeschlossene Kreditgeber unerlässlich, um die zentrale Datenaustauschfunktion derartiger Einrichtungen für die kreditgebende Wirtschaft zu erhalten. Anderenfalls würden Kreditauskunfteien in Frage gestellt, deren Bedeutung für Kreditgeber und -nehmer bei der Kreditvergabe in Artikel 9 der Richtlinie 2008/48/EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge besonders betont wird.

2. Keine Einschränkung des Einwilligungsprinzips (Artikel 7 Absatz 4)

Gemäß Artikel 7 Absatz 4 des Verordnungsvorschlags soll eine Einwilligung dann keine ausreichende Grundlage für die Datenverarbeitung sein, wenn zwischen der betroffenen Person und des für die Verarbeitung Verantwortlichen ein „erhebliches Ungleichgewicht" gegeben ist. Es besteht das Risiko, dass im Kunde-Bank-Verhältnis generell ein Ungleichgewicht unterstellt wird und deshalb die Einwilligungslösung für Banken faktisch verboten würde. Dies führt zu einer übermäßigen Bevormundung und dem Abbau von Gestaltungsrechten des Betroffenen und der datenverarbeitenden Stelle. Soweit das Prinzip der Freiwilligkeit der Einwilligung gewahrt ist, muss diese weiter zulässig bleiben. Überdies ist es Prinzip des Bankgeheimnisses als Jahrhunderte altem Handelsbrauch, dass der Kunde die Bank hiervon durch ausdrückliche Einwilligung in eine Datenweitergabe befreien kann. Das Datenschutzrecht sollte dieses Prinzip nicht konterkarieren.

3. Arbeitsteilige Strukturen in der Wirtschaft berücksichtigen durch Stärkung des Prinzips der gemeinschaftlichen Verantwortung (Artikel 24) und durch eigenständige Zulässigkeitsnorm für die Einschaltung von Auftragsverarbeitern (Artikel 26)

In der Wirtschaft gewinnt das arbeitsteilige Zusammenwirken immer mehr an Bedeutung. Kreditinstitute arbeiten in Konzernen und Verbünden zusammen und bedürfen der Inanspruchnahme externer Datenverarbeitungsdienstleister, auch außerhalb des EWR-Raums. Das modifizierte Verantwortlichkeitskonzept

(Artikel 22 und 24) in der Verordnung bietet mit der „gemeinsamen Verantwortung" bereits gute Ansätze für die gemeinschaftliche Datennutzung in Konzernen und Verbünden. Dabei muss aber weiter geklärt werden, dass eine gemeinsame Verantwortung von Stellen nicht nur eine Haftungsgemeinschaft begründet, sondern – in Abgrenzung zur erlaubnispflichtigen Datenübermittlung – auch den Datenaustausch in der Gruppe dem unternehmensinternen Datenverkehr bei einer alleinverantwortlichen Stelle gleichstellt. Dies wäre ein enormer Fortschritt, um den arbeitsteiligen Prozessen in Konzernen und Unternehmensverbünden Rechnung zu tragen. Nachteile für den Betroffenen sind dabei nicht erkennbar, denn der datenschutzrechtliche Zweckbindungsgrundsatz gilt fort und die beteiligten Stellen sind dem Betroffenen gemeinschaftlich gegenüber verantwortlich und haftbar.

In dem Zusammenhang müsste auch eine klare Abgrenzung zur Auftragsdatenverarbeitung vorgenommen werden, bei der nur der Auftraggeber die verantwortliche Stelle ist und die Einschaltung des Auftragnehmers den Voraussetzungen des Artikel 26 des Verordnungsvorschlags entsprechen muss. Dazu ist es erforderlich, in Abgrenzung zur erlaubnispflichtigen Datenübermittlung dem Artikel 26 den Charakter einer eigenständigen Zulässigkeitsvorschrift für den Datenaustausch zwischen Auftraggeber und Auftragnehmer zu geben. Zudem sind die Begriffe „Auftragsverarbeiter" (Artikel 4 Absatz 6) und „Empfänger" (Artikel 4 Absatz 7) entsprechend zu gestalten.

Ferner müssen für die Einschaltung von Stellen in Drittstaaten einfach umsetzbare Lösungen gefunden werden.

IV. Rechte der betroffenen Person

1. Informationspflichten bedarfsgerecht ausgestalten (Artikel 14)

Transparenz für den von der Datenverarbeitung Betroffenen ist sicherlich eine Grundvoraussetzung dafür, dass der Betroffene seine Rechte wahrnehmen kann. Doch schon im Verbraucherschutzrecht ist die Tendenz zu verzeichnen, dass durch gesetzliche Vorgaben die Menge der dem Bankkunden zu erteilenden Informationen ein Ausmaß erreicht hat, das die Gefahr birgt, vom Kunden als Belästigung wahrgenommen zu werden. Die Folge ist häufig eine Desensibilisierung für datenschutzrechtliche Belange. Insofern ist der mit Artikel 14 verfolgte Ansatz einer „umfassenden" Informationspflicht kontraproduktiv, wenn er in einer für den Kunden nicht mehr verarbeitbaren „Informationsflut" mündet. Dabei ist einzubeziehen, dass gerade Kreditinstitute vielfältigen spezialgesetzlichen Informationspflichten unterliegen, z. B. im Zahlungsverkehr-, Kredit- und Wertpapierbereich. Nun den Umfang der heute schon viele Seiten Papier füllenden Informationen für den Kunden noch weiter auszubauen, kann nicht im Kundeninteresse sein. Zielführender wäre ein zweistufiger Ansatz: Auf der ersten Stufe muss es ausreichen, dem Kunden allgemeine Informationen erteilen zu können. Erst bei dessen konkreter Nachfrage sollten in zweiter Stufe die Informationen bedarfsgerecht konkretisiert werden. Das bedeutet, dass gesetzliche Informationspflichten sich auf das unbedingt Erforderliche beschränken sollten und weitergehende Informationen erst auf Nachfrage zu erteilen sind (Beispiel: Der Kunde ist über das Vorliegen einer automatisierten Einzelentscheidung von der Bank zu informieren. Erst auf Nachfrage muss die Bank dem Kunden weitere Informationen geben).

2. Sachgerechte Gestaltung des Auskunftsrechts (Artikel 15)

Es muss sichergestellt werden, dass der Auskunftsanspruch des Betroffenen nach Artikel 15 nicht von Dritten instrumentalisiert wird, um eigene Informationsbedürfnisse zu stillen. So besteht bereits nach derzeitiger Rechtslage die sich zunehmend auch tatsächlich realisierende Gefahr, dass Betroffene dazu angehalten werden, von ihren datenschutzrechtlichen Informationsrechten Gebrauch zu machen, um etwa ihre Bonität gegenüber einem potentiellen Vermieter nachzuweisen. Betroffene geraten so oft durch das Auskunftsrecht erst unter den Druck, Sachverhalte offenbaren zu müssen, deren Kundgabe sie sonst möglicherweise aus berechtigtem Interesse verweigern dürften.

Zudem dürfen die Auskunftspflichten eines Unternehmens nicht dazu instrumentalisiert werden können, die Grenzen der Auskunftspflichten eines Verfahrensbeteiligten nach den nationalen Vorschriften zum gerichtlichen Zivilrechtsprozess und Strafrechtsprozess zu unterlaufen. Verfassungsmäßig garantierte Prozessrechte der Verfahrensbeteiligten müssen unberührt bleiben. Der Auskunftsanspruch durch den Betroffenen darf nicht selbst dazu missbraucht werden, etwa sich in Zivilprozessen unberechtigte Beweisvorteile zu verschaffen oder strafprozessuale Zeugnisverweigerungsrechte zu unterlaufen.

Ferner dürfen Auskunftsrechte – wie heute schon gesetzlich normiert – nur insoweit bestehen, als nicht ein berechtigtes Geheimhaltungsinteresse seitens der verantwortlichen Stelle gegeben ist.

Für den Datenschutz wäre es kontraproduktiv, dem Unternehmen generell eine Auskunftspflicht auf elektronischem Wege aufzuerlegen (Artikel 15 Absatz 2). Denn dies gefährdet dann den Datenschutz, wenn eine elektronische Auskunftserteilung nicht von einer sicheren Authentifizierung des Auskunftsersuchenden und einem sicheren elektronischen Transportweg abhängig gemacht werden kann (vgl. auch Erwägungsgrund 52).

3. Uneingeschränkte Datenportabilität nicht interessengerecht (Artikel 18)

Das in Artikel 18 vorgesehene Recht auf Datenportabilität ist nur insoweit sachgerecht, als der Betroffene bestimmte Internet-Plattformen zur eigeninitiativen Speicherung privater Daten nutzt. Diese Daten werden gerade nicht zur Erfüllung geschäftlicher Zwecke erhoben. Vielmehr verfolgt der Betroffene in diesen Fällen mit dem von ihm selbst vollzogenen Speichervorgang ausschließlich einen eigenen, in der Regel kommunikativen Zweck. Er stellt sein ansonsten nur bei sich befindliches Archiv von Daten (z. B. auf der Festplatte seines Rechners, Aufzeichnungen in Alben und Tagebüchern) einem Nutzerkreis online zur Verfügung. Damit verlagert er seine Datensammlung in die „Cloud" des sozialen Netzwerks. Die auf diese Weise gespeicherten Daten bleiben die Privatangelegenheit des Betroffenen und sein alleiniges Verfügungsrecht wird mit dem Portabilitätsanspruch gewahrt.

Auf die „konventionelle Datenverarbeitung" in unternehmensinternen Datenbanken ist dieser Gedanke nicht übertragbar. Die gespeicherten Daten erhebt die verantwortliche Stelle nur insoweit, als dies für die Abwicklung einer konkreten Geschäftsbeziehung erforderlich ist. Es handelt sich um geschäftliche Daten, deren Anordnung und Speicherung allein durch das Unternehmen in unternehmenseigenen Datenbanken gesteuert wird, auf die der Kunde selbst regelmäßig keinen direkten Zugriff hat. Eine solche „elektronische Kundenakte" dient zur Erfüllung vertraglicher Pflichten (z. B. Zahlungsdiensterahmenvertrag, Kreditvertrag) oder gesetzlicher Pflichten (z. B. Handels- und Steuerrecht, Bankaufsichtsrecht) und kann nicht mehr dem „geistigen Eigentum" des Kunden zugerechnet werden. Mit dem Recht auf Datenportabilität

würde diese Kundenakte, die gerade bei langjährigen Geschäftsbeziehungen von Traditionsunternehmen einen nicht unerheblichen Wert des Unternehmens ausmacht, zu einem freien Handelsgut. Dies würde zu einer nicht hinnehmbaren Wettbewerbsverzerrung zulasten solcher Unternehmen führen, die auf Kundenpflege besonderen Wert legen.

Das Recht auf Datenportabilität wäre in Bezug auf „konventionelle Datenverarbeitungen" nur vermeintlich eine Verbesserung des Datenschutzrechts. Dahinter steht ein rein wettbewerbspolitischer Ansatz, denn im Ergebnis wird über eine Instrumentalisierung des Betroffenen damit der kostenlose Zugriff von Wettbewerbern auf bei einem Unternehmen vorhandene Kundendaten schrankenlos ermöglicht. Folge wird auch sein, dass die Datenmacht von Internet-Plattformen, insbesondere sozialen Netzwerken, erheblich ausgebaut wird. Denn diese werden den Betroffenen dazu verleiten, mittels seines Portabilitätsanspruchs bislang dezentral vorhandene Datenbestände zur Vervollständigung seines „Lebenszyklus" auf diesen Plattformen zu konzentrieren. Aber auch außerhalb der „Internet-Welt" besteht die deutliche Gefahr, dass der Betroffene in vielen Fällen von Dritten zur Geltendmachung dieses Rechts instrumentalisiert werden wird, mit der Folge, dass der Zugriff auf personenbezogene Daten bei Unternehmen erleichtert und einmal erhaltene Dateikopien unbegrenzt zum Handelsgut werden (Beispiel: Vermieter könnten die Vorlage der elektronischen Kreditakte als Bonitätsnachweis von Mietinteressenten fordern.).

V. Pflichten des für die Datenverarbeitung Verantwortlichen

1. Meldepflichten bei Datenpannen auf wesentliche Ereignisse begrenzen (Artikel 31)

Nach derzeitigem Recht hat eine Meldung von Datenpannen an die Behörde nur dann zu erfolgen, wenn schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen (vgl. § 42a BDSG). Diese Ausprägung des Verhältnismäßigkeitsgrundsatzes sollte auch in Artikel 31 der Verordnung Berücksichtigung finden, da anderenfalls eine Überlastung der verantwortlichen Stellen (und der zuständigen Behörden) durch Meldungen von Bagatellfällen zu befürchten ist.

2. Datenschutz-Folgenabschätzung eingrenzen (Artikel 33)

Eine Datenschutz-Folgenabschätzung ohne jegliche Ausnahmen ist überflüssig und schafft nur neue, unnötige bürokratische Verfahren. Durch die allgemeinen Formulierungen ist unklar, welche Bereiche tatsächlich einer solchen Folgenabschätzung unterliegen. Diese Rechtsunsicherheit, der der Verantwortliche ausgesetzt wird, in Kombination mit den umfangreichen Verpflichtungen, denen er unterworfen wird (u. a. Beschreibung der Verarbeitungsvorgänge, Bewertung der Risiken, Abhilfemaßnahmen, Garantien, Meinungseinholung der betroffenen Person oder des Vertreters, Konsultation der Aufsichtsbehörde nach Artikel 34 Absatz 2 lit. a)), führt zu einem erheblichen Zuwachs an Bürokratie und Unsicherheit. Dies gilt umso mehr, als bei einem Verstoß gegen Artikel 33 nach Artikel 79 Absatz 6 lit. i) eine empfindliche Geldbuße verhängt werden kann.

3. Genehmigungserfordernis begrenzen (Artikel 34 Absatz 1)

Die Regelung zum Erfordernis einer vorherigen Genehmigung durch die Aufsichtsbehörde in Artikel 34 Absatz 1 ist missverständlich formuliert. Eine aufsichtsbehördliche Genehmigung sollte nur bei Datenübermittlungen in Drittstaaten erforderlich sein, wenn ein Fall nach Artikel 42 Absatz 2 lit. d) oder

Artikel 42 Absatz 5 vorliegt. Liegt eine Ausnahme nach Artikel 44 vor, dann sollte die Datenübermittlung keiner vorherigen Genehmigung durch die Aufsichtsbehörde bedürfen. Gerade im internationalen Zahlungsverkehr oder der weltweiten Wertpapierabwicklung beruhen damit einhergehende Datenübermittlungen auf Artikel 44 Absatz 1 lit. b) und c) (Übermittlung zur Erfüllung vertraglicher Pflichten). Ein Genehmigungserfordernis könnte seit Jahrzehnten zulässige Vorgänge in Frage stellen.

4. Bedeutung des betrieblichen Datenschutzbeauftragten wahren (Artikel 35 f.)

Das Instrument des betrieblichen Datenschutzbeauftragten hat sich in Deutschland sehr bewährt. Gerade in Kreditinstituten nimmt der betriebliche Datenschutzbeauftragte eine wichtige Funktion in der Selbstkontrolle wahr und hilft, gesetzeskonforme Datenverarbeitungen zu betreiben. Folglich ist zu begrüßen, dass dieses Instrument in der Verordnung gestärkt werden soll. Ob dazu aber die vorgesehenen Regelungen zu den Voraussetzungen für eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten beitragen, ist fraglich. Sofern die vorgenannten Pflichten zur Datenschutzfolgenabschätzung sowie zur Genehmigung von Datenverarbeitungsvorgängen entgegen der hier vertretenen Auffassung beibehalten werden sollen, sollte erwogen werden, Anreize für die Bestellung eines Datenschutzbeauftragten zu schaffen. Institute, deren betriebliche Prozesse eine Vielzahl von Datenverarbeitungsvorgängen beinhalten, sollten dazu von diesen Pflichten entbunden werden, wenn sie sich für die Einrichtung einer eigenständigen und neutralen Instanz zur Kontrolle von Datenverarbeitungsvorgängen entscheiden.

VI. Zertifizierungen auf Datenverarbeitungsdienstleister fokussieren (Artikel 39)

Die Einführung datenschutzrechtlicher Zertifikate bietet nur dort einen Mehrwert, wo Unternehmen Dienstleistungen erbringen, die in besonderer Weise datenschutzrechtlich relevant sind (z. B. gewerbliche Auftragsdatenverarbeiter). Eine Erstreckung auf andere Branchen würde eher zur Verunsicherung der Verbraucher und zur wirtschaftlichen Belastung kleinerer und mittlerer Unternehmen führen, die sich aus Marktdruck gezwungen sähen, den Zertifizierungsprozess zu durchlaufen.

Die Deutsche Kreditwirtschaft sieht auch insbesondere für ihren Tätigkeitsbereich keinen Bedarf für ein „Datenschutz-Siegel", da sich alle Banken und Sparkassen vertraglich zur Wahrung des Bankgeheimnisses verpflichtet haben, welches heute bereits höchstes Vertrauen der Kunden genießt.

VII. Datenschutzkontrolle durch Aufsichtsbehörden und Gerichte

1. Einheitlichkeit der Auslegung auch innerhalb der EU-Mitgliedstaaten sicherstellen (Artikel 46)

Zu begrüßen ist, dass die Kommission auch die Strukturen für eine einheitliche Rechtsauslegung zwischen den EU-Mitgliedstaaten verbessern will. Dieses Ziel kann aber nur dann sinnvollerweise für Kreditinstitute aller Mitgliedstaaten gleichermaßen erreicht werden, wenn auch innerhalb eines Mitgliedstaates eine einheitliche Auslegung sichergestellt ist. Derzeit wird die Datenschutzaufsicht in Deutschland durch die Bundesländer wahrgenommen, mit der Folge, dass deutschlandweit agierende Institute oder ein Verbund regional tätiger Institute wie Sparkassen und Genossenschaftsbanken sich mit zum Teil erheblich divergierenden Rechtsauslegungen von Aufsichtsbehörden in den verschiedenen Bundesländern auseinander-

zusetzen hat. Hier sollte dringend an früheren Überlegungen der Europäischen Kommission festgehalten werden, wonach die Aufsicht innerhalb eines EU-Mitgliedstaates vereinheitlicht werden soll.

2. Rollen klar abgrenzen (Artikel 46 ff., 57 ff. und 64 ff.)

Die Verordnung sollte dafür Sorge tragen, dass behördliche und gerichtliche Zuständigkeiten für das Datenschutzrecht allen Betroffenen und den Datenverarbeitern transparent und zur Wahrung des Gewaltenteilungsprinzips klar voneinander abgegrenzt sind. Hierzu ist die Verpflichtung zur Benennung einer zentralen Behörde pro EU-Mitgliedstaat ein begrüßenswerter Schritt, um im jeweiligen EU-Mitgliedstaat eindeutige Zuständigkeiten zu haben und unterschiedliches aufsichtsbehördliches Handeln innerhalb eines EU-Mitgliedstaates zu vermeiden.

Zudem sollte die Unabhängigkeit der jeweiligen Aufsichtsbehörde (Artikel 47) nicht durch Zuweisung von Aufsichtsbefugnissen an die Europäische Kommission unterlaufen werden. Vielmehr muss der vorgesehene Kohärenzprozess (Artikel 57 ff.) für ein abgestimmtes Handeln der nationalen Aufsichtsbehörden sorgen. Dazu kommt dem Europäischen Datenschutzausschuss (Artikel 64 ff.) eine zentrale Rolle zu. Die Europäische Kommission sollte nicht getrennt neben diesem Ausschuss stehen, sondern dort selber Mitglied sein. Als „Gleicher unter Gleichen" kann dann die Kommission an den aufsichtsbehördlichen Entscheidungen des Ausschusses mitwirken. Ein Unterlaufen des Ausschusses durch eine Sonderzuständigkeit der Kommission neben dem Ausschuss wird damit vermieden.

3. Kollektiver Rechtsschutz nicht sachgerecht (Artikel 73)

Die EU-Verordnung sollte keine neuen Instrumente kollektiver Rechtsdurchsetzung (vgl. Artikel 73) schaffen. Dem Recht auf informationelle Selbstbestimmung ist immanent, dass jedes Individuum entscheiden kann, welche Informationen es wem gegenüber wie preisgeben möchte. Folgerichtig wird es allgemein als ein höchstpersönliches Recht begriffen. Darum sollte auch die Rechtsdurchsetzung individuell erfolgen.

Einer Verbandsklage – etwa nach amerikanischem Vorbild – bedarf es zudem deswegen nicht, weil hierzulande jeder Verbraucher die Möglichkeit hat, sich auf Basis der Verordnung an die für ihn zuständige Behörde zu wenden, welche mit den zur Durchsetzung der Vorschriften dieser Verordnung notwendigen Befugnissen ausgestattet ist, über eine hohe Fachkompetenz verfügt und welche insbesondere keine sachfremden wirtschaftlichen Eigeninteressen verfolgt. Ergänzend kann die Hilfe eines Rechtsanwalts in Anspruch genommen werden.

Abzulehnen ist auch die Einführung einer gewillkürten Prozessstandschaft für sogenannte Datenschutzverbände nach Artikel 76 Absatz 1. Eine solche Regelung ist insbesondere mit deutschem Zivilprozessrecht nicht vereinbar. Ausreichend ist vielmehr die bereits bestehende nationale Regelung, wonach besonders qualifizierten Einrichtungen ein eigenes Klagerecht eingeräumt wird. Anderenfalls ist zu befürchten, dass Unterschiede der Mitgliedstaaten bei den Voraussetzungen zur Gründung derartiger Verbände ausgenutzt werden, um aus reinen Profitinteressen „Klagevereine" unter dem Deckmantel des Datenschutzes zu gründen.

4. Rechtsstaatlichkeit und Verhältnismäßigkeit bei Sanktionen beachten (Artikel 78 und 79)

Die Differenzierung zwischen „Sanktionen" (Artikel 78) und „verwaltungsrechtlichen Sanktionen" (Artikel 79) ist nicht nachvollziehbar. Es darf nicht zu einer doppelten Sanktionierung eines Verstoßes kommen. Zudem sind Bußgeldvorschriften originärer Bestandteil des Strafrechts und entziehen sich damit der Regelungszuständigkeit der Europäischen Union. Diese kollisionsrechtliche Regel würde umgangen, wenn man – wie in Artikel 79 Absätze 4 bis 6 angedacht – nun ein bis dato dem europäischen Recht fremdes „verwaltungsrechtliches Bußgeld" einführte.

Die von der EU-Kommission vorgeschlagenen Sanktionen von bis zu 2 % des weltweiten Jahresumsatzes stellen eine deutliche Verschärfung gegenüber derzeit gültigen Sanktionsregimen in den EU-Mitgliedstaaten dar. Die EU-Kommission verliert bei der Festsetzung der Höhe eines Bußgeldes den von ihr selbst aufgestellten Verhältnismäßigkeitsgrundsatz völlig aus dem Auge, indem die Sanktion im Verhältnis zum Verstoß nicht mehr zu rechtfertigende Dimensionen erreichen kann.

Zumindest ist eine Differenzierung im Hinblick auf die hinter einem Datenschutzverstoß stehende Motivation erforderlich. Im jetzigen Verordnungsentwurf erfolgt in den drei Kategorien der Sanktionshöhen (0,5 %, 1 % und 2 %) etwa keine Differenzierung im Hinblick auf vorsätzliches oder fahrlässiges Handeln – beide Handlungsformen werden vielmehr gleichgestellt und können nur im Rahmen des Ermessens der Aufsichtsbehörden bei der Festlegung der Höhe der Sanktion berücksichtigt werden.

Außerdem empfiehlt sich eine Differenzierung danach, ob ein Verstoß mit Bereicherungsabsicht erfolgte oder nicht. Dies gilt umso mehr für ein Sanktionsregime, das, ebenso wie das wettbewerbsrechtliche Sanktionssystem, an den weltweiten Jahresumsatz anknüpft. Geldbußen, die rechnerisch in Milliardenhöhe verhängt werden können, sind nicht zu rechtfertigen. Das gilt besonders, wenn der Datenschutzverstoß fahrlässig und ohne eine Absicht der Bereicherung geschehen ist.

VIII. Übergangsregelungen notwendig für Altfälle

Das Recht des Einzelnen auf informationelle Selbstbestimmung sollte nicht dadurch konterkariert werden, dass einmal erteilte Einwilligungen in eine Datenverarbeitung nachträglich unwirksam werden. Deswegen ist es erforderlich, Artikel 91 um eine Bestandsschutzregel für nach derzeitigem Recht erteilte Einwilligungserklärungen zu ergänzen.

Anmerkungen der Deutsche Kreditwirtschaft vom 16. Mai 2012

zu einzelnen Regelungen des
Vorschlags der Europäischen Kommission für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) [2012/0011 (COD)]

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 1 ***Gegenstand und Ziele***	
1. Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.	Die EU-einheitliche Regelung des Datenschutzrechts durch eine Verordnung ist zur Schaffung einheitlicher Rahmen- und Wettbewerbsbedingungen grundsätzlich zu begrüßen. Allerdings ist festzustellen, dass einige Regelungen im Verordnungsvorschlag noch nicht präzise genug gefasst sind. Im Vergleich zum Rechtsinstrument der Richtlinie müssen Vorschriften in einer Verordnung ein deutlich höheres Maß an Bestimmtheit aufweisen, da diese unmittelbar in jedem EU-Mitgliedstaaten gelten und für die Regelungsadressaten hinreichend verständlich sein müssen. Klärungsbedürftig ist ferner das Verhältnis zu

	datenschutzbezogenen Vorschriften in anderen EU-Rechtsakten und nationalen Gesetzen. Insbesondere die folgenden Spannungsfelder bedürfen der Klärung: • Verhältnis zu den datenschutzbezogenen Rechtsvorschriften anderer europäischer Rechtsakte (wie etwa der EU-Verbraucherkreditrichtlinie), • Verhältnis der Verordnung zu datenschutzbezogenen nationalen Rechtsvorschriften anderer Regelungsbereiche (z.B. den Vorschriften betreffend Kreditauskunfteien sowie bankaufsichtsrechtliche Regelungen zur Geldwäsche-, Korruptions- und Betrugsbekämpfung, zum Scoring) sowie spezialgesetzlichen Datenschutzvorschriften betreffend bestimmte Kommunikationsdienste (etwa durch das Telemediengesetz oder das Telekommunikationsgesetz), • Verhältnis zu den in einigen Staaten geltenden gesetzlichen Regelungen zum Bankgeheimnis.
2. Die Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.	
3. Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt oder verboten werden.	
Artikel 2 ***Sachlicher Anwendungsbereich***	
1. Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden	Die Regelungen des Artikel 2 Absatz 1 des Verordnungsentwurfs („VO-E“) entspricht dem sachlichen Anwendungsbereich der Richtlinie 95/47/EG. Insofern hat es sich bewährt, die Datenschutzvorschriften auf die strukturierte Erfassung von Daten zu

sollen.	beschränken. Ausweislich des Erwägungsgrundes 13 des VO-E sind damit auch künftig Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, vom Anwendungsbereich ausgenommen.
2. Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird	Die in Artikel 2 Abs. 2 VO-E vorgesehenen Bereichsausnahmen setzen ebenfalls auf den bewährten Regelung der Richtlinie 95/46/EG auf. Diese bedürfen allerdings als Verordnungsregelung einer weiteren Präzisierung.
a) im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt, etwa im Bereich der nationalen Sicherheit,	Soweit nur solche Tätigkeiten von dem Verordnungsentwurf umfasst sein sollen, die in den Geltungsbereich des Unionsrechts fallen, ist klarstellungsbedürftig, ob datenschutzrechtlich relevante Regelungsbereiche, für die die Gesetzgebungskompetenz ganz oder teilweise bei den EU-Mitgliedstaaten liegt, weiterhin nach den nationalen Datenschutzregelungen zu beurteilen sind. Betroffen wären hier datenschutzbezogene Sachverhalte im Bereich des Sozialrechts, des Betriebsverfassungsgesetzes, des Strafrechts, des Gesellschaftsrechts sowie des Telekommunikationsrechts.
b) durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union,	
c) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Kapitel 2 des Vertrags über die Europäische Union fallen,	Siehe Anmerkung zu Art. 2 Abs. 2 a)
d) durch natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht,	
e) zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden.	
3. Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und	

speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit von Anbietern von Vermittlungsdiensten unberührt.	
	Wie schon zu Artikel 1 dargelegt, fehlt eine Abgrenzungsregelung zu bereichsspezifischen Vorschriften mit Datenschutzrelevanz in anderen EU-Rechtsakten (wie der EU-Verbraucherkreditrichtlinie), zu bestehenden bereichsspezifischen Datenschutzvorschriften der einzelnen EU-Mitgliedstaaten (wie dem Telemediengesetz, dem Telekommunikationsgesetz etc.) und zu spezialgesetzlichen Vorschriften anderer Regelungsbereiche mit datenschutzrechtlichen Bezügen etwa des Bankaufsichtsrechts (wie § 10 Abs. 1 Satz 3ff., § 25c Abs. 2 KWG).
Artikel 3 ***Räumlicher Anwendungsbereich***	
1. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt.	
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	
a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, oder	Zielrichtung der neuen Regelung ist, die Erfassung von Internet-Anbietern in Drittstaaten, die Daten von EU-Bürgern verarbeiten. Diese Ausdehnung der Schutzwirkung des EU-Datenschutzrechts ist grundsätzlich nachvollziehbar, jedoch führt eine solche Einschränkung des völkerrechtlichen Territorialitätsprinzips bei Tochtergesellschaften deutscher Kreditinstitute (z.B. Bank in den USA) in Drittstaaten zu kollisionsrechtlichen Problemen, wenn diese

	zugleich in der EU ansässige Kunden haben. Unterliegt die Tochtergesellschaft im Drittstaat besonderen aufsichtsrechtlichen Anforderungen oder bestimmten hoheitlichen Eingriffen, wie z.B. strafrechtlichen Beschlagnahmen, so sollten diese im Konfliktfall vorrangig anzuwenden sein. Eine entsprechende Vorschrift könnte etwa in Artikel 25 des VO-E eingefügt werden.
b) der Beobachtung ihres Verhaltens dient.	
3. Die Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.	
Artikel 4 ***Begriffsbestimmungen***	
Im Sinne dieser Verordnung bezeichnet der Ausdruck	
(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 besonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;	Die Begriffsbestimmung begegnet Bedenken. Die Formulierung, wonach eine Bestimmbarkeit der Person mit „indirekten“ Mitteln ausreichend sein soll, um einen Personenbezug von Daten anzunehmen, könnte im Sinne einer sog. objektiven Bestimmtheit verstanden werden, wonach bereits ausreichend ist, dass irgendjemand, also nicht notwendigerweise die verantwortliche Stelle, die betreffende Person bestimmen kann. Damit wäre eine erhebliche Erweiterung des Anwendungsbereichs verbunden, mit der Folge, dass schon die Kombination Kontonummer und Bankleitzahl (zukünftig IBAN) als personenbezogen selbst dann einzustufen wäre, wenn der Empfänger dieser Daten über kein Zusatzwissen verfügt, um eine Namensverbindung mit einem solchen Zahlencode herzustellen. Bislang ist die subjektive Möglichkeit der datenverarbeitenden Stelle zur

	Personenbestimmbarkeit maßgeblich. An diesem Grundsatz sollte festgehalten werden, um auch Anreize für die datenschutzfreundliche Lösung der Pseudonymisierung bzw. der Verschlüsselung zu setzen. Positiv zu bewerten ist, dass der VO-E weiterhin auf den Schutz personenbezogener Daten von natürlichen Personen beschränkt bleiben soll (Erwägungsgrund 12). Dies entspricht auch dem bisherigen Ansatz der Richtlinie 95/46/EG sowie des Bundesdatenschutzgesetzes. Für einen besonderen Schutz von Daten juristischer Personen und (teil-)rechtsfähiger Personengesellschaften besteht auch weiterhin kein Anlass. Im Übrigen würde dies auch zu unlösbaren Widersprüchen mit den bestehenden Publizitätspflichten führen. Ferner sollte auch weiterhin an dem Prinzip festgehalten werden, anonymisierte Daten vom Anwendungsbereich auszunehmen (so Erwägungsgrund 23). Die Anonymisierung von Daten ist für Institute insbesondere im Bereich des Ratings ein wesentliches Instrument zur Wahrung des Grundsatzes der Datensparsamkeit. Letztlich besteht für den Betroffenen auch kein besonderes Schutzinteresse mehr, wenn Merkmale etwa zu statistischen Zwecken genutzt werden, ohne dass ein Bezug zu seiner Person hergestellt werden kann. Aus dem gleichen Grund sollte auch die Pseudonymisierung weiterhin gesetztlich anerkannt werden. Sowohl Anonymisierung als auch Pseudonymisierung sollten unmittelbar in Artikel 4 definiert werden. Offen bleibt auch nach Erwägungsgrund 24, ob IP-Adressen oder Cookie-Kennungen personenbezogen sind. Maßgeblich sollte hier ebenfalls die subjektive Bestimmbarkeit sein. Diese Frage sollte angesichts der bestehenden Rechtsunsicherheiten durch den Gesetzgeber abschließend geklärt werden.
(2) „personenbezogene Daten" alle Informationen, die sich auf eine	Siehe dazu die Anmerkungen zu Artikel 4

	betroffene Person beziehen;	Absatz 1.
(3)	„Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung–, Verbreitung oder jede andere Form der Bereitstellung an Empfänger, der Abgleich oder die Verknüpfung sowie das Löschen, Sperren –oder Vernichten der Daten;	Die Definition des Verarbeitungsbegriffs knüpft zwar an Artikel 2 Abs. b der Richtlinie 95/46/EG an, lässt aber im Gegensatz zur Vorgängervorschrift das notwendige Maß an Konkretisierung vermissen. So ist nicht ersichtlich, warum das „Sperren“ aus dem Katalog der Verarbeitungs-tatbestände gestrichen worden ist. Dies sollte gerade auch im Verhältnis zur Löschung als „milderes Mittel“ der Datenverarbeitung in die Definition aufgenommen werden Zudem sollte der Begriff „Löschen“ wie in § 3 Abs. 4 Nr. 5 BDSG definiert werden als *„das Unkenntlichmachen gespeicherter personenbezogener Daten“.* Dies ist ins-besondere zur Erfüllung der Anforderungen in Artikel 17 VO-E notwendig. Das Tatbestandsmerkmal der Übermittlung sollte auf Datenweiterleitungen an „Empfänger“ im Sinne des Artikel 4 Absatz 7 beschränkt werden (zu der notwendigen Konkretisierung des Empfängerbegriffs siehe Kommentierung zu Abs. 7).
(4)	„Datei" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;	
(5)	"für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke, Bedingungen und Mittel der	

	Verarbeitung von personenbezogenen Daten durch einzelstaatliches oder Unionsrecht vorgegeben, können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung nach einzelstaatlichem oder Unionsrecht bestimmt werden;	
(6)	"Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;	Wie in der EU-Datenschutzrichtlinie angelegt, sollte aus der Definition in Artikel 4 Absatz 7 bzw. Artikel 26 VO-E deutlich werden, dass der Datenaustausch mit dem Auftragsverarbeiter keine Datenübermittlung ist, sondern alleine den Zulässigkeitsregeln für eine Auftragsdatenverarbeitung nach Artikel 26 VO-E unterliegt.
(7)	"Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem oder den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten; ~~, an die personenbezogene Daten weitergegeben werden;~~	Der VO-E unterscheidet im Gegensatz zur Richtlinie 95/46/EG nicht mehr zwischen „Dritter“ und „Empfänger“. Stattdessen wird die Definition des „Dritten“ aus Artikel 2 f) der EU-Datenschutzrichtlinie für den Begriff „Empfänger“ verwendet. Wenn die Begrifflichkeiten nunmehr unter dem Wort „Empfänger“ zusammengefasst werden sollen, muss allerdings entsprechend der Definition in Artikel 2 f) der Richtlinie 95/46/EG klargestellt werden, dass mit „Empfänger“ nur Stellen außerhalb der verantwortlichen Stelle gemeint sind (vgl. insoweit Anmerkung zu Abs. 3).
(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;	Positiv zu bewerten ist, dass die Einwilligung nicht der Schriftform bedarf, wie dies aktuell - in Abweichung von der EU-Datenschutzrichtlinie - nach § 4a BDSG der Fall ist. Damit wird den geänderten Rahmenbedingungen gerade im elektronischen Geschäftsverkehr Rechnung getragen. Der Betroffene wird dabei mit der vorgesehenen Beweislastverteilung hinreichend geschützt. Es obliegt dem Verantwortlichen, durch sachgerechte Gestaltung der Prozesse die Einwilligung des Betroffenen nachweissicher einzuholen. Wie bereits im nationalen Recht vorgesehen

		wird auch nach dem VO-E eine informierte Einwilligungserklärung vorausgesetzt (Erwägungsgrund 25). Kritisch zu sehen sind jedoch die Ausführungen in Erwägungsgrund 33, wonach eine Einwilligungserklärung unwirksam ist, wenn der Betroffene „keine echte Wahlfreiheit hat und somit nicht in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden“. Diese Ausführungen sind zu vage. Grundsätzlich steht es den Beteiligten frei, Einwilligungen im Rahmen von Vertragsbeziehungen zu verweigern, wenn ihnen die angebotenen Konditionen nicht zusagen. In Ausübung dieser Wahlfreiheit kann der Betroffene entscheiden, ob er eine Bindung eingehen möchte oder nicht. Dieses Prinzip muss auch grundsätzlich erhalten bleiben. Sanktionswürdig ist insoweit nur die unzulässige Kopplung von Einwilligungen in die Datenverarbeitung und Erbringung einer vertraglichen Leistung, auf dessen Inanspruchnahme gerade vom Verantwortlichen der Betroffene zur Sicherung seiner Teilnahme am öffentlichen Leben und zur Befriedigung seiner Grundbedürfnisse angewiesen ist. Dies ist etwa bei Monopolstellungen denkbar. Die mit dem VO-E geplanten Anforderungen an die Freiwilligkeit gehen aber über die aktuellen Voraussetzungen nach deutschem Recht für eine freiwillige Einwilligungserklärung weit hinaus. Erwägungsgrund 33 sollte daher entsprechend angepasst werden. Vorbild könnte hier § 4a Abs. 1 BDSG sein, wonach „die Einwilligung nur wirksam ist, wenn sie auf der freien Entscheidung des Betroffenen beruht.“
(9)	"Verletzung des Schutzes personenbezogener Daten" eine schwerwiegende Verletzung der Sicherheit, die ~~zur Vernichtung~~, zumVerlust oder zur Veränderung, ob unbeabsichtigt oder widerrechtlich, oder zur unbefugten Weitergabe von beziehungsweise	Die Definition der „Verletzung des Schutzes personenbezogener Daten“ birgt die Gefahr in sich, im Zusammenspiel mit den im Rahmen des VO-E vorgesehenen Meldepflichten zu einer für die Aufsichtsbehörden sowie die Betroffenen nicht mehr zu bewältigenden Informations- und Meldeflut zu führen. Um dies zu vermeiden, sollten

	zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;	nach dem Vorbild der Regelung des § 42a BDSG die Meldepflicht auf „schwerwiegende“ Beeinträchtigungen beschränkt werden. Bei einer Vernichtung von Daten besteht eigentlich aus Sicht des Betroffenen kein Missbrauchsrisiko bezüglich seiner Daten, das eine Warnung begründen würde. Daher sollte der Vorgang „Vernichtung“ keine datenschutzrechtliche Meldepflicht auslösen.
(10)	„genetische Daten“ Daten - mit Ausnahme des Geschlechts - jedweder Art zu den ererbten oder während der vorgeburtlichen Entwicklung erworbenen Merkmalen eines Menschen;	Eine Regelung für „genetische Daten“ erscheint durchaus sachgerecht. Allerdings muss auch hier wieder beachtet werden, dass nicht „versehentlich“ Prozesse der gewöhnlichen Datenverarbeitung im Geschäftsverkehr erschwert werden. Unter diesem Blickwinkel ist es zu weitgehend, auch das Geschlecht eines Menschen als genetisches Datum zu erfassen, da dieses häufig schon aus dem Namen bzw. der Anrede erkennbar ist. Ansonsten würden alle Kundenstammdatensätze den Sonderregeln für genitische Daten unterliegen.
(11)	„biometrische Daten“ Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die dessen eindeutige Identifizierung ermöglichen, wie Gesichtsbilder oder daktyloskopische Daten (;die Unterschrift des Betroffenen ist ausgenommen);	Siehe auch Art. 33 Abs. 2 d). Der neuen Datenart der „biometrischen Daten“ kann Relevanz zukommen bei biometrischen Authentifzierungsverfahren (Iriserkennung, Fingerabdruck, etc.). Um aber auch hier herkömmliche Verfahren nicht unnötig einzubeziehen, sollte in der Definition festgehalten werden, dass die händische Unterschrift eines Menschen nicht unter diesen Begriff zu fassen ist. Andernfalls würden gewöhnliche Verfahren der Geschäfte des täglichen Lebens unter den Anwendungsbereich einer Folgenabschätzung nach Art. 33 VO-E fallen (siehe auch die Kommentierung dort).
(12)	„Gesundheitsdaten“ Informationen, die sich auf den körperlichen oder geistigen Gesundheitszustand einer Person oder auf die Erbringung von Gesundheitsleistungen für die	Relevant bei Mitarbeiterdaten sowie ggf. bei Betreuungssachverhalten (Führung von Konten für unter gesetzlicher Betreuung stehender Personen).

	betreffende Person beziehen;	
(13)	„Hauptniederlassung“ im Falle des für die Verarbeitung Verantwortlichen der Ort seiner Niederlassung in der Union, an dem die Grundsatzentscheidungen hinsichtlich der Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten getroffen werden; wird über die Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten nicht in der Union entschieden, ist die Hauptniederlassung der Ort, an dem die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen in der Union hauptsächlich stattfinden. Im Falle des Auftragsverarbeiters bezeichnet „Hauptniederlassung“ den Ort, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat;	
(14)	„~~Vertreter~~Repräsentant“ jede in der Union niedergelassene natürliche oder juristische Person, die von dem für die Verarbeitung Verantwortlichen ausdrücklich bestellt wurde und in Bezug auf die diesem nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle handelt und gegenüber den Aufsichtsbehörden oder sonstigen Stellen in der Union als Ansprechpartner fungiert;	Klarstellung im Vergleich zur englischen Fassung und in Bezug auf Artikel 25.
(15)	„Unternehmen“ jedes Gebilde, das eine selbständige wirtschaftliche Tätigkeit ausübt, unabhängig von seiner Rechtsform, das heißt vor allem natürliche und juristische Personen sowie Personengesellschaften oder Vereinigungen, die regelmäßig einer selbständigen wirtschaftlichen	= juristische Person, Gewerbetreibende, Einzelkaufleute, Freiberufler (nicht Verbraucher), Klarstellung, dass nicht Mitarbeiter eines Unternehmens erfasst sind.

	Tätigkeit nachgehen;	
(16)	„Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;	
(17)	„verbindliche unternehmensinterne Datenschutzregelungen“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines EU-Mitgliedstaats niedergelassener für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe in einem oder mehreren Drittländern verpflichtet;	
(18)	„Kind“ jede Person bis zur Vollendung des achtzehnten Lebensjahres;	
(19)	„Aufsichtsbehörde“ eine von einem Mitgliedstaat nach Maßgabe von Artikel 46 eingerichtete staatliche Stelle.	

KAPITEL II
GRUNDSÄTZE

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 5 ***Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten***	
Personenbezogene Daten müssen	
a) auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in ~~einer~~	Zutreffend ist, dass die Verarbeitungs-vorgänge grundsätzlich in ihren für den

~~für die betroffene Person~~ nachvollziehbaren Weise verarbeitet werden;	Betroffenen wesentlichen Zügen nachvollziehbar sein sollten. Allerdings knüpft die Vorschrift an eine subjektive Nachvollziehbarkeit der konkret betroffenen Person an. Maßgeblich kann aber nicht die Auffassungsgabe und intellektuelle Leistungsfähigkeit des Einzelnen sein. Es muss vielmehr auf die objektive Nachvollziehbarkeit eines „Durchschnitts-Betroffenen“ abgestellt werden.
b) für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;	
c) dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Maß ausgerichtet sein ~~Mindestmaß beschränkt sein; sie dürfen nur verarbeitet werden, wenn und solange die Zwecke der Verarbeitung nicht durch die Verarbeitung von anderen als personenbezogenen Daten erreicht werden können~~;	Der Zweckbindungsgrundsatz sollte nicht mit dem Grundsatz der Datensparsamkeit und -vermeidung vermischt werden. Zudem könnte eine Kollision mit Datenverarbeitungen aufgrund vom Betroffenen freiwillig erteilten Angaben auftreten.
d) sachlich richtig und, wenn nötig, auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unzutreffend sind, unverzüglich gelöscht oder berichtigt werden;	Die Einschränkung „wenn nötig“ aus Art. 6 Abs. 1 d) EU-Datenschutzrichtlinie sollte beibehalten werden, um die Überprüfungs-zyklen von der tatsächlichen Notwendigkeit abhängig machen zu können, die sich nach Datenart und Verarbeitungszweck erheblich unterscheiden kann. Es sollte überlegt werden, eine Mitwirkungspflicht des Betroffenen zu normieren, die verantwortliche Stelle über Änderungen in seiner Sphäre zu informieren.
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, jedoch höchstens so lange, wie es für die Realisierung der Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, wenn die Daten ausschließlich zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke im	Zu begrüßen ist, dass im Umkehrschluß bei Zweckablauf die Daten noch in anonymisierter Form weiterverarbeitet werden dürfen. Es sollten zudem die besonderen Anforderungen der - zumeist national geregelten - gesetzlichen handels- und steuerrechtlichen sowie bankaufsichtsrechtlichen Aufbewahrungspflichten (u. a. § 146 AO, §§ 256, 257 HGB, § 34 Abs. 3 WpHG, § 8 Abs. 3

Einklang mit den Vorschriften und Modalitäten des Artikels 83 verarbeitet werden und die Notwendigkeit ihrer weiteren Speicherung in regelmäßigen Abständen überprüft wird;	GwG) Berücksichtigung finden.
f) unter der Gesamtverantwortung des für die Verarbeitung Verantwortlichen verarbeitet werden, der dafür haftet, dass bei jedem Verarbeitungsverfahren ~~jedem Verarbeitungsvorgang~~ die Vorschriften dieser Verordnung eingehalten werden, ~~und der den Nachweis hierfür erbringen muss.~~	Die deutsche Fassung weicht deutlich vom englischen Entwurf ab, die lautet: *"processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation"* Insbesondere der Begriff „Gesamtverantwortung" ist nicht deckungsgleich mit der englischen Fassung. Auch ist die Rechtsnatur der Vorschrift unklar. Sie beantwortet insbesondere nicht die Frage, ob nur eine Geltung in Bezug auf eine zivilrechtliche Haftung gewollt ist oder ob der Begriff auch verwaltungsrechtlich bei der Bestimmung des Adessatenkreises im Sanktionsverfahren durch die Aufsichtsbehörden relevant wird (Strafrecht, Ordnungswidrigkeit). Im letzteren Fall bestünden nach nationalem Verfassungsrecht erhebliche rechtsstaatliche Bedenken gegen die Vorschrift, da die damit einhergehende Beweislastumkehr nicht mit rechtsstaatlichen Grundsätzen im Verwaltungs- und Strafrecht vereinbar wäre. Insgesamt sollte nicht an einzelne Verarbeitungsvorgänge, sondern an Verarbeitungsverfahren angeknüpft werden.
Artikel 6 ***Rechtmäßigkeit der Verarbeitung***	
1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:	
a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie	

betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben.	
b) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die im Interesse ~~auf Antrag~~ der betroffenen Person erfolgen.	Das Tatbestandsmerkmal „auf Antrag“ ist jedenfalls nach deutschem Rechtsverständnis zu eng gefasst und bildet gerade nicht alle Möglichkeiten ab, die ein die Verarbeitung von Kundendaten rechtfertigendes vorvertragliches Schuldverhältnis begründen kann.
c) Die Verarbeitung ist zur Erfüllung einer gesetzlichen Verpflichtung oder Erlaubnis, einer aufsichtsrechtlichen Anforderung oder einer anderen Rechtsvorschrift erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.	Sicherzustellen ist, dass der Erlaubnistatbestand jegliche Form von gesetzlichen Pflichten und Erlaubnissen sowie auch darauf beruhender aufsichtsbehördlicher Anordnungen erfasst. Datenverarbeitungen bei Banken beruhen in vielen Fällen auf aufsichtsrechtlichen Anforderungen. Zudem fehlt die bisherige Einbeziehung von Tarifvereinbarungen und Betriebsvereinbarungen als „andere Rechtsvorschrift“.
d) Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person zu schützen.	
e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde.	
f) Die Verarbeitung ist erforderlich zur Wahrung des~~r~~ berechtigten Interesses~~n~~, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Empfängern wahrgenommen wird, denen die Daten übermittelt werden~~, 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. Dies~~er~~ gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.	Nach der EU-Datenschutzrichtlinie sind auch schutzwürdige Interessen Dritter einbeziehbar. Dies ist wichtig beispielsweise für die Funktionsweise von Kreditauskunfteien. Artikel 7f der Richtlinie lautet bislang *„f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiesen.“* Insofern sollte hier auch das Interesse des bzw. der Empfänger berücksichtigt werden. Sofern eine Datenverarbeitung nach Art. 6

	Abs. 1 f VO-E legitimiert ist, wäre es bloßer Formalismus, wenn der Betroffene, wie in Erwägungsgrund 38 vorgesehen, vom Verantwortlichen über sein Widerspruchsrecht informiert werden muss und der Verantwortliche seine berechtigten Interessen gegenüber dem Betroffenen ausdrücklich darlegen muss. Über die Interessenabwägung müsste auch die Verarbeitung öffentlich zugänglicher Daten erfasst sein (vgl. § 28 Absatz 3 BDSG).
2. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke unterliegt den Bedingungen und Garantien des Artikels 83.	
3. Die Verarbeitungen gemäß Absatz 1 Buchstaben c und e müssen einer gesetzlichen Verpflichtung oder Erlaubnis, einer aufsichtsrechtlichen Anforderung oder einer anderen Rechtsvorschrift ~~eine Rechtsgrundlage haben~~ im	Gleichlauf mit Formulierungsvorschlag zu Art. 6 Abs. 1c.
a) Unionsrecht oder	
b) Recht des Mitgliedstaats unterliegen, dem der für die Verarbeitung Verantwortliche unterliegt.	
~~Die einzelstaatliche Regelung muss ein im öffentlichen Interesse liegendes Ziel verfolgen oder zum Schutz der Rechte und Freiheiten Dritter erforderlich sein, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem mit der Verarbeitung verfolgten legitimen Zweck stehen.~~	Diese Regelung legt den Verantwortlichen bei der Anwendbarkeit nationaler Vorschriften und Anordnungen die Last der Prüfung auf, ob diese mit dem Verfassungsrecht vereinbar sind, obgleich dies Aufgabe der Verwaltung und der Gesetzgeber ist. Die rechtsanwendende verantwortliche Stelle muss auf auf ein solches rechtskonformes Verhalten regelmäßig vertrauen dürfen. Die Vorschrift ist ersatzlos zu streichen oder so zu fomulieren, dass nur die EU-Mitgliedstaaten selbst in die Verwantwortung genommen werden.
4. Ist der Zweck der Weiterverarbeitung	Satz 1: Eine Änderung des Verarbeitungs-

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~~ f genannten Gründe zutreffen. ~~Dies gilt insbesondere bei Änderungen von Geschäfts- und allgemeinen Vertragsbedingungen.~~	zwecks sollte grundsätzlich im Rahmen einer Interessenabwägung nach Artikel 7 Absatz 1 f VO-E möglich bleiben. Wir gehen insoweit von einem Redaktionsversehen aus. Satz 2: Der zweite Satz sollte gestrichen werden, da aus der mit dem Betroffenen vereinbarten Vertragsänderung bereits eine Veränderung des Verarbeitungszwecks folgt und diese damit vom Betroffenen ohnehin legitimiert ist.
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.~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen, sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
Artikel 7 ***Einwilligung***	
1. Der für die Verarbeitung Verantwortliche trägt die Beweislast dafür, dass die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für eindeutig festgelegte Zwecke erteilt hat.	
2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, die noch einen anderen Sachverhalt betrifft, muss das Erfordernis der Einwilligung äußerlich erkennbar von dem anderen Sachverhalt getrennt werden.	
3. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.	
4. ~~Die Einwilligung bietet keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der Position der betroffenen Person~~	Gemäß Artikel 7 Absatz 4 VO-E soll eine Einwilligung dann keine ausreichende Grundlage für die Datenverarbeitung sein,

~~und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht.~~	wenn zwischen der betroffenen Person und des für die Verarbeitung Verantwortlichen ein „erhebliches Ungleichgewicht“ besteht. Es besteht das Risiko, dass im Kunde-Bank-Verhältnis generell ein Ungleichgewicht unterstellt wird und deshalb die Einwilligungslösung für Banken verboten würde. Dies führt zu einer übermäßigen Bevormundung und dem Abbau von Gestaltungsrechten des Betroffenen. Soweit das Prinzip der Freiwilligkeit der Einwilligung gewahrt ist, muss diese weiter zulässig bleiben. Überdies ist es Prinzip des Bankgeheimnisses als Jahrhunderte altem Handelsbrauch, dass der Kunde die Bank hiervon durch ausdrückliche Einwilligung in eine Datenweitergabe befreien kann. Folglich sollte Absatz 4 gestrichen werden. Die Einwilligung muss regelmäßig einen Datenverarbeitungsvorgang legitimieren können.
Artikel 8 ***Verarbeitung personenbezogener Daten eines Kindes***	
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.	
2. Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags mit einem Kind, unberührt.	

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 nachprüfbaren Einwilligung gemäß Absatz 1 näher zu regeln. Dabei zieht die Kommission spezifische Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen in Betracht.~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
4. ~~Die Kommission kann Standardvorlagen für spezielle Arten der Erlangung einer nachprüfbaren Einwilligung gemäß Absatz 1 festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen~~.	Die Entwicklung von Vordrucken und Formularen sollte den Verwendern und nicht der Kommission obliegen. Eine gesetzliche Standardisierung würde zu einer erheblichen Bürokratisierung führen.
Artikel 9 ***Verarbeitung besonderer Kategorien von personenbezogenen Daten***	
1. Die Verarbeitung personenbezogener Daten, aus denen die Rasse oder ethnische Herkunft, politische Überzeugungen, die Religions- oder Glaubenszugehörigkeit oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, sowie von genetischen Daten, Daten über die Gesundheit oder das Sexualleben ~~oder Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln~~ ist untersagt.	In den Erwägungsgründen sollte nach dem Vorbild der EU-Gleichbehandlungsrichtlinien klargestellt werden, dass die „Staatsangehörigkeit“ nicht von den Merkmalen „Rasse oder ethnische Herkunft“ umfasst wird. Bislang sind in Artikel 8 der Datenschutzrichtlinie Daten über Strafurteile keine sensible Daten: *„Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervo~~r~~rgehen, sowie von Daten über Gesundheit oder Sexualleben.“* Die Aufnahme dieser Datenart wäre für die – auch bankaufsichtsrechtlich erforderlichen – Sicherheitsüberprüfungen ein problematisches Verarbeitungshindernis. Deshalb sollte diese Datenkategorie aus dem Katalog der sensiblen Daten gestrichen werden. Es sollte besser bei der autonomen Sonderregelung in Artikel 8 Absatz 5 der Richlinie bleiben und dort die besonderen Aspekte

	heutiger Complianceanforderungen berücksichtigt werden. Artikel 8 Absatz 5 der Datenschutzrichtlinie lautet: *„Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen, wobei ein Mitgliedstaat jedoch Ausnahmen aufgrund innerstaatlicher Rechtsvorschriften, die geeignete besondere Garantien vorsehen, festlegen kann. Ein vollständiges Register der strafrechtlichen Verurteilungen darf allerdings nur unter behördlicher Aufsicht geführt werden.* *Die Mitgliedstaaten können vorsehen, daß Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.“*
2. Absatz 1 gilt nicht in folgenden Fällen:	
a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten vorbehaltlich der in den Artikeln 7 und 8 genannten Bedingungen eingewilligt, es sei denn, nach den Rechtsvorschriften der Union oder eines Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden, oder	
b) die Verarbeitung ist erforderlich, damit der für die Verarbeitung Verantwortliche seine ihm aus dem Arbeitsrecht erwachsenden Rechte ausüben und seinen arbeitsrechtlichen Pflichten nachkommen kann, soweit dies nach den Vorschriften der Union oder dem Recht der Mitgliedstaaten, das angemessene Garantien vorsehen muss, zulässig ist, oder	
c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person erforderlich und die betroffene Person ist aus physischen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben, oder	

d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Erwerbszweck im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen nach außen weitergegeben werden, oder	
e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder	
f) die Verarbeitung ist zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen erforderlich oder	
g) die Verarbeitung ist erforderlich, um auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene Garantien zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht, eine im öffentlichen Interesse liegende Aufgabe oder eine zivilrechtliche Pflicht gegenüber dem Betroffenen zu erfüllen, oder	Wir verstehen die Vorschrift so, dass damit alle gesetzlichen Verarbeitungspflichten einer Bank mit öffentlichen Bezug (z.B. im Rahmen des Steuerrechts, der Geldwäsche-bekämpfung, des Sozialrechts) abgebildet werden. Der verantwortlichen Stelle kann es allerdings nicht obliegen, die Qualität der maßgeblichen Rechtsvorschrift zu prüfen. Sie muss sich darauf verlassen können, dass der nationale Gesetzgeber die Vorgabe der Verordnung einhält. Nicht abgedeckt wird hingegen die Erfüllung gesetzlicher Pflichten aus dem Zivilrecht. So wird nach dem Zahlungdiensterecht (das auf der EU-Zahlungsdiensterichtlinie beruht) ein Zahlungsdienstleister z.B. verpflichtet, die Daten, die vom Kunden im Verwendungs-zweck einer Überweisung angegeben werden, an den Zahlungsempfänger weiterzuleiten. Dieser kann ggf. auch besondere Kategorien von personenbezogenen Daten, wie z.B. Gewerkschaftsbeitrag, enthalten. Auch für

	diese Sachverhalte sind Ausnahmetatbestände vorzusehen.
h) die Verarbeitung betrifft Gesundheitsdaten und ist vorbehaltlich der Bedingungen und Garantien des Artikels 81 für Gesundheitszwecke erforderlich oder	
i) die Verarbeitung ist vorbehaltlich der Bedingungen und Garantien des Artikels 83 für historische oder statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung erforderlich oder	
j) ~~die Verarbeitung von Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln erfolgt entweder unter behördlicher Aufsicht oder aufgrund einer gesetzlichen oder rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Erfüllung einer Aufgabe, der ein wichtiges öffentliches Interesse zugrunde liegt, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene Garantien vorsehen muss, zulässig ist. Ein vollständiges Strafregister darf nur unter behördlicher Aufsicht geführt werden.~~	Siehe bereits die Ausführungen zu Artikel 9 Abs. 1; hier sollte der bisherigen Artikel 8 Absatz 5 der Richtlinie 95/46/EG übernommen werden: *„Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen, wobei ein Mitgliedstaat jedoch Ausnahmen aufgrund innerstaatlicher Rechtsvorschriften, die geeignete besondere Garantien vorsehen, festlegen kann. Ein vollständiges Register der strafrechtlichen Verurteilungen darf allerdings nur unter behördlicher Aufsicht geführt werden.* *Die Mitgliedstaaten können vorsehen, daß Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.“*
3. ~~Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten sowie angemessene Garantien für die Verarbeitung der in Absatz 1 genannten besonderen Kategorien von personenbezogenen Daten und die in Absatz 2 genannten Ausnahmen näher zu regeln~~.	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.

Artikel 10 ***Verarbeitung, ohne dass die betroffene Person bestimmt werden kann***	
Kann der für die Verarbeitung Verantwortliche anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen, ist er nicht verpflichtet, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen.	

KAPITEL III
RECHTE DER BETROFFENEN PERSON

ABSCHNITT 1
TRANSPARENZ UND MODALITÄTEN

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 11 ***Transparente Information und Kommunikation***	
1. ~~Der für die Verarbeitung Verantwortliche verfolgt in Bezug auf die Verarbeitung personenbezogener Daten und die Ausübung der den betroffenen Personen zustehenden Rechte eine nachvollziehbare und für jedermann leicht zugängliche Strategie~~. Der für die Verarbeitung Verantwortliche soll transparente und leicht zugängliche Informationen über die allgemeinen Grundsätze bezüglich der Verarbeitung personenbezogener Daten und der Ausübung der Rechte von Betroffenen vorhalten.	Die deutsche Fassung weicht erheblich von der englischen Fassung ab, diese lautet: *"The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights."* Die englische Fassung ist verständlicher und damit für den Rechtsanwender besser umsetzbar als die deutsche Fassung. Gleichwohl darf nicht verkannt werden, dass gerade für kleine und mittlere Unternehmen, die Aufstellung von Datenschutzgrundsätzen eine neue bürokratische Belastung darstellen kann.
2. ~~Der für die Verarbeitung Verantwortliche stellt der betroffenen Person alle~~ Die Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten für den Betroffenen hat in verständlicher Form unter Verwendung einer klaren, ~~—~~und einfachen ~~und adressatengerechten~~ Sprache	Die Vorgabe „adressatengerecht" führt zu dem bereits oben zu Artikel 5 a) VO-E beschriebenen Problem, dass auf die individuelle Einsichtsfähigkeit abgestellt werden müsste. Maßgeblich muss auch hier der typische „Durchschnitts-Betroffe" als Empfänger der Mitteilung sein. Andernfalls

zu erfolgenr ~~Verfügung~~, besonders dann, wenn die Information an ein Kind gerichtet ist.	ist die Vorschrift nicht umsetzbar, denn sie würde in der Konsequenz vom Verantwortlichen eine Vielzahl unterschiedlicher Informationsangebote verlangen. Es reicht, dass das Transparenzgebot gewahrt wird.
Artikel 12 ***Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann***	
1. Der für die Verarbeitung Verantwortliche legt fest, mittels welcher Verfahren er die Informationen gemäß Artikel 14 bereitstellt und den betroffenen Personen die Ausübung der ihnen gemäß Artikel 13 sowie den Artikeln 15 bis 19 zustehenden Rechte ermöglicht. Er trifft insbesondere Vorkehrungen, um die Beantragung der in Artikel 13 sowie in den Artikeln 15 bis 19 genannten Maßnahmen zu ermöglichen~~erleichtern~~. Im Falle, dass der für die Verarbeitung Verantwortliche gegenüber dem Betroffenen ausschließlich auf elektronischem Wege kommuniziert, ~~der automatischen Verarbeitung personenbezogener Daten~~ sorgt der für die Verarbeitung Verantwortliche dafür, dass die Maßnahme elektronisch beantragt werden kann.	Zu Satz 1: Der erste Satz normiert Selbstverständliches und ist daher zu streichen. Jede gesetzliche Anforderung muss vollzogen werden. Zu Satz 2: Die Formulierung „erleichtern“ ist zu unbestimmt und bereitet nur Raum für nicht zielführende Diskussionen darüber, welches Maß an Erleichterung dem Betroffenen zu verschaffen ist. Besser ist darauf abzustellen, dass die verantwortliche Stelle in angemessenem Rahmen die Wahrnehmung der Rechte ermöglicht. Zu Satz 3: Aus dem Umstand, dass Daten automatisiert verarbeitet werden, folgt nicht zwingend, dass das Unternehmen auch über die technischen Mittel verfügt, dem Betroffenen auch eine elektronische Beantragung einer Maßnahme zu ermöglichen. Insofern ist mit dieser Forderung insbesondere für kleinere und mittlere Unternehmen ein erheblicher Mehraufwand verbunden. Satz 3 hat nur in den Fällen eine Berechtigung, in denen der Verantwortliche der Verarbeitung mit dem betroffenen ausschließlich auf elektronischem Wege kommuniziert.
2. Der für die Verarbeitung Verantwortliche kommt seiner Informationspflicht gegenüber der betroffenen Person umgehend nach und teilt ihr spätestens innerhalb eines Monats nach Eingang eines Antrags mit, ob eine Maßnahme nach Artikel 13 oder den	Zu Satz 2: Eine Möglichkeit zur Verlängerung der Reaktionsfrist ist neben massenhaften Anfragen auch bei komplexen Sachverhalten erforderlich (zur Angemessenheit der Frist siehe auch die Ausführungen zu Satz 4 unten).

Artikeln 15 bis 19 ergriffen wurde, und erteilt die erbetene Auskunft. Diese Frist kann um einen Monat verlängert werden, wenn mehrere betroffene Personen von ihren Rechten Gebrauch machen und der für die Verarbeitung Verantwortliche darlegen kann, dass die Bearbeitung innerhalb der Frist nach Satz 1 nicht mit verhältnismäßigem Aufwand möglich ist, oder die~~ihre~~ Zusammenarbeit der Betroffenen bis zu einem vertretbaren Maß notwendig ist, um einen unnötigen und unverhältnismäßig hohen Aufwand seitens des für die Verarbeitung Verantwortlichen zu vermeiden. Die Unterrichtung hat ~~schriftlich~~ in Textform zu erfolgen. ~~Stellt die betroffene Person den Antrag in elektronischer Form, ist sie auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.~~	Zu Satz 3: Auskünfte sollen nach der englischen Fassung „in writing“ erteilt werden. Die Schriftform geht darüber hinaus, so dass das Tatbestandsmerkmal „in Textform“ („on durable medium“) vorzugswürdig ist. Zu Satz 4: Es muss dem Verantwortlichen obliegen, zu entscheiden, in welcher Form er dem Betroffenen Auskunft erteilt. Eine elektronische Auskunftserteilung kann auch im Interesse des Betroffenen nur erfolgen, wenn der Auskunftssuchende sich eindeutig identifiziert hat (z.B. mittels elektronischem Identitätsnachweis des Personalausweises) und auch selbst Vorkehrungen für eine technisch sichere Übertragung getroffen hat (z.B. verschlüsselte Datenübermittlung). Die Antwortfrist von einem Monat sollte wie bereits vorgesehen Ausnahmen zulassen, beispielsweise bei Massenauskunftsersuchen, die eine längere Bearbeitungszeit erfordern können. Dabei sollte eine „geeignete“ Fristverlängerung eingeräumt werden..
3. Weigert sich der für die Verarbeitung Verantwortliche, auf Antrag der betroffenen Person tätig zu werden, unterrichtet er die betroffene Person über die Gründe für die Weigerung und über die Möglichkeit, bei der Aufsichtsbehörde Beschwerde einzulegen oder den Rechtsweg zu beschreiten.	
4. Die Unterrichtung und die auf Antrag ergriffenen Maßnahmen gemäß Absatz 1 sind kostenlos. Bei offenkundig unverhältnismäßigen Anträgen und besonders im Fall ihrer Häufung kann der für die Verarbeitung Verantwortliche ein Entgelt für die Unterrichtung oder die Durchführung der beantragten Maßnahme verlangen oder die beantragte Maßnahme unterlassen. In diesem Fall trägt der für die Verarbeitung Verantwortliche die Beweislast für den offenkundig unverhältnismäßigen Charakter des Antrags.	

5. ~~Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Voraussetzungen für offenkundig unverhältnismäßige Anträge sowie die in Absatz 4 genannten Entgelte näher zu regeln.~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
6. ~~Die Kommission kann Standardvorlagen und Standardverfahren für die Mitteilungen gemäß Absatz 2, auch für solche in elektronischer Form, festlegen. Dabei ergreift die Kommission geeignete Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.~~	Die Entwicklung von Vordrucken und Formularen sollte den Verwendern obliegen. Eine Standardisierung würde zu einer erheblichen Bürokratisierung führen.
Artikel 13 ***Rechte gegenüber Empfängern***	
Sofern ein berechtigtes Interesse des Betroffenen besteht, teilt 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 oder die weitergegebenen Daten wurden vom Betroffenen bereits fehlerhaft überlassen~~.~~.	Die Regelung konterkariert den datenschutzrechtlichen Grundsatz der Datenvermeidung und Datensparsamkeit, denn sie bedingt einen permanenten und zeitlich unbegrenzten Datenfluss zwischen Verantwortlichem und Empfänger. So wären Zahlungsdienstleister verpflichtet, jährlich mehrere Milliarden Datensätze zu speichern und zu monitoren, um fehlerhafte Daten an Empfängerbanken weiterleiten zu können. Die Nachmeldepflicht sollte daher auf die Fälle beschränkt werden, in denen der Betroffene ein berechtigtes Interesse hieran hat (z.B. Meldung an eine Kreditauskunftei). Er hat beispielsweise dann kein Interesse mehr an der Korrektur, wenn die Datenübermittlung auf einen Informationsstand zu einem bestimmten Zeitpunkt bezogen ist und der Datenempfänger selber nicht mehr davon ausgeht, dass es sich um aktuelle Daten handelt.

ABSCHNITT 2
INFORMATIONSPFLICHT UND AUSKUNFTSRECHT

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 14 ***Information der betroffenen Person***	
1. Einer Person, von der personenbezogene Daten erhoben werden, stellt~~teilt~~ der für die Verarbeitung Verantwortliche zumindest folgende Informationen ~~Folgendes~~ zur Verfügung~~mit~~:	1. Grundsätzliches Transparenz für den von der Datenverarbeitung Betroffenen ist sicherlich eine Grundvoraussetzung dafür, dass der Betroffene seine Rechte wahrnehmen kann. Doch schon im Verbraucherschutzrecht ist die Tendenz zu verzeichnen, dass durch gesetzliche Vorgaben die Menge der dem Bankkunden zu erteilenden Informationen ein Ausmaß erreicht hat, bei dem man sich fragt, ob der Bankkunde dies möchte und verstehen kann. Insofern ist der mit Artikel 14 verfolgte Ansatz einer „umfassenden" Informationspflicht fragwürdig, wenn er letztlich in einer für den Kunden nicht mehr verarbeitbaren „Informationsflut" mündet. Zielführender ist ein zweistufiger Ansatz: Auf der ersten Stufe muss es ausreichen, dem Kunden allgemeine Informationen erteilen zu können. Erst bei dessen konkreter Nachfrage sollte in zweiter Stufe die Informationen bedarfsgerecht konkretisiert werden. Das bedeutet, dass gesetzliche Informationspflichten sich auf das unbedingt Erforderliche beschränken sollten und weitergehende Informationen erst auf Nachfrage zu erteilen sind (Beispiel: Der Kunde ist über das Vorliegen einer automatisierten Einzelentscheidung von der Bank zu informieren. Erst auf Nachfrage muss die Bank weitere Informationen dem Kunden geben). 2. Berücksichtigung des Umweltschutzes bei Art und Weise der Informationserteilung Es sollte auch ausreichen können, dem Betroffenen die gebotenen Informationen beispielsweise im Internet oder in der

	Geschäftsstelle zur Abholung zur Verfügung zu stellen. Damit wird verhindert, dass den Betroffenen in jedem Fall flächendeckend ein umfangreiches papierhaftes Informationspaket auszuhändigen oder zu übermitteln ist und die große Mehrheit dies mangels Interesse sogleich wegschmeißt. Auch unter Umweltschutzgesichtspunkten ist eine solche Verschwendung von Papier nicht sachgerecht.
a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Repräsentant~~Vertreters~~ und auf Nachfrage die für Datenschutz zuständige Stelle ~~und des Datenschutzbeauftragten~~,	Die Nennung des Namens und die Kontaktdaten des für die Verarbeitung Verantwortlichen ist ausreichend, damit der Betroffene den für die Verarbeitung Verantwortlichen eindeutig identifizieren und ggf. seine Rechte gegenüber diesem durchsetzen kann. Dagegen sollte die Nennung des Datenschutzbeauftragten nicht obligatorisch sein, weil dieser gegenüber dem Betroffenen keine rechtliche Vertretungsfunktion für die verantwortliche Stelle innehat. Es sollte ausreichen, auf Nachfrage eine Kontaktstelle für Datenschutzfragen zu benennen. Zudem Folgeänderung zu Artikel 4 Abs. 14.
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~~ auf Nachfrage die von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen, wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht,	Die Regelung sollte entsprechend Art. 10 Abs. b der Richtlinie 95/46/EG gefasst werden, um zusätzlichen bürokratischen Aufwand zu vermeiden. Die Verpflichtung zur Mitteilung der Geschäfts- und allgemeinen Vertragsbedingungen greift in zivilrechtlichen Mechanismen zur Einbeziehung von Allgemeinen Geschäftsbedingungen ein und ist folglich nicht im Datenschutzrecht zu regeln. Datenschutzrechtlich ist die Kenntnis des Betroffenen über die Verarbeitungszwecke ausreichend. Eine Darstellung der von der verantwortlichen Stelle verfolgten berechtigten Interessen ist ein unötiger Formalismus und bringt keinen Informationsgewinn. Nur in den Fällen, in denen der Betroffene hierzu ausdrücklich nachfragt, sollte diese

	Information bedarfsgerecht erfolgen.
c) die Dauer, für die die personenbezogenen Daten gespeichert werden,	Zu Beginn der Geschäftsbeziehung ist es nicht möglich, den Betroffenen über die Dauer der Speicherung seiner Daten zu informieren, da nicht absehbar ist, wie lange die Geschäftsbeziehung dauert. Dies gilt insbesondere für im Bereich der Kreditwirtschaft üblichen Dauerschuldverhältnisse. Deshalb muss eine generische Beschreibung ausreichen.
d) ~~das Bestehen eines Rechts auf Auskunft sowie Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchsrechts gegen die Verarbeitung dieser Daten,~~	Diese Information ist redundant, da diese bereits von Artikel 11 Absatz 1 VO-E abgedeckt ist. Zudem kann es nicht alleine die Aufgabe der verantwortlichen Stelle sein, den Betroffenen über seine gesetzlichen Pflichte aufzuklären.
e) ~~das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,~~	Siehe d).
f) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,	
g) ~~gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das dort geltende Datenschutzniveau unter Bezugnahme auf einen Angemessenheitsbeschluss der Kommission,~~	Die Informationen können im Bereich der Abwicklung des internationalen Zahlungsverkehrs sowie des internationalen Wertpapiergeschäfts nicht erfüllt werden.
h) sonstige Informationen, die unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.	
2. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, teilt der für die Verarbeitung Verantwortliche dieser Person neben den in Absatz 1 zur Verfügung gestelltengenannten Informationen außerdem mit, ob die Bereitstellung der Daten	Folgeänderung zu Absatz 1 dieser Vorschrift.

obligatorisch oder fakultativ ist und welche mögliche Folgen die Verweigerung der Daten hätte.	
3. Werden die personenbezogenen Daten nicht bei der betroffenen Person erhoben, stellt~~teilt~~ der für die Verarbeitung Verantwortliche dieser Person neben den in Absatz 1 genannten Informationen außerdem Informationen über die Herkunft der personenbezogenen Daten zur Verfügung~~mit~~, außer die Daten stammen aus einer öffentlich zugänglichen Quelle oder ein Gesetz schreibt die Datenerhebung vor.	Die Vorschrift entspricht weitgehend Art. 11 der Richtlinie 95/46/EG. Bei öffentlich zugänglichen Daten bedarf es keiner Information des Betroffenen. Eine Informationspflicht sollte nicht bestehen, wenn die Datenerhebung bei Dritten aufgrund einer gesetzlichen Verpflichtung oder Erlaubnis erfolgt. Auch sollte die bisherigen Ausnahmetatbestände aus § 33 Absatz 2 BDSG Berücksichtigung finden.
4. Der für die Verarbeitung Verantwortliche ~~erteilt~~ stellt die Informationen gemäß den Absätzen 1, 2 und 3 zur Verfügung	Vgl. Anmerkungen zu Absatz 1. Damit würde auch die Bereitstellung der Informationen in der Geschäftsstelle oder auf der Internetseite der Bank ausreichen.
a) zum Zeitpunkt der Erhebung der personenbezogenen Daten bei der betroffenen Person oder	
b) falls die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, zum Zeitpunkt ihrer Erfassung oder innerhalb einer angemessenen Frist nach ihrer Erhebung, die den besonderen Umständen, unter denen die Daten erhoben oder auf sonstige Weise verarbeitet wurden, Rechnung trägt, oder, falls die Weitergabe an einen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Weitergabe.	
5. Die Absätze 1 bis 4 finden in folgenden Fällen keine Anwendung:	
a) Die betroffene Person hat bereits auf andere Weise Kenntnis ~~verfügt bereits~~ über die Informationen gemäß den Absätzen 1, 2 und 3 erlangt, oder	Die praxisgerechte Formulierung in § 4 Abs. 3 Satz 1 BDSG sollte übernommen werden, um unnötige Formalismen bei bereits informierten Betroffenen zu vermeiden.
b) die Daten werden nicht bei der betroffenen Person erhoben und die Unterrichtung erweist sich als unmöglich oder ist mit einem unverhältnismäßig hohen	

Aufwand verbunden oder	
c) die Daten werden nicht bei der betroffenen Person erhoben und die Erfassung oder Weitergabe erfolgt ~~ist~~ zur Erfüllung einer gesetzlichen Pflicht oder im Rahmen einer gesetzlichen Erlaubnis, einer aufsichtsrechtlichen Anordnung oder einer sonstigen Rechtsvorschrift, ~~oder ausdrücklich per Gesetz geregelt~~	Siehe Kommentierung zu Art. 6 Abs. 1 c.
d) die Daten werden nicht bei der betroffenen Person erhoben und die Bereitstellung der Informationen greift nach Maßgabe des Unionsrechts oder des Rechts der Mitgliedstaaten gemäß Artikel 21 in die Rechte, ~~und~~ Freiheiten und sonstigen berechtigten Interessen des für die Verarbeitung Verantwortlichen oder anderer Personen ein.	Die Regelung ist ein Korrektiv für den Fall, dass unterschiedliche Grundrechtspositionen in Einklang miteinander gebracht werden müssen. Dabei müssen auch die Rechte bzw. die berechtigten Interessen der verantwortlichen Stelle hinreichend Beachtung finden.
6. Im Fall des Absatzes 5 Buchstabe b ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person.	
7. ~~Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten zu den Kategorien von Empfängern gemäß Absatz 1 Buchstabe f, den Anforderungen an Informationen gemäß Absatz 1 Buchstabe g, den Kriterien für die Erteilung sonstiger Informationen im Sinne von Absatz 1 Buchstabe h für verschiedene Bereiche und Verarbeitungssituationen und zu den Bedingungen und geeigneten Garantien im Hinblick auf die Ausnahmen gemäß Absatz 5 Buchstabe b zu regeln. Dabei ergreift die Kommission geeignete Maßnahmen für Kleinst und Kleinstunternehmen sowie mittlere Unternehmen~~.	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen, sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
8. ~~Die Kommission kann Standardvorlagen für die Bereitstellung der Informationen gemäß den Absätzen 1 bis 3 festlegen, wobei sie gegebenenfalls die Besonderheiten und Bedürfnisse der verschie-~~	Die Entwicklung von Vordrucken und Formularen sollte den Verwendern obliegen. Eine Standardisierung würde zu einer erheblichen Bürokratisierung führen.

~~denen Sektoren und Verarbeitungssituationen berücksichtigt. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen~~.	
Artikel 15 ***Auskunftsrecht der betroffenen Person***	
1. Die betroffene Person kann ~~hat~~ zur Wahrnehmung ihrer Rechte nach dieser Verordnung ~~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, informiert ~~teilt~~ der für die Verarbeitung Verantwortliche über Folgendes, soweit dem Betroffenen die Informationen nicht bereits erteilt wurden ~~mit~~:	Zu Satz 1: Es muss vermieden werden, dass der Auskunftsanspruch von Dritten instrumentalisiert wird (z.B. Missbrauch der „Selbstauskunft“ des Mieters auf Veranlassung des Vermieters zur Bonitätsprüfung). Zudem muss klargestellt werden, dass der gewährte Anspruch nur zu Zwecken von datenschutzrechtlichen Rechten geltend gemacht werden darf. Er darf nicht zu einem allgemeinen Ausforschungsanspruch gegen den Verantwortlichen im Zivilprozess führen oder zur Verwendung in Strafprozessen zweckentfremdet werden. Zu Satz 2: Redaktionelle Anpassung. Sind dem Betroffenen bereits die Informationen erteilt worden (beispielsweise mit den Vertragsunterlagen oder im Wege der Erfüllung von Rechnungslegungspflichten), ist der kostenlose Auskunftsanspruch verbraucht.
a) die Verarbeitungszwecke,	
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,	
d) die Dauer, für die die personenbezogenen Daten gespeichert werden,	

e) ~~das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchrechts gegen die Verarbeitung dieser Daten,~~	Über das Bestehen gesetzlicher Ansprüche sollte im Rahmen einer Vertragsbeziehung nicht noch zusätzlich informiert werden müssen.
f) ~~das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,~~	Siehe Anmerkungen zu lit. e) dieser Vorschrift.
g) diejenigen personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten,	In den Erwägungsgründen sollte Eingang finden, dass das Auskunftsrecht bislang nur eine Beschreibung der Dateninhalte und nicht einen „Original-Auszug“ aus der Datenbank oder die Wiedergabe des Original-Datensatzes umfasst. Für die Wahrnehmung der Betroffenenrechte reicht eine Darlegung der Dateninhalte in der Regel aus. Zudem erlaubt es eine dem Transparenzgebot entsprechende Aufbereitung der beim Verantwortlichen verarbeiteten Daten.
h) die Tragweite der Verarbeitung und die mit ihr angestrebten Auswirkungen, zumindest im Fall der Maßnahmen gemäß Artikel 20.	Artikel 20 könnte auch auf Scoring-Verfahren Anwendung finden. Zu Wahrung von Geschäftsgeheimnissen ist es notwendig, dass das Auskunftsrecht sich nicht auch auf die Art und Weise der Funktion von Scoring-Verfahren bezieht. Ansonsten könnten Wettbewerber die Scorefunktion nachvollziehen. Der im Erwägungsgrund 51 zugestandene Schutz des Geschäftsgeheimnisses, des geistigen Eigentums und des Urheberrechts sollte unmittelbar in Artikel 14 der VO beschrieben werden.
2. ~~Die betroffene Person hat Anspruch darauf, dass ihr von dem für die Verarbeitung Verantwortlichen mitgeteilt wird, welche personenbezogenen Daten verarbeitet werden. Stellt die betroffene Person den Antrag in elektronischer Form, ist sie auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.~~	Zu Satz 1: Satz 1 ist redundant, siehe dazu bereits oben Abs. 1 g) dieser Vorschrift. Zu Satz 2: Es muss grundsätzlich im Ermessen des Verantwortlichen liegen, über die Form der Auskunft zu entscheiden. Ggf. sprechen Sicherheitsaspekte gegen eine Beauskunftung in elektronischer Form. Dies betrifft die ggf. nicht mögliche Identifizierung des Anfragenden sowie die

	Sicherheit der Übertragungswege.
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~~. Eine Auskunftspflicht besteht nicht, wenn a. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Beauskunftung einen unverhältnismäßigen Aufwand erfordern würde, b. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen, c. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde, d. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden würde, e. die Daten für eigene Zwecke gespeichert sind und aa) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder bb) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein. Stattdessen sollten analog zu § 33 Abs. 2 BDSG in der Verordnung selber die Schranken des Auskunftsrechts normiert werden. Diese ergeben sich insbesondere aus Geschäftsgeheimnissen und Eigentumsrechten des Verantwortlichen, wie auch in Erwägungsgrund 51 VO-E zutreffend beschrieben. Darüber hinaus sind für die Kreditwirtschaft auch Beschränkungen aufgrund gesetzlicher Schweigepflichten, wie z.B. § 12 Geldwäschegesetz, relevant.
4. ~~Die Kommission kann Standardvorlagen und -verfahren für~~	Die Entwicklung von Vordrucken und Formularen sollte den Verwendern obliegen.

~~Auskunftsgesuche und die Erteilung der Auskünfte gemäß Absatz 1 festlegen, darunter auch für die Überprüfung der Identität der betroffenen Person und die Mitteilung der personenbezogenen Daten an die betroffene Person, wobei sie gegebenenfalls die Besonderheiten und Bedürfnisse der verschiedenen Sektoren und Verarbeitungssituationen berücksichtigt. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen~~.	Eine Standardisierung würde zu einer erheblichen Bürokratisierung führen.

ABSCHNITT 3
BERICHTIGUNG UND LÖSCHUNG

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 16 ***Recht auf Berichtigung***	
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, soweit dies für den Verarbeitungszweck erforderlich ist.	In der Regelung werden Fallkonstellationen nicht bedacht, in denen unter den Parteien Streit über die Richtigkeit der erhobenen Daten besteht. Ein Korrekturanspruch kann insoweit nur dann durchsetzbar sein, wenn über die Unrichtigkeit Klarheit herbeigeführt worden ist. Das reine Korrekturverlangen des Betroffenen darf hier noch nicht maßgeblich sein. Im Übrigen sollte ein Ergänzungsanspruch – auch in Form des Korrigendums – nur dann bestehen, wenn dies für den Verarbeitungszweck erforderlich ist.
Artikel 17 ***Recht auf Vergessenwerden und auf Löschung***	
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:	
a) Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.	Wir gehen davon aus, dass die „Verarbeitung auf sonstige Weise“ auch zulässige Zweckänderungen umfasst. Bei Beendigung eines Vertrages kann es noch nachvertragliche Pflichte geben, die einer Datenlöschung bzw. –sperrung entgegenstehen können.
b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a stützte, oder die Speicherfrist, für die die Einwilligung gegeben wurde, ist abgelaufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung der Daten.	
c) Die betroffene Person legt gemäß Artikel 19 Widerspruch gegen die Verarbeitung ein.	
d) ~~Die Verarbeitung der Daten ist aus anderen Gründen nicht mit der Verordnung vereinbar.~~	Eine generelle Auffangsbestimmung für einen Löschungsanspruch ist unpraktikabel. Die Verordnung muss die Fälle genau bestimmen, in den der Betroffene einen Löschungsanspruch hat.
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.	
3. Der für die Verarbeitung Verantwortliche sorgt unter den Voraussetzungen des Absatzes 1 für eine umgehende Löschung der personenbezogenen Daten, soweit deren Speicherung nicht erforderlich ist	Das Verhältnis zwischen Absatz 3 und Absatz 1 ist klarzustellen. Ansonsten könnte der Eindruck entstehen, es handele sich um zwei selbständige Vorgaben zur Löschung von Daten.
(a) zur Ausübung des Rechts auf freie Meinungsäußerung gemäß Artikel 80;	
(b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 81;	
(c) für historische und statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung gemäß Artikel 83;	
(d) zur Erfüllung einer gesetzlichen oder aufsichtsrechtlichen Pflicht zur Vorhaltung der personenbezogenen Daten, der der für die Verarbeitung Verantwortliche nach dem Unionsrecht oder dem Recht eines Mitgliedstaats unterliegt~~, wobei das mitgliedstaatliche Recht ein im öffentlichen Interesse liegendes Ziel verfolgen, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen muss;~~	Die Speicherung von Daten kann auch zur Erfüllung von bankaufsichtsrechtlichen Vorgaben erforderlich sein. Die qualitative Anforderung an die gesetzliche Vorschrift sollte sich alleine an den Gesetzgeber richten. Dem Verantwortlichen kann nicht eine Pflicht auferlegt werden, seinerseits eine Rechtmäßigkeit der Norm vorzunehmen.
(e) in den in Absatz 4 genannten Fällen.	
4. Anstatt die personenbezogenen Daten	Statt der Formulierung „beschränken“ sollte

zu löschen, kann der für die Verarbeitung Verantwortliche diese Daten sperren ~~deren Verarbeitung beschränken~~, wenn	das bisherige Sperrkonzept fortgeführt werden.
a) ihre Richtigkeit von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem für die Verarbeitung Verantwortlichen ermöglicht, die Richtigkeit zu überprüfen;	
b) der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Erfüllung seiner Aufgabe nicht länger benötigt, sie aber für Beweiszwecke oder zur Erfüllung gesetzlicher Aufbwahrungsvorschriften weiter aufbewahrt werden müssen;	Gesetzliche Aufbewahrungspflichten müssen berücksichtigt werden.
c) die Verarbeitung unrechtmäßig ist, die betroffene Person aber Einspruch gegen ihre Löschung erhebt und stattdessen deren eingeschränkte Nutzung fordert;	Reflex zu Art. 35 Absatz 2?
d) die betroffene Person gemäß Artikel 18 Absatz 2 die Übertragung der personenbezogenen Daten auf ein anderes automatisiertes Verarbeitungssystem fordert.	
e) eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.	Der Sperrgrund in § 35 Absatz 3 Nr. 3 BDSG sollte übernommen werden, um in der Praxis auch Sachverhalte berücksichtigen zu können, in denen eine Löschung aus technischen Gründen (z.B. WORM-Technologie, siehe GDPdU sowie die Regelungen zu Basel II) nicht möglich ist.
5. Die in Absatz 4 genannten personenbezogenen Daten dürfen mit Ausnahme ihrer Speicherung nur verarbeitet werden, wenn sie für Beweiszwecke und zur Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich sind, wenn die betroffene Person ihre Einwilligung gegeben hat oder die Rechte einer anderen natürlichen oder juristischen Person geschützt werden müssen oder wenn dies im öffentlichen Interesse liegt.	Klarstellung, dass auch die Erfüllung von gesetzliche Aufbewahrungspflichten bei der Sperre zu berücksichtigen ist.
6. Unterliegt die Verarbeitung	Unklar ist, in welchen Fällen eine Sperrung

personenbezogener Daten gemäß Absatz 4 a), c) oder d) einer Beschränkung, teilt der für die Verarbeitung Verantwortliche der betroffenen Person im Voraus mit, dass die Sperrung ~~Beschränkung~~ aufgehoben werden soll.	rückgängig gemacht werden kann.
7. Der für die Verarbeitung Verantwortliche trifft Vorkehrungen, um sicherzustellen, dass die Fristen für die Löschung personenbezogener Daten und/oder die regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung eingehalten werden.	
8. Wird eine Löschung vorgenommen, darf der für die Verarbeitung Verantwortliche die personenbezogenen Daten vorher nicht auf sonstige Weise verarbeiten, außer sie sind anonymisiert.	Eine Weiternutzung von Daten in anonymisierter Form sollte möglich bleiben.
~~9. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten festzulegen in Bezug auf~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
~~a) die Kriterien und Anforderungen im Hinblick auf die Anwendung von Absatz 1 für bestimmte Bereiche und spezielle Verarbeitungssituationen,~~	
~~b) die Bedingungen für die Löschung gemäß Absatz 2 von Internet-Links, Kopien oder Replikationen von personenbezogenen Daten aus öffentlich zugänglichen Kommunikationsdiensten,~~	
~~c) die Kriterien und Bedingungen für die Beschränkung der Verarbeitung personenbezogener Daten gemäß Absatz 4.~~	

Artikel 18 ***Recht auf Datenübertragbarkeit***	
1. Stellt der Betroffene ~~Werden~~ personenbezogene Daten in ein soziales Netzwerk im Internet, das der elektronischen Kommunikation dient, oder in eine Online-Datenbank ein und werden diese Daten 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 oder deren Überführung in ein anderes System zu verlangen.	Ein Recht auf Datenportabiltät ist nur in den Fällen nachvollziehbar und sachgerecht, in denen der Betroffene Daten auf einer Internetplattform (z.B. Online-Speicher, Cloud-Anwendung oder soziales Netzwerk) selber einstellt und er diese Daten wieder in seine Verfügungsgewalt oder auf eine andere Plattform übertragen bekommen möchte. Folglich sollte der Anwendungsbereich auf solche Online-Datenbanken beschränkt werden. Für „konventionelle Datenverarbeitungen“ in unternehmensinternen Datenbanken ist der Anspruch auf Datenportabilität nicht sachgerecht und würde unverhältnismäßig in die Grundrechtsposition und sonstigen berechtigten Interessen von Unternehmen eingreifen: Zum einen ist es nicht der Betroffene, der in unternehmensinterne Datenbanken „seine“ Daten einstellt, sondern die Datenverarbeitung wird verfahrenstechnisch alleine von dem Unternehmen gesteuert. Des Weiteren handelt es sich außerhalb von sozialen Netzwerken, Online-Datenbanken oder „Cloud“-Anwendungen gespeicherten Kundendaten nicht um ausschließlich im „Eigentum“ des Betroffenen stehende Daten („seine Daten“). Vielmehr handelt es sich um eine „elektronische Kundenakte“ in einer Datenbank des Unternehmens, die bei Kreditinstituten zur Erfüllung vertraglicher Pflichten (z.B. Zahlungsdiensterahmenvertrag, Kreditvertrag) und gesetzlicher Pflichten (z.B. Handels- und Steuerrecht, Bankaufsichtsrecht) geführt wird. Überdies wird in Dauerschuldverhältnissen (z.B. Kontovertrag zwischen Kunde und Bank) damit ein Erfahrungswissen des Unternehmens über die Geschäftsbeziehung angesammelt, das für das Unternehmen einen

	besonderen wirtschaftlichen Wert bildet. Diese Informationen sind folglich ein Gut des Unternehmens, über das der Kunde kein alleiniges Verfügungsrecht in Gestalt eines Herausgabeanspruchs haben kann. Seinem Datenschutzinteresse wird bereits durch sein Recht auf Auskunft, Berichtigung und Löschung bzw. Sperrung ausreichend Rechnung getragen. Konsequenz des Rechts auf Datenportabilität wäre auch, dass andere Unternehmen – als Wettbewerber - das Erfahrungswissen beispielsweise einer Bank aus einer langjährigen Geschäftsbeziehung ohne Vergütung dessen Werts einfach „geschenkt" bekämen. Damit würde die aus einer bilateralen Vertragsbeziehung stammende „elektronische Kundenakte" zu einem frei verfügbaren Handelsgut. Dahinter steht somit ein rein wettbewerbspolitischer Ansatz, denn im Ergebnis wird über eine Instrumentalisierung des Betroffenen damit der kostenlose Zugriff von Wettbewerbern auf bei einem Unternehmen vorhandene Kundendaten schrankenlos ermöglicht. Folge wird auch sein, dass die Datenmacht von Internet-Plattformen, insbesondere sozialen Netzwerken, erheblich ausgebaut wird. Denn diese werden den Betroffenen dazu verleiten, mittels seines Portabilitätsanspruchs bislang dezentral vorhandene Datenbestände zur Vervollständigung seines „Lebenszyklus" auf diesen Plattformen zu konzentrieren.
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~~	Siehe Kommentierung zu Art. 18 Abs. 1.

~~personenbezogenen Daten entzogen werden, behindert zu werden.~~	
3. ~~Die Kommission kann das elektronische Format gemäß Absatz 1 festlegen sowie die technischen Standards, Modalitäten und Verfahren für die Überführung der personenbezogenen Daten gemäß Absatz 2. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen~~.	Die Regelung ist entbehrlich. Zudem stellt die Möglichkeit der Festlegung des elektronischen Formats nach Absatz 1 durch die Kommission einen nicht erforderlichen Eingriff in die verfassungsrechtlich geschützte Betriebsorganisationsfreiheit dar.

ABSCHNITT 4

WIDERSPRUCHSRECHT UND PROFILING

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 19 ***Widerspruchsrecht***	
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 <u>im konkreten Fall</u> nicht ~~zwingende~~ <u>berechtigte</u>~~schutzwürdige~~ Gründe für die Verarbeitung nachweisen kann, die die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.	In der Regelung sollte deutlicher werden, dass im Falle des Widerspruchs eine einzelfallbezogene individuelle Interessenabwägung vorzunehmen ist. Der Begriff „zwingend“ ist zu eng. Damit könnte der Erlaubnistatbestand der Interessenabwägung weitgehend ausgehöhlt werden, weil in Privatrechtsverhältnissen kaum „zwingende“ Gründe vorliegen dürften. Zudem trägt die nach dem Vorbild des § 35 Absatz 5 BDSG etwas weiter gefasste Regelung der Situation Rechnung, dass durch einen Widerspruch bestehende Vertragsverhältnisse betroffen sein können und der Datenverarbeiter die Möglichkeit haben sollte, nach erfolgtem Widerspruch das Vertragsverhältnis unter Beachtung vertraglicher und gesetzlicher Kündigungsfristen ordnungsgemäß abzuwickeln.
2. Werden personenbezogene Daten verarbeitet, um Direktwerbung ~~für nicht kommerzielle Zwecke~~ zu betreiben, hat die betroffene Person das Recht, dagegen	Übersetzungsfehler im ersten Satz, der aber in der offiziellen Kommissionsfassung mittlerweile bereinigt zu sein scheint (Vgl. auch Erwägungsgrund 57 der deutschen

unentgeltlich Widerspruch einzulegen. Die betroffene Person muss ausdrücklich in einer verständlichen und von anderen Informationen klar abgegrenzten Weise~~Form~~ auf dieses Recht hingewiesen werden.	Fassung). Satz 2: „manner“ sollte besser mit „Weise“ übersetzt werden.
3. Im Falle eines Widerspruchs gemäß Absatz 1 ~~und 2~~ darf der für die Verarbeitung Verantwortliche die betreffenden personenbezogenen Daten nicht weiter nutzen oder anderweitig verarbeiten. Im Falle eines Widerspruchs gemäß Absatz 2 darf der für die Verarbeitung Verantwortliche die betreffenden personenbezogenen Daten nicht für Zwecke der Direktwerbung weiter nutzen.	Mit einem neuen zweiten Satz wird klargestellt, dass bei einem Widerspruch gegen Verarbeitungen zu Werbezwecken die Verarbeitung zur Erfüllung eines Vertrages unberührt bleibt.
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	
b) ausdrücklich aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten gestattet ist ~~und diese Rechtsvorschriften geeignete Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person enthalten~~ oder	Der zweite Halbsatz ist zu streichen, da es nicht Aufgabe von Unternehmen sein kann, zu prüfen, ob die gesetzliche Bestimmung, die die Maßnahme erlaubt oder fordert, dem Datenschutz angemessen Rechnung trägt. Vielmehr muss sich das Unternehmen auf diese gesetzliche Vorschrift verlassen können.
c) mit Einwilligung der betroffenen Person nach Maßgabe von Artikel 7 ~~und vorbehaltlich entsprechender Garantien~~ erfolgt.	Der zweite Halbsatz ist zu streichen. Die Einwilligung muss als Legitimation der Datenverarbeitung ausreichen. Es ist unklar, welche zusätzlichen „Garantien“ erforderlich sein sollten.
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.	
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.	Der Begriff „Auswirkungen“ ist unklar.
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.~~	Die Kodifizierung von Zulässigkeits-tatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.

ABSCHNITT 5
BESCHRÄNKUNGEN

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 21 ***Beschränkungen***	
1. Die Union oder die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5 Buchstaben a bis e und den Artikeln 11 bis 20 sowie gemäß Artikel 32 beschränken, sofern eine solche Beschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist	Die im Folgenden angedachten Beschränkungen sollten weitgehend in der Verordnung selbst geregelt werden und nicht der Rechtsetzung der Mitgliedstaaten überlassen bleiben. Der Regelungsinhalt sollte sich an § 33 Abs. 2 BDSG orientieren (siehe auch Ergänzung von Artikel 15). Die Beschränkungen sollten insbesondere Geschäftsgeheimnisse und Eigentumsrechte der Verantwortlichen schützen, vgl. z.B. Erwägungsgrund 51 VO-E in Bezug auf die dort bereits dargelegte Beschränkung von Auskunftsansprüchen des Betroffenen durch Geschäftsgeheimnisse und Eigentumsrechte.
a) zum Schutz der öffentlichen Sicherheit	
b) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten	
c) zum Schutz sonstiger öffentlicher Interessen der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats etwa im Währungs-, Haushalts- und Steuerbereich und zum Schutz der Marktstabilität und Marktintegrität	
d) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe	
e) für Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher	

Gewalt für die unter den Buchstaben a, b, c und d genannten Zwecke verbunden sind	
f) zum Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.	
2. Jede Legislativmaßnahme im Sinne des Absatzes 1 muss spezifische Vorschriften zumindest zu den mit der Verarbeitung verfolgten Zielen und zur Bestimmung des für die Verarbeitung Verantwortlichen enthalten.	

KAPITEL IV

FÜR DIE VERARBEITUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER

ABSCHNITT 1
ALLGEMEINE PFLICHTEN

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 22 ***Pflichten des für die Verarbeitung Verantwortlichen***	
1. Der für die Verarbeitung Verantwortliche dokumentiert die von ihm aufzustellenden Datenschutzgrundsätze und ~~stellt durch~~ von ihm zu treffenden geeigneten ~~Strategien und~~ Maßnahmen, ~~sicher, dass~~damit personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden.~~ und er den Nachweis dafür erbringen kann.~~	Die deutsche Fassung weicht von der englischen Fassung ab. Diese lautet: *„The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.“* Die nebenstehende Fassung entspricht dagegen den von der englischen Fassung vorgegebenen Anforderungen. Das Erbringen von Nachweisen und Informationen gegenüber der Aufsichtsbehörde ist bereits in Artikel 29 VO-E geregelt. Überdies ist eine generelle Beweislastumkehr abzulehnen, da damit Rechte im Verwaltungs- und Strafverfahren unverhältnismäßig beschnitten würden.

2. Die in Absatz 1 genannten Maßnahmen umfassen insbesondere	
(a) die Dokumentation nach Maßgabe von Artikel 28;	Zur Kommentierung siehe Artikel 28.
(b) die Umsetzung der in Artikel 30 vorgesehenen Vorkehrungen für die Datensicherheit;	Zur Kommentierung siehe Artikel 30.
(c) die Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 33;	Zur Kommentierung siehe Artikel 33.
(d) die Umsetzung der nach Artikel 34 Abätze 1 und 2 geltenden Anforderungen in Bezug auf die vorherige Genehmigung oder Zurateziehung der Aufsichtsbehörde;	Zur Kommentierung siehe Artikel 34.
(e) die Benennung eines Datenschutzbeauftragten gemäß Artikel 35 Absatz 1.	Zur Kommentierung siehe Artikel 35.
3. Der für die Verarbeitung Verantwortliche setzt geeignete Verfahren zur Überprüfung der Wirksamkeit der in den Absätzen 1 und 2 genannten Maßnahmen ein. Die Überprüfung wird von ~~unabhängigen~~ internen oder externen Prüfern durchgeführt, wenn dies angemessen ist.	Zu Satz 2: Um klarzustellen, dass eine Prüfung beispielsweise durch eine interne Revision bzw. den betrieblichen Datenschutzbeauftragten ausreichend ist, sollte in Satz 2 das Tatbestandsmerkmal „unabhängig“ gestrichen werden. Die bestehenden Prüfungskompetenzen für den Datenschutz durch den betrieblichen Datenschutzbeauftragten sowie die in den Unternehmen installierten Revisoren haben sich in der Praxis bewährt. Diese Prüfungsmechanismen sind auch im Bankaufsichtsrecht anerkannt. Die Normierung neuer zusätzlicher Prüfmechanismen würde die Zielsetzung der Verordnung in Frage stellen, Bürokratie abzubauen und administrativen Aufwand zu reduzieren.
~~4. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament

~~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.~~	vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
Artikel 23 ***Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen***	
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. Es sind nur solche Maßnahmen zu treffen, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.	Neuer zweiter Satz: Es sollte sichergestellt werden, dass die zu treffenden Maßnahmen in einem angemessenen Verhältnis zu den Kosten der Implementierung stehen (so schon Artikel 17 Abs. 1 sowie Erwägungsgrund 46 der EU-Datenschutzrichtlinie, vgl. auch bankaufsichtsrechtliche Vorgaben in AT 7.2 der MaRisk).
2. Der für die Verarbeitung Verantwortliche setzt Verfahren ein, die sicherstellen, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, die für den jeweiligen ~~die spezifischen~~ Zwecke~~n~~ der Verarbeitung benötigt werden, und dass ~~vor allem~~ nicht mehr personenbezogene Daten zusammengetragen oder vorgehalten werden als für diese Zwecke erforderlich ~~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 einem abgegrenzten Kreis ~~nicht einer unbestimmten Zahl~~ von natürlichen Personen	Satz 1: Die Füllwörter führen zu Auslegungsproblemen und sind zu streichen. Satz 2: Durch die Änderung wird das Prinzip der Zugriffskontrolle verständlicher abgebil-

zugänglich gemacht werden.	det.
~~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.~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
~~4. Die Kommission kann technische Standards für die in den Absätzen 1 und 2 genannten Anforderungen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.~~	Die Entwicklung technischer Standards sollte den für die Datenverarbeitung Verantwortlichen überlassen bleiben. Andernfalls droht ein Mehr an Bürokratismus. Zudem könnten Produktinovationen verhindert werden, wenn die Standards zu eng gefasst wären.
Artikel 24 ***Gemeinsam für die Verarbeitung Verantwortliche***	
In allen Fällen, in denen ein für die Verarbeitung Verantwortlicher die Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten gemeinsam mit anderen Personen festlegt, vereinbaren diese gemeinsam für die Verarbeitung Verantwortlichen, wer von ihnen welche ihnen gemäß dieser Verordnung obliegenden Aufgaben erfüllt, insbesondere was die Verfahren und Mechanismen betrifft, die den betroffenen Personen die Wahrnehmung ihrer Rechte ermöglichen.	In der Wirtschaft gewinnt das arbeitsteilige Zusammenwirken immer mehr an Bedeutung. Kreditinstitute arbeiten in Konzernen und Verbünden zusammen und bedürfen der Inanspruchnahme externer Datenverarbeitungsdienstleister, auch außerhalb des EWR-Raums. Das modifizierte Verantwortlichkeitskonzept (Artikel 22 und 24) in der Verordnung bietet mit der „gemeinsamen Verantwortung“ bereits gute Ansätze für die gemeinschaftliche Datennutzung in Konzernen und Verbünden. Dabei muss aber weiter geklärt werden, dass eine gemeinsame Verantwortung von Stellen nicht nur eine Haftungsgemeinschaft begründet, sondern - in Abgrenzung zur erlaubnispflichtigen Datenübermittlung - auch den Datenaustausch in der Gruppe dem unternehmensinternen Datenverkehr bei einer

	alleinverantwortlichen Stelle gleichstellt. Dies wäre ein enormer Fortschritt, um den arbeitsteiligen Prozessen in Konzernen und Unternehmensverbünden Rechnung zu tragen. Nachteile für den Betroffenen sind dabei nicht erkennbar, denn der datenschutzrechtliche Zweckbindungsgrundsatz gilt fort und die beteiligten Stellen sind dem Betroffenen gemeinschaftlich gegenüber verantwortlich und haftbar. In dem Zusammenhang müsste auch eine klare Abgrenzung zur Auftragsdatenverarbeitung vorgenommen werden, bei der nur der Auftraggeber die verantwortliche Stelle ist und die Einschaltung des Auftragnehmers den Voraussetzungen des Artikel 26 des Verordnungsvorschlags entsprechen muss. Dazu ist es erforderlich, in Abgrenzung zur erlaubnispflichtigen Datenübermittlung dem Artikel 26 den Charakter einer eigenständigen Zulässigkeitsvorschrift für den Datenaustausch zwischen Auftraggeber und Auftragnehmer zu geben. Zudem sind die Begriffe „Auftragsverarbeiter“ (Artikel 4 Absatz 6) und „Empfänger“ (Artikel 4 Absatz 7) entsprechend zu gestalten.
Artikel 25 ***Repräsentant~~Vertreter~~ von nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen***	Folgeänderung zu Artikel 4 Absatz 14.
1. Jeder für die Verarbeitung Verantwortliche, der sich in der in Artikel 3 Absatz 2 beschriebenen Situation befindet, benennt einen Repräsentat~~Vertreter~~ in der Union.	Folgeänderung zu Artikel 4 Absatz 14.
2. Diese Pflicht gilt nicht für	
a) für die Verarbeitung Verantwortliche, die in einem Drittland niedergelassen sind, das laut Beschluss der Kommission einen angemessenen Schutz im Sinne von Artikel 41 bietet; oder	

b) Unternehmen, die weniger als 250 Mitarbeiter beschäftigen; oder	
~~c) Behörden oder öffentliche Einrichtungen;~~ oder	Es ist kein Grund ersichtlich, dass Behörden und öffentliche Einrichtungen privilegiert werden. Abs. 2 a) ist ausreichend.
d) für die Verarbeitung Verantwortliche, die in der Union ansässigen betroffenen Personen nur gelegentlich Waren oder Dienstleistungen anbieten.	
3. Der Repräsentant~~Vertreter~~ muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, ansässig sind.	Folgeänderung zu Artikel 4 Absatz 14.
4. Die Benennung eines Repräsentant~~Vertreters~~ durch den für die Verarbeitung Verantwortlichen erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den für die Verarbeitung Verantwortlichen.	Folgeänderung zu Artikel 4 Absatz 14.

Artikel 26 ***Auftragsverarbeiter***	Durch die von uns in Artikel 4 Absätze 3 und 7 der VO nunmehr vorgeschlagenen Ergänzungen wird deutlich, dass eine Weitergabe von personenbezogenen Daten an einen Auftragsdatenverarbeiter keine „Datenübermittlung“ und folglich keine „Verarbeitung“ im Sinne von Artikel 4 Abs. 3 darstellt. Daher muss die Datenweitergabe an einen Auftragsdatenverarbeiter nicht – zusätzlich - gemäß Artikel 6 VO-E legitimiert werden. Dieses Konzept entspricht der Richtlinie 95/46/EG sowie dem Bundesdatenschutzgesetz (vgl. Artikel 2f) und g) Richtlinie 95/46/EG; § 3 Abs. 8 BDSG). Durch die von uns vorgeschlagenen Ergänzungen ist sichergestellt, dass die Weiterleitung von Daten an einen Auftragsdatenverarbeiter bei Erfüllung der Vorgaben aus Artikel 26 datenschutzrechtlich stets zulässig ist und keiner weiteren besonderen Legitimation bedarf.
1. Der für die Verarbeitung Verantwortliche wählt für alle in seinem Auftrag durchzuführenden Verarbeitungs- vorgänge einen Auftragsverarbeiter aus, der hinreichende Sicherheitsvorkehrungen ~~Garantien~~ dafür bietet, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und dass der Schutz der Rechte der betroffenen Person durch geeignete technische Sicherheitsvorkehrungen und organisatorische Maßnahmen für die vorzunehmende Verarbeitung sichergestellt wird; zudem prüft er, ~~sorgt er dafür,~~ ob ~~dass~~ diese Maßnahmen eingehalten werden.	Der Begriff „Garantie“ ist nach nationaler Lesart mit haftungsrechtlichen Fragen verbunden. In der englischen Fassung wird in Artikel 26 der Begriff „safeguards“ verwendet. Dieser sollte besser mit dem neutralen Begriff „Sicherheitsvorkehrungen“ übersetzt werden. (Diese Anmerkung gilt für alle Fälle, in denen sich der Begriff „safeguards“ auf einen technisch-organisatorischen Prozess bezieht und keine „Garantie“ im Rechtssinne gemeint ist). Die Formulierung eines Prüfungserfordernisses ist praxisgerechter und bildet die Einflussnahmemöglichkeiten des Auftraggebers angemessen ab.
2. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder sonstigen Rechtsakts, ~~durch~~ der den ~~der~~ Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet ~~gebunden ist~~ und in denen~~dem~~ insbesondere vorgesehen ist, dass der Auftragsverarbeiter	Sprachliche Klarstellung.

a) nur auf Weisung des für die Verarbeitung Verantwortlichen tätig wird, insbesondere in Fällen, in denen eine Übermittlung der personenbezogenen Daten nicht zulässig ist;	
b) mit der Datenverarbeitung ausschließlich Mitarbeiter betraut~~beschäftigt~~, die sich zur Vertraulichkeit verpflichtet haben oder der gesetzlichen Verschwiegenheitspflicht unterliegen;	Die Verpflichtung zum vertraulichen Umgang mit Daten kann sich nur auf solche Mitarbeiter beziehen, die mit der Datenverarbeitung beschäftigt sind. Hiezu gehören beispielsweise regelmäßig nicht Gärtner, Kantinenpersonal, etc.
c) alle in Artikel 30 genannten erforderlichen Maßnahmen ergreift;	
d) die Dienste eines weiteren Auftragsverarbeiters nur mit vorheriger Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch nehmen darf;	
e) soweit es verarbeitungsbedingt möglich ist, in Absprache mit dem für die Verarbeitung Verantwortlichen die notwendigen technischen und organisatorischen Voraussetzungen dafür schafft, dass der für die Verarbeitung Verantwortliche seine Pflicht erfüllen kann, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;	Zur Kommentierung der Vorschriften nach Kapitel III siehe dort.
f) den Auftragsverarbeiter bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unterstützt;	
g) nach Abschluss der Verarbeitung dem für die Verarbeitung Verantwortlichen überlassene Daten~~träger~~ zurückgibt ~~sämtliche Ergebnisse aushändigt~~ oder auf Weisung nachweislich löscht und die personenbezogenen Daten auf keine andere Weise weiterverarbeitet;	Die hier vorgeschlagene Formulierung entspricht dem Interesse des Auftraggebers, dass die überlassen Daten zurückgegeben oder gelöscht werden.
(h) dem für die Verarbeitung Verantwortlichen und der Aufsichtsbehörde auf Verlangen alle erforderlichen Informationen für die Kontrolle der	Klarstellung, dass die erforderlichen Informationen nur „auf Verlangen“ zur Verfügung zu stellen sind.

Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt.	
3. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter dokumentieren <u>den Umfang der Weisungsbefugnisse</u> ~~die Anweisungen~~ des für die Verarbeitung Verantwortlichen und die in Absatz 2 aufgeführten Pflichten des Auftragsverarbeiters.	Es sollte genügen, wenn der Umfang der Weisungsbefugnisse vertraglich fixiert wird. Vorbild kann auch hier wieder § 11 Abs. 2 Satz 2 Nr. 9 des deutschen BDSG sein.
4. Jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, gilt für diese Verarbeitung als für die Verarbeitung Verantwortlicher und unterliegt folglich den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche.	
~~5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Verantwortlichkeiten, Pflichten und Aufgaben des Auftragsverarbeiters in Übereinstimmung mit Absatz 1 festzulegen sowie die Bedingungen, durch die die Verarbeitung personenbezogener Daten in Unternehmensgruppen speziell zu Kontroll- und Berichterstattungszwecken vereinfacht werden kann.~~	Die Kodifizierung von Zulässigkeits-tatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
Artikel 27 ***Verarbeitung unter der Aufsicht des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters***	
Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten, sofern sie keinen anders lautenden, aus dem Unionsrecht oder dem	

mitgliedstaatlichen Recht erwachsenden Pflichten unterliegen.	
Artikel 28 ***Dokumentation***	
1. Alle für die Verarbeitung Verantwortlichen, alle Auftragsverarbeiter sowie etwaige Repräsentanten~~Vertreter~~ von für die Verarbeitung Verantwortlichen dokumentieren die ihrer Zuständigkeit unterliegenden Verfahren automatisierter Verarbeitungen~~Verarbeitungsvorgänge~~.	Der Begriff „Verarbeitungsvorgang“ ist nicht legal definiert. In Anknüpfung an den in Artikel 4 Abs. 3 der Verordnung definierten Begriff der „Verarbeitung“ könnte damit jegliche Verwendung personenbezogener Daten erfasst sein. Dies ginge erheblich über den in § 4e BDSG verorteten Begriff des „Verfahrens automatisierter Verarbeitungen“ hinaus und würde zu einer erheblichen Mehrbelastung der Unternehmen führen. Zudem: Folgeänderung zu Artikel 4 Absatz 14.
2. Die Dokumentation enthält mindestens folgende Informationen:	
a) Name und Kontaktdaten des für die Verarbeitung Verantwortlichen (oder etwaiger gemeinsam für die Verarbeitung Verantwortlicher) oder des Auftragsverarbeiters sowie eines etwaigen Repräsentanten~~Vertreters~~;	Folgeänderung zu Artikel 4 Absatz 14.
b) Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten;	
c) Angaben über die Zwecke der Verarbeitung sowie – falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f gründet – über die von dem für die Verarbeitung Verantwortlichen verfolgten legitimen Interessen;	
d) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien der sich auf diese beziehenden personenbezogenen Daten;	
e) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten einschließlich der für die Verarbeitung	

Verantwortlichen, denen personenbezogene Daten aus dem von diesen verfolgtem legitimen Interesse mitgeteilt werden;	
f) gegebenenfalls Angaben über etwaige Datenübermittlungen in Drittländer oder an internationale Organisationen einschließlich deren Namen sowie bei den in Artikel 44 Absatz 1 Buchstabe h genannten Datenübermittlungen ein Beleg dafür, dass geeignete ~~Sicherheitsgarantien~~ Sicherheitsvorkehrungen vorgesehen wurden;	In der englischen Fassung wird in Artikel 28 und Artikel 44 das Wort „safeguards“ verwendet. Dies sollte besser mit dem neutralen Begriff „Sicherheitsvorkehrungen“ übersetzt werden.
g) eine allgemeine Angabe der Fristen für die Löschung der verschiedenen Datenkategorien;	
(h) eine Beschreibung der in Artikel 22 Absatz 3 genannten Verfahren.	
3. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Repräsentant~~Vertreter~~ des für die Verarbeitung Verantwortlichen stellen die Dokumentation der Aufsichtsbehörde auf Anforderung zur Verfügung.	Folgeänderung zu Artikel 4 Absatz 14.
4. Die in den Absätzen 1 und 2 genannten Anforderungen gelten nicht für folgende für die Verarbeitung Verantwortliche und Auftragsverarbeiter:	
a) natürliche Personen, die personenbezogene Daten ohne eigenwirtschaftliches Interesse verarbeiten; oder	
b) Unternehmen oder Organisationen mit weniger als 250 Beschäftigten, die personenbezogene Daten nicht geschäftsmäßig, sondern nur zur Unterstützung ~~als Nebentätigkeit zusätzlich zu~~ ihrer~~n~~ Haupttätigkeit~~en~~ verarbeiten.	Klarstellung im Vergleich zur englischen Fassung. Ursprüngliche Fassung dürfte kaum zur Entlastung kleiner und mittlerer Unternehmen führen.
~~5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannte Dokumentation festzulegen, so dass~~	Die Kodifizierung von Zulässigkeits-tatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig

~~insbesondere den Verantwortlichkeiten des für die Verarbeitung Verantwortlichen, des Auftragsverarbeiters sowie des etwaigen Vertreters des für die Verarbeitung Verantwortlichen Rechnung getragen wird.~~	nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
~~6. Die Kommission kann Standardvorlagen für die in Absatz 1 genannte Dokumentation festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.~~	Die Entwicklung von Vordrucken und Formularen sollte den Verwendern obliegen. Eine Standardisierung würde zu einer erheblichen Bürokratisierung führen.
Artikel 29 ***Zusammenarbeit mit der Aufsichtsbehörde***	
1. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Repräsentant~~Vertreter~~ des für die Verarbeitung Verantwortlichen unterstützen ~~arbeiten der~~ die Aufsichtsbehörde auf Verlangen bei der Erfüllung ihrer Pflichten ~~erleichtern~~, indem sie dieser insbesondere die in Artikel 53 Absatz 2 Buchstabe a genannten Informationen übermitteln und ihr den in Artikel 53 Absatz 2 Buchstabe b genannten Zugang gewähren.	Im deutschen Verwaltungsrecht ist eine aktive Unterstützungspflicht der Aufsichtsbehörde nicht die Regel. Gleichwohl wird ein Unternehmen mit der Aufsichtsbehörde kooperieren. Allerdings muss es der Aufsichtsbehörde nicht die Aufsicht „erleichtern“. Auch die englische Fassung fordert kein „erleichtern“. Der Begriff „unterstützen“ ist sachgerechter. Zudem: Folgeänderung zu Artikel 4 Absatz 14.
2. Auf von der Aufsichtsbehörde im Rahmen der Ausübung ihrer Befugnisse erteilte Anordnungen gemäß Artikel 53 Absatz 2 antworten der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter der Aufsichtsbehörde binnen einer von der Aufsichtsbehörde zu setzenden angemessenen Frist. Die Antwort muss auch eine Beschreibung der im Anschluss an die Bemerkungen der Aufsichtsbehörde getroffenen Maßnahmen und der damit erzielten Ergebnisse beinhalten.	

ABSCHNITT 2
DATENSICHERHEIT

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 30 ***Sicherheit der Verarbeitung***	
1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik und der Implementierungskosten technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Es sind nur solche Maßnahmen zu treffen, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.	Es sollte sichergestellt werden, dass die zu treffenden Maßnahmen in einem angemessenen Verhältnis zu den Kosten der Implementierung stehen (so schon Artikel 17 Abs. 1 sowie Erwägungsgrund 46 der EU-Datenschutzrichtlinie, vgl. auch bankaufsichtsrechtliche Vorgaben in AT 7.2 der MaRisk-).
2. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen im Anschluss an eine Risikobewertung die in Absatz 1 genannten Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder widerrechtlichen Zerstörung oder vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung.	Nach Bankaufsichtsrecht gibt es bereits die Pflicht zu einer grundsätzlichen Risikobewertung (vgl. § 25a KWG, MaRisk). Es sollte ausreichen, dass die Bank die zu ergreifenden Sicherheitsmaßnahmen auf diese Risikobewertung stützen kann, um Doppelarbeit zu vermeiden.
~~3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen für die in den Absätzen 1 und 2 genannten technischen und organisatorischen Maßnahmen festzulegen und den aktuellen Stand der Technik für bestimmte Sektoren und Datenverarbeitungssituationen zu bestimmen, wobei sie die technologische Entwicklung sowie Lösungen für einen~~	Die Kodifizierung von Zulässigkeits-tatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.

~~Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen berücksichtigt, sofern nicht Artikel 4 gilt.~~	
~~4. Die Kommission kann erforderlichenfalls Durchführungsbestimmungen zu einer situationsabhängigen Konkretisierung der in den Absätzen 1 und 2 genannten Anforderungen erlassen, um insbesondere~~	Wenn weiterer Konkretisierungsbedarf besteht, dann sollte nach dem Vorbild der Anlage zu § 9 des deutschen BDSG vorgegangen und ein Maßnahmenkatalog zusammen mit der Verordnung verabschiedet werden. Zudem sollte der in § 9 BDSG verortete Verhältnismäßigkeitsgrundsatz auch nach den Vorschriften des VO-E maßgebliche Richtschnur sein.
~~a) jedweden unbefugten Zugriff auf personenbezogene Daten zu verhindern;~~	
~~b) jedwede unbefugte Einsichtnahme in personenbezogene Daten sowie jedwede unbefugte Offenlegung, Kopie, Änderung, Löschung oder Entfernung von personenbezogenen Daten zu verhindern;~~	
~~c) sicherzustellen, dass die Rechtmäßigkeit der Verarbeitungsvorgänge überprüft wird.~~	
~~Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.~~	
Artikel 31 ***Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde***	
1. Bei einer Verletzung des Schutzes personenbezogener Daten, bei der dem Betroffenen schwerwiegende Beeinträchtigungen seiner Rechte oder schutzwürdigen Interessen drohen, benachrichtigt der für die Verarbeitung Verantwortliche die Aufsichtsbehörde unverzüglich~~ohne unangemessene Verzögerung und nach Möglichkeit binnen 24 Stunden~~ nach Feststellung der Verletzung. ~~Falls die Meldung an die Aufsichtsbehörde nicht~~	Nach derzeitigem deutschem Recht hat eine Meldung von Datenpannen an die Behörde nur dann zu erfolgen, wenn schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen (vgl. § 42a BDSG). Diese Ausprägung des Verhältnismäßigkeitsgrundsatzes sollte auch in Artikel 31 der Verordnung Berücksichtigung finden, da anderenfalls eine Überlastung der verantwortlichen Stellen (und der zuständigen Behörden) durch Mel-

~~binnen 24 Stunden erfolgt, ist dieser eine Begründung beizufügen.~~	dungen von Bagatellfällen zu befürchten ist. Eine konkrete Fristvorgabe sollte nicht geregelt werden. Vielmehr sollte der allgemeine Grundsatz der Unverzüglichkeit der Meldung gelten.
2. In Übereinstimmung mit Artikel 26 Absatz 2 Buchstabe f ~~alarmiert und~~ informiert der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen unverzüglich und unmittelbar nach Feststellung einer Verletzung des Schutzes personenbezogener Daten.	Eine unverzügliche Information des Verantwortlichen ist ausreichend.
3. Die in Absatz 1 genannte Benachrichtigung enthält mindestens folgende Informationen:	
a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten mit Angabe Datenkategorien ~~der Kategorien~~ und der Zahl der betroffenen Personen~~, der betroffenen Datenkategorien und der Zahl der betroffenen Datensätze~~;	Die Angabe von „Kategorien“ und „Datenkategorien“ ist redundant. Des weiteren ist eine Mitteilung der betroffenen Datensätze dann nicht erforderlich, wenn die Aufsichtsbehörde darüber informiert wurde, wieviele Personen von der „Datenpanne“ betroffen sind. Denn die Ausichtsbehörde kann an Hand der Nennung der Anzahl der betroffenen Personen das Ausmaß der Verletzung des Schutzes personenbezogener Daten bewerten.
b) Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen;	
c) soweit möglich, Empfehlungen für Maßnahmen zur Eindämmung etwaiger negativer Auswirkungen der Verletzung des Schutzes personenbezogener Daten;	Es wird nicht in jedem Fall die Möglichkeit bestehen, entsprechende Maßnahmen zu treffen, so dass die nebenstehnde Einschränkung geboten ist.
d) eine Beschreibung der Folgen der Verletzung des Schutzes personenbezogener Daten;	
~~e) eine Beschreibung der vom für die Verarbeitung Verantwortlichen vorgeschlagenen oder ergriffenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten.~~	Redundant zu c).

~~4. Der für die Verarbeitung Verantwortliche dokumentiert etwaige Verletzungen des Schutzes personenbezogener Daten unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen. Die Dokumentation enthält nur die zu diesem Zweck erforderlichen Informationen.~~	Durch die oben normierte Informationspflicht ist die hier angedachte Dokumentationspflicht erfüllt. Der Absatz ist daher zu streichen. Insbesondere sollte der letzte Satz gestrichen werden, da er zu Abgenzungsschwierigkeiten führen kann.
~~5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Feststellung der in den Absätzen 1 und 2 genannten Verletzungen des Schutzes personenbezogener Daten festzulegen sowie die konkreten Umstände, unter denen der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden haben.~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
~~6. Die Kommission kann das Standardformat für derartige Meldungen an die Aufsichtsbehörde, die Verfahrensvorschriften für die vorgeschriebene Meldung sowie Form und Modalitäten der in Absatz 4 genannten Dokumentation einschließlich der Fristen für die Löschung der darin enthaltenen Informationen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.~~	
Artikel 32 ***Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes ihrer personenbezogenen Daten***	
1. Der für die Verarbeitung Verantwortliche benachrichtigt im Anschluss an die Meldung nach Artikel 31 die	Artikel 32 sollte sich am Vorbild des § 42a des deutschen BDSG orientierend und sich nicht auf alle personenbezogenen Daten be-

betroffene Person ohne unangemessene Verzögerung von der Verletzung des Schutzes personenbezogener Daten, wenn schwerwiegende Beeinträchtigungen für den ~~die Wahrscheinlichkeit besteht, dass der~~ Schutz der personenbezogenen Daten oder der Privatsphäre der betroffenen Person durch eine festgestellte Verletzung des Schutzes personenbezogener Daten drohen ~~beeinträchtigt wird~~.	ziehen, sondern nur solche erfassen, deren Verletzung sich für den Betroffenen besonders nachteilhaft auswirken kann. Darüber hinaus sollten die Regelungen nur dann eingreifen, wenn besonders schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Erwägungsgrund 67 geht daher zu weit.
2. Die in Absatz 1 genannte Benachrichtigung der betroffenen Person umfasst mindestens die in Artikel 31 Absatz 3 Buchstaben b und c genannten Informationen und Empfehlungen.	
3. Die Benachrichtigung der betroffenen Person über die Verletzung des Schutzes personenbezogener Daten ist nicht erforderlich, wenn der für die Verarbeitung Verantwortliche ~~zur Zufriedenheit~~ der Aufsichtsbehörde darlegt ~~nachweist~~, dass er geeignete technische Sicherheits- vorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden. ~~Durch diese technischen Sicherheitsvorkehrungen sind die betreffenden Daten für alle Personen zu verschlüsseln, die nicht zum Zugriff auf die Daten befugt sind.~~	„darlegt“ entspricht der englischen Vorgabe „demonstrate“. Der letzte Satz ist zu streichen, da er schon nicht verständlich und in der Art und Weise nicht technisch umsetzbar ist.
4. Unbeschadet der dem für die Verarbeitung Verantwortlichen obliegenden Pflicht, der betroffenen Person die Verletzung des Schutzes personenbezogener Daten mitzuteilen, kann die Aufsichtsbehörde, falls der für die Verarbeitung Verantwortliche die betroffene Person noch nicht in Kenntnis gesetzt hat, nach Prüfung der zu erwartenden negativen Auswirkungen der Verletzung den für die Verarbeitung Verantwortlichen auffordern, dies zu tun.	
~~5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die

~~Anforderungen in Bezug auf die Umstände festzulegen, unter denen sich eine Verletzung des Schutzes personenbezogener Daten negativ auf die in Absatz 1 genannten personenbezogenen Daten auswirken kann.~~	Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
~~6. Die Kommission kann das Format für die in Absatz 1 genannte Mitteilung an die betroffene Person und die für die Mitteilung geltenden Verfahrensvorschriften festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.~~	Soweit Regelungsbedarf besteht, sollte das Meldeformular sogleich mit der Verordnung verabschiedet werden.

ABSCHNITT 3
DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE GENEHMIGUNG

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 33 ***Datenschutz-Folgenabschätzung***	
1. Bei Verarbeitungs<u>verfahren</u>~~vorgängen~~, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke <u>besondere</u> ~~konkrete~~ Risiken für die Rechte und Freiheiten betroffener Personen <u>aufweisen</u> ~~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. <u>Eine Folgenabschätzung ist nicht erforderlich, wenn für das</u> ~~den~~ <u>Verarbeitungs-verfahren</u> ~~vorgang~~ <u>eine gesetzliche Verpflichtung,</u> ~~vorliegt~~ <u>eine Einwilligung des Betroffenen vorliegt oder</u> <u>für die Erfüllung oder Durchführung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen im Interesse des Betroffenen erforderlich ist.</u>	Allgemein: Die Folgenabschätzung soll (wohl) die bisherige Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten ersetzen. Durch die fehlende Anknüpfung an die Rolle des Datenschutzbeauftragten, wird dessen Kontrollfunktion erheblich gemindert. Des Weiteren ist eine Datenschutz-Folgenabschätzung ohne jegliche Ausnahmen überflüssig und schafft nur neue, unnötige bürokratische Verfahren. Durch die allgemeinen Formulierungen ist unklar, welche Bereiche tatsächlich einer solchen Folgenabschätzung unterliegen. Diese Rechtsunsicherheit, der der Verantwortliche ausgesetzt wird, in Kombination mit den umfangreichen Verpflichtungen, denen er unterworfen wird (u. a. Beschreibung der Verarbeitungsvorgänge, Bewertung der Risiken, Abhilfemaßnahmen, Garantien, Meinungseinholung der betroffenen Person oder des Vertreters, Konsultation der Aufsichtsbehörde nach Artikel 34 Absatz 2 lit. a), führt zu einem erheblichen Zuwachs an Bürokratie und Unsicherheit. Dies gilt um-

	so mehr, als bei einem Verstoß gegen Artikel 33 nach Artikel 79 Absatz 6 lit. i) eine empfindliche Geldbuße verhängt werden kann. Zu Satz 1: Es sollte nicht an einzelne Verarbeitungsvorgänge, sondern an Verarbeitungsverfahren angeknüpft werden. Maßstab für eine Folgenabschätzung sollten „besondere" Risiken sein (vgl. auch § 4d Absatz 5 BDSG). Dies entspricht auch eher der englischen Fassung „specific". Zu Satz 2: Es sollte nach dem Vorbild des § 4d Absatz 5 des deutschen BDSG eine Folgenabschätzung in den genannten Fällen nicht erforderlich sein. Insbesondere sollte keine Pflicht zur Folgeabschätzung bestehen, wenn die Datenverarbeitung auf einer gesetzlichen Verpflichtung beruht und das Unternehmen als gesetzlich Verpflichteter keinen Umsetzungsspielraum hat. Denn in diesem Fall müsste bereits der Gesetzgeber die Folgenabschätzung durchführen.
2. Die in Absatz 1 genannten Risiken bestehen insbesondere bei folgenden Verarbeitungsvorgängen:	
a) systematische und umfassende Auswertung persönlicher Aspekte einer natürlichen Person, beispielsweise zwecks Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens oder zwecks diesbezüglicher Voraussagen, die sich auf eine automatisierte Verarbeitung von Daten gründet und ihrerseits als Grundlage für Maßnahmen dient, welche Rechtswirkung gegenüber der betroffenen Person entfalten oder erhebliche Beeinträchtigungen ~~Auswirkungen~~ für diese mit sich bringen;	Die Regelung sollte wie Artikel 20 Abs. 1 der VO gefasst werden.
b) Verarbeitung von Daten über das Sexualleben, den Gesundheitszustand, die Rasse oder die ethnische Herkunft oder für die Erbringung von Gesundheitsdiensten, für epidemiologische Studien oder für Erhebungen über Geisteskrankheiten oder	

ansteckende Krankheiten, wenn die betreffenden Daten in großem Umfang im Hinblick auf Maßnahmen oder Entscheidungen verarbeitet werden, welche sich auf spezifische Einzelpersonen beziehen sollen;	
c) weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels Videoüberwachung;	
d) Verarbeitung personenbezogener Daten aus umfangreichen Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten;	
~~e) sonstige Verarbeitungsvorgänge, bei denen gemäß Artikel 34 Absatz 2 Buchstabe b vorab die Aufsichtsbehörde zu Rate zu ziehen ist.~~	Hiermit würde die Aufsichtsbehörde über Artikel 34 Absatz 2 b i.V.m. Artikel 34 Absatz 4 eine Rolle als Gesetzgeber zugewiesen, was mit dem Gewaltenteilungsprinzip nicht vereinbar ist. In der Verordnung sollten die Regelbeispiele konkret formuliert werden und nicht der Bestimmung durch die Aufsichtsbehörden unterliegen. Sollten an anderer Stelle konkret besondere Prüfungspflichten statuiert werden, könnte auf diese in Artikel 33 Absatz 2 verwiesen werden.
3. Die Folgenabschätzung trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung; sie enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten ~~Abhilfem~~ risikobezogenen Maßnahmen, ~~Garantien,~~ Sicherheitsvorkehrungen und ~~–~~maßnahmen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden.	Angleichung an die englische Fassung.
4. ~~Der für die Verarbeitung Verantwortliche holt die Meinung der~~	Diese Regelung verletzt die Betriebs- und Geschäftsgeheimnisse der Unternehmen und

~~betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein~~. Soweit ein betrieblicher Datenschutzbeauftragter bestellt ist, ist dieser in die Folgenabschätzung einzubeziehen.	greift in deren auch verfassungsrechtlich geschütze Rechte bzw. berechtigen Interessen ein (vgl. auch Erwägungsgrund 51 der VO). Zudem ist mit dieser Regelung ein erheblicher Mehraufwand für die Unternehmen verbunden. Plant eine Bank z.B. Scoring-Verfahren einzuführen, müsste sie vorab die Meinung der Betroffenen oder ihrer Vertreter einholen. Dies ist nicht angemessen. Darüber hinaus werden durch die Vorgabe Produktinovationen verhindert; es drohen Wettbewerbsnachteile für die in der EU ansässigen Unternehmen. Zudem ist beispielsweise ein Verbraucherschutzverband nicht unbedingt von den Verbrauchern mit Stellvertretungsrechten ausgestattet. Mithin wird vielen Verbänden das rechtliche Mandat fehlen.
~~5. Falls es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde oder um eine öffentliche Einrichtung handelt und die Verarbeitung aufgrund einer im Unionsrecht festgelegten rechtlichen Verpflichtung nach Artikel 6 Absatz 1 Buchstabe c erfolgt, welche Vorschriften und Verfahren für die betreffenden Verarbeitungsvorgänge vorsieht, gelten die Absätze 1 bis 4 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.~~	Aus Sicht des Betroffenen ist nicht nachvollziehbar, warum der öffentliche Sektor keine Folgenabschätzung vornehmen sollte.
~~6. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen für Verarbeitungsvorgänge, die mit den in den Absätzen 1 und 2 genannten Risiken behaftet sein können, sowie die Anforderungen an die in Absatz 3 genannte Folgenabschätzung einschließlich der Bedingungen für die Skalierbarkeit und für die interne und externe Überprüfbarkeit festzulegen. Dabei berücksichtigt die Kommission spezifische Maßnahmen für Kleinst-, Klein- und mittlere Unternehmen.~~	Die Kodifizierung von Zulässigkeitstat-beständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.

~~7. Die Kommission kann Standards und Verfahren für die Durchführung sowie für die interne und externe Überprüfung der in Absatz 3 genannten Folgenabschätzung festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.~~	
Artikel 34 ***Vorherige Genehmigung und vorherige Zurateziehung***	
~~1. Der für die Verarbeitung Verantwortliche oder gegebenenfalls der Auftragsverarbeiter holt vor der Verarbeitung personenbezogener Daten eine Genehmigung der Aufsichtsbehörde ein, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und um insbesondere die Risiken zu mindern, welche für die betroffenen Personen bestehen, wenn dieser Vertragsklauseln nach Artikel 42 Absatz 2 Buchstabe d vereinbart oder keine geeigneten Garantien für die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation in einem rechtsverbindlichen Instrument nach Artikel 42 Absatz 5 vorsieht.~~	Die Regelung ist selbst in der englischen Fassung schwer verständlich. Es kann keine generelle Vorabgnehmigungspflicht beabsichtigt sein. Vielmehr könnte eine Genehmigungspflicht bei Drittstaatenübermittlungen intendiert sein. Diese ist bereits in Artikel 42 Absatz 2d und Absatz 4 geregelt. Deshalb sollte der Absatz 1 gestrichen werden. Die Einholung einer Genehmigung vor der Verarbeitung personenbezogener Daten ist sehr aufwendig und dürfte in der Praxis angesichts der geringen Kapazitäten der Aufsichtsbehörden zu erheblichen Verzögerungen im Hinblick auf die Genehmigung von Datenverarbeitungen führen. Dies führt zu Wettbewerbsverzerrungen im Vergleich zu nicht in der EU tätigen Unterenhmen. Angesichts des Umstandes, dass die Verordnung bereits eine Datenschutz-Folgeabschätzung verpflichtend vorschreibt, sollte auf einen generellen Genehmigungsvorbehalt der Aufsichtsbehörde verzichtet werden. Allenfalls dann, wenn im Unternehmen Zweifel an der Zulässigkeit der Datenverarbeitung bestehen, sollte dem Verantwortlichen die Möglichkeit eingeräumt werden, die zuständige Aufsichtsbehörde zu Rate zu ziehen.
2. Der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter zieht vor der Verarbeitung personenbezogener Daten die Auf-	Es muss deutlich werden, dass die Konsultationspflicht ausschließlich in den genannten Fällen besteht.

sichtsbehörde zu Rate, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und um insbesondere die für die betroffenen Personen bestehenden Risiken zu mindern; dies gilt für ~~alle~~ Fälle, in denen	
a) aus einer Datenschutz-Folgenabschätzung nach Artikel 33 hervorgeht, dass die geplanten Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke im hohen Maße besondere~~konkrete~~ Risiken bergen können; oder	Angleichung an die englische Fassung.
~~b) die Aufsichtsbehörde eine vorherige Zurateziehung bezüglich der in Absatz 4 genannten Verarbeitungsvorgänge, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, für erforderlich hält.~~	Hiermit würde die Aufsichtsbehörde über Artikel 34 Absatz 2 b i.V.m. Artikel 34 Absatz 4 eine Rolle als Gesetzgeber zugewiesen, was mit dem Gewaltenteilungsprinzip nicht vereinbar ist. In der Verordnung sollten – soweit erforderlich – weitere Fälle abschließend normiert werden.
3. Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung steht, insbesondere weil die Risiken unzureichend ermittelt wurden oder eingedämmt werden, untersagt sie die geplante Verarbeitung und unterbreitet geeignete Vorschläge, wie diese Mängel beseitigt werden könnten.	
~~4. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, die Gegenstand der vorherigen Zurateziehung nach Absatz 2 Buchstabe b sind, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt derartige Listen an den Europäischen Datenschutzausschuss.~~	Hiermit würde die Aufsichtsbehörde über Artikel 34 Absatz 2 b i.V.m. Artikel 34 Absatz 4 eine Rolle als Gesetzgeber zugewiesen, was mit dem Gewaltenteilungsprinzip nicht vereinbar ist. In der Verordnung sollten – soweit erforderlich – weitere Fälle abschließend normiert werden. Eine Veröffentlichung solcher Listen ist mit dem Betriebs- und Geschäftsgeheimnis der Unternehmen nicht vereinbar (vgl. auch Erwägungsgrund 51 der VO).
~~5. Wenn auf der in Absatz 4 genannten Liste Verarbeitungsvorgänge aufgeführt~~	Folgeänderung zu 4.

~~werden, die sich auf Waren oder Dienstleistungen beziehen, welche betroffenen Personen in mehreren Mitgliedstaaten angeboten werden, oder die dazu dienen sollen, das Verhalten dieser betroffenen Personen zu beobachten, oder die wesentliche Auswirkungen auf den freien Verkehr personenbezogener Daten in der Union haben können, bringt die Aufsichtsbehörde vor der Annahme der Liste das in Artikel 57 beschriebene Kohärenzverfahren zur Anwendung.~~	
~~6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter legt der Aufsichtsbehörde die Datenschutz-Folgenabschätzung nach Artikel 33 vor und übermittelt ihr auf Aufforderung alle sonstigen Informationen, die sie benötigt, um die Ordnungsgemäßheit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Risiken und die diesbezüglichen Sicherheitsgarantien bewerten zu können.~~	Fraglich ist, ob die Regelung autonom gilt und damit jegliche Folgenabschätzung der Aufsichtsbehörde vorzulegen ist. Dies ist ein unnötiger administrativer Aufwand für die Unternehmen und die Aufsichtsbehörden. Gerade wenn ein betrieblicher Datenschutzbeauftragter bestellt und in die Folgenabschätzung eingebunden ist, sind bereits nach der EU-Datenschutzrichtlinie keine zusätzlichen Meldepflichten gegenüber der Datenschutzaufsicht sinnvoll.
7. Die Mitgliedstaaten ziehen die Aufsichtsbehörde bei der Ausarbeitung einer von ihren nationalen Parlamenten zu erlassenden Legislativmaßnahme oder einer sich auf eine solche Legislativmaßnahme gründenden Maßnahme, durch die die Art der Verarbeitung definiert wird, zu Rate, damit die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sichergestellt ist und insbesondere die für die betreffenden Personen bestehenden Risiken gemindert werden.	
~~8. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Bestimmung der in Absatz 2 Buchstabe a genannten hohen konkreten Risiken festzulegen.~~	Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch erfassen.

~~9. Die Kommission kann Standardvorlagen und Verfahrensvorschriften für die in den Absätzen 1 und 2 genannte vorherige Genehmigung beziehungsweise Zurateziehung sowie für die in Absatz 6 vorgesehene Unterrichtung der Aufsichtsbehörde festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.~~	

ABSCHNITT 4
DATENSCHUTZBEAUFTRAGTER

Regelung ggf. mit Änderungsvorschlag	**Anmerkungen**
Artikel 35 ***Benennung eines Datenschutzbeauftragten***	
1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls	
a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder	
b) die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder	Das Instrument des betrieblichen Datenschutzbeauftragten hat sich in Deutschland sehr bewährt. Gerade in Kreditinstituten nimmt der betriebliche Datenschutzbeauftragte eine wichtige Funktion in der Selbstkontrolle wahr und hilft, gesetzeskonforme Datenverarbeitungen zu betreiben. Folglich ist zu begrüßen, dass dieses Instrument in der Verordnung gestärkt werden soll. Ob dazu aber die vorgesehenen Regelungen zu den Voraussetzungen für eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten beitragen, ist fraglich. Sofern die vorgenannten Pflichten zur Datenschutzfolgenabschätzung sowie zur Genehmigung von Datenverarbeitungs-vorgängen entgegen der hier vertretenen

	Auffassung beibehalten werden sollen, sollte erwogen werden, Anreize für die Bestellung eines Datenschutzbeauftragten zu schaffen. Institute, deren betriebliche Prozesse eine Vielzahl von Datenverarbeitungsvorgängen beinhalten, sollten dazu von diesen Pflichten entbunden werden, wenn sie sich für die Einrichtung einer eigenständigen und neutralen Instanz zur Kontrolle von Datenverarbeitungsvorgängen entscheiden.
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.	Klarstellung erforderlich, wer damit erfasst sein soll.
2. Im Fall des Absatzes 1 Buchstabe b und c darf eine Gruppe von Unternehmen einen gemeinsamen Datenschutzbeauftragten ernennen.	Auch in der Fallgruppe Absatz 1 c sollte es möglich sein, in einer Unternehmensgruppe einen gemeinsamen betrieblichen Datenschutzbeauftragten zu bestellen.
3. Falls es sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder um eine öffentliche Einrichtung handelt, kann der Datenschutzbeauftragte unter Berücksichtigung der Struktur der Behörde beziehungsweise der öffentlichen Einrichtung für mehrere Bereiche benannt werden.	
4. In anderen als den in Absatz 1 genannten Fällen können der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Gremien, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen.	
5. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter benennt den Datenschutzbeauftragten nach Maßgabe der beruflichen Qualifikation und insbesondere des Fachwissens, das dieser auf dem Gebiet des Datenschutzrechts und der	

einschlägigen Praktiken besitzt, sowie nach Maßgabe von dessen Fähigkeit zur Erfüllung der in Artikel 37 genannten Aufgaben. Der Grad des erforderlichen Fachwissens richtet sich insbesondere nach der Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten.	
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass etwaige sonstige berufliche Pflichten des Datenschutzbeauftragten mit den Aufgaben und Pflichten, die diesem in seiner Funktion als Datenschutzbeauftragter obliegen, vereinbar sind und zu keinen schwerwiegenden Interessenkonflikten führen.	Eine völlige Interessenkonfliktfreiheit ist gerade bei kleineren Unternehmen nicht generell ausschließbar. Es sollte ausreichen, durch geeignete innerorganisatorische Maßnahmen mögliche Interessenkonflikte weit möglichst auszuschließen.
7. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter benennt einen Datenschutzbeauftragten ~~für einen Zeitraum von mindestens zwei Jahren. Der Datenschutzbeauftragte kann für weitere Amtszeiten wiederernannt werden. Während seiner Amtszeit kann d~~Der Datenschutzbeauftragte kann, auch auf Verlangen der Aufsichtsbehörde, seines Postens nur enthoben werden, wenn er die Voraussetzungen für die Erfüllung seiner Pflichten nicht mehr erfüllt oder er nach arbeitsrechtlichen Gründen oder bei einem externen Datenschutzbeauftragten aus vertraglichen Gründen außerordentlich gekündigt werden kann.	Eine Befristung der Bestellung des internen Datenschutzbeauftragten birgt die Gefahr, dass die betreffende Person nicht in der erforderlichen betriebsinternen Unabhängigkeit wirken kann. Vielmehr sollte die Bestellung unbefristet sein und ggf. statt dessen die Abbestellungsgründe konkretisiert werden (entsprechend § 4f BDSG).
8. Der Datenschutzbeauftragte kann durch den für die Verarbeitung Verantwortlichen oder durch den Auftragsverarbeiter beschäftigt werden oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.	Zu begrüßen ist, dass die Bestellung externer Datenschutzbeauftragter nach wie vor zulässig ist.
9. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter teilt der Aufsichtsbehörde und der Öffentlichkeit den Namen und die Kontaktdaten des Datenschutzbeauftragten	

mit.	
10. Betroffene Personen haben das Recht, den Datenschutzbeauftragten zu allen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten stehenden Fragen zu Rate zu ziehen und die Wahrnehmung ihrer Rechte gemäß dieser Verordnung zu beantragen.	
~~11. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 Buchstabe c genannte Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sowie die Kriterien für die berufliche Qualifikation des in Absatz 5 genannten Datenschutzbeauftragten festzulegen.~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
Artikel 36 ***Stellung des Datenschutzbeauftragten***	
1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.	
2. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte seinen Pflichten und Aufgaben unabhängig nachkommen kann und keine Anweisungen bezüglich der Ausübung seiner Tätigkeit erhält. Der Datenschutzbeauftragte ist~~berichtet~~ unmittelbar der Leitung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters zu unterstellen.	Entsprechen dem BDSG ist der Datenschutzbeauftragte unmittelbar der Geschäftsleitung zu unterstellen.
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben und stellt das	

erforderliche Personal, die erforderlichen Räumlichkeiten, die erforderliche Ausrüstung und alle sonstigen Ressourcen, die für die Erfüllung der in Artikel 37 genannten Pflichten und Aufgaben erforderlich sind, zur Verfügung.	
Artikel 37 ***Aufgaben des Datenschutzbeauftragten***	
1. Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieser Verordnung und anderer Vorschriften über den Datenschutz hin. Soweit für den Schutz personenbezogener Daten beim für die Verarbeitung Verantwortlichen oder beim Auftragsdatenverarbeiter geboten, betraut der ~~Der~~ für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter ~~betraut~~ den Datenschutzbeauftragten hierzu mit ~~mindestens~~ folgenden Aufgaben:	Die Regelung lehnt sich an § 4g Abs. 1 Satz 1 BDSG an. Sie ermöglicht die Einhaltung datenschutzrechtlicher Vorschriften unter Berücksichtigung der individuellen Strukturen und Abläufe in den Unternehmen.
a) ~~Unterrichtung und~~ Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters über dessen aus dieser Verordnung erwachsenden Pflichten ~~sowie Dokumentation dieser Tätigkeit und der erhaltenen Antworten~~;	Die Rechte und Pflichten ergeben sich aus der Verordnung, hierüber ist keine gesonderte Unterrichtung im Unternehmen erforderlich. Eine verpflichtende Dokumentation der Beratungstätigkeit stellt eine erhebliche Bürokratisierung dar und ist daher zu streichen.
b) Überwachung der Umsetzung und Anwendung der Strategien des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter ~~und der diesbezüglichen Überprüfungen~~;	Eine Schulung der Mitarbeiter ist ausreichend.
c) Überwachung der Umsetzung und Anwendung dieser Verordnung, insbesondere ihrer Anforderungen an einen Datenschutz durch Technik und an datenschutzfreundliche Voreinstellungen, an die Datensicherheit, an die Benachrichtigung der betroffenen Personen und an die Anträge der betroffenen Personen zur Wahrnehmung der ihren nach	

dieser Verordnung zustehenden Rechte;	
d) Überwachung~~Sicherstellung~~, dass die in Artikel 28 genannte Dokumentation vorgenommen wird;	Die Erstellung der Dokumentaion ist originäre Aufgabe des für die Verarbeitung Verantwortlichen. Der Datenschutzbeauf-tragte kann die Erstellung nur überprüfen.
e) Überwachung der Dokumentation und Meldung von Verletzungen des Schutzes personenbezogener Daten sowie die Benachrichtigung davon gemäß den Artikeln 31 und 32;	Siehe Kommentierung zu Artikeln 31 und 32.
f) Überwachung der von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter durchgeführten Datenschutz-Folgenabschätzung sowie der Beantragung einer vorherigen Genehmigung beziehungsweise Zurateziehung gemäß den Artikeln 33 und 34;	Siehe Kommentierung zu Artikeln 33 und 34.
g) Überwachung der ~~auf Anfrage der Aufsichtsbehörde ergriffenen Maßnahmen sowie~~ Zusammenarbeit im Rahmen der Zuständigkeiten des Datenschutzbeauftragten mit der Aufsichtsbehörde auf deren Ersuchen oder auf eigene Initiative des Datenschutzbeauftragten;	Klarstellung. Gleichklang mit (h).
(h) Tätigkeit als Ansprechpartner für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen sowie gegebenenfalls Zurateziehung der Aufsichtsbehörde auf eigene Initiative.	
~~2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Aufgaben, die Zertifizierung, die Stellung, die Befugnisse und die Ressourcen des in Absatz 1 genannten Datenschutzbeauftragten festzulegen.~~	Die Kodifizierung von Zulässigkeitstat-beständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.

ABSCHNITT 5
VERHALTENSREGELN UND ZERTIFIZIERUNG

Artikel 38 ***Verhaltensregeln***	
1. Die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen und sich insbesondere auf folgende Aspekte beziehen:	
a) faire und transparente Datenverarbeitung,	
b) Datenerhebung,	
c) Unterrichtung der Öffentlichkeit und der betroffenen Personen;	
d) von betroffenen Personen in Ausübung ihrer Rechte gestellte Anträge;	
e) Unterrichtung und Schutz von Kindern;	
f) Datenübermittlung in Drittländer oder an internationale Organisationen;	
g) Mechanismen zur Überwachung und zur Sicherstellung der Einhaltung der Verhaltensregeln durch die diesen unterliegenden für die Verarbeitung Verantwortlichen;	
(h) außergerichtliche Verfahren und sonstige Streitschlichtungsverfahren zur Beilegung von Streitigkeiten zwischen für die Verarbeitung Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten unbeschadet der den betroffenen Personen aus den Artikeln 73 und 75 erwachsenden Rechte.	
2. Berufsv~~V~~erbände und andere Vereinigungen ~~Einrichtungen~~, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in einem Mitgliedstaat vertreten	Zu Satz 1: Entsprechend Art. 27 Abs. 1 Richtlinie 95/46/EG sowie § 38a des deutschen BDSG sollte klargestellt werden, dass die

und beabsichtigen, eigene Verhaltensregeln aufzustellen oder bestehende Verhaltensregeln zu ändern oder zu erweitern, können diesbezügliche Vorschläge der Aufsichtsbehörde in dem betreffenden Mitgliedstaat zur Stellungnahme vorlegen. Die Aufsichtsbehörde hat~~kann~~ zu der Frage Stellung zu nehmen, ob der betreffende Entwurf von Verhaltensregeln beziehungsweise der Änderungsvorschlag mit dieser Verordnung vereinbar ist. Die Aufsichtsbehörde holt die Stellungnahmen der ~~hört die~~ betroffenen Personen oder ihrer Vertreter zu diesen Vorschlägen ein, falls ihr dies angebracht erscheint ~~an~~.	Verhaltensregeln nur aus dem Kreis der verantwortlichen Stellen entwickelt werden können sollen. Zu Satz 2: Die Aufsichtsbehörde sollte verpflichtet sein, eine Stellungnahme abzugeben. Ansonsten besteht die Gefahr, dass das Verfahren ergebnislos bleibt. Zu Satz 3: Entsprechend Art. 27 Abs. 2 der Richtlinie 95/46/EG sollte für die Aufsichtsbehörde keine Pflicht bestehen, Vertreter von betroffenen Personen zu hören.
3. BerufsV~~V~~erbände und andere Vereinigungen ~~Einrichtungen~~, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in mehreren Mitgliedstaaten vertreten, können dem Europäischen Datenschutzausschuss ~~der Kommission~~ Entwürfe von Verhaltensregeln sowie Vorschläge zur Änderung oder Ausweitung bestehender Verhaltensregeln vorlegen. Der Ausschuss nimmt insbesondere dazu Stellung, ob die ihm unterbreiteten Entwürfe mit den Regelungen dieser Verordnung in Einklang stehen. Er holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihm dies angebracht erscheint. Die Kommission hat dafür Sorge zu tragen, dass die Verhaltensregeln, zu denen der Ausschuss eine positive Stellungnahme abgegeben hat, in geeigneter Weise veröffentlicht werden.	Folgeänderung zu Abs. 2. Darüber hinaus sollte Art. 27 Abs. 3 der Richtlinie 95/46/EG hier Berücksichtigung finden.
~~4. Die Kommission kann im Wege einschlägiger Durchführungsrechtsakte beschließen, dass die ihr gemäß Absatz 3 vorgeschlagenen Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender Verhaltensregeln allgemeine Gültigkeit in der Union besitzen. Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.~~	Absatz 4 sollte gestrichen werden, da über Absatz 4 Verhaltensregeln quasi verbindlichen Gesetzescharakter erhalten könnten, ohne den üblichen Gesetzgebungsprozess durchlaufen zu müssen. Es ist zu gewährleisten, dass alle Interessengruppen im Rahmen von Konsultationsverfahren gehört werden. Absatz 4 könnte diesen Prozess konterkarieren.
~~5. Die Kommission trägt dafür Sorge, dass die Verhaltensregeln, denen gemäß Absatz 4 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise~~	Folgeänderung zu Absatz 3.

~~veröffentlicht werden.~~	
Artikel 39 ***Zertifizierung***	
1. Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von freiwilligen datenschutzspezifischen Zertifizierungsverfahren unter Berücksichtigung der Datensicherheit sowie von Datenschutzsiegeln und –zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung.	1. Die Zertifizierung sollte freiwillig sein. Zudem sollte eine Zertifizierung auch den technischen Schutz von Daten (Datensicherheit) umfassen. 2. Die Einführung datenschutzrechtlicher Zertifikate bietet nur dort einen Mehrwert, wo Unternehmen Dienstleistungen erbringen, die in besonderer Weise datenschutzrechtlich relevant sind (z. B. gewerbliche Auftragsdatenverarbeiter). Eine Erstreckung auf andere Branchen würde eher zur Verunsicherung der Verbraucher und zur wirtschaftlichen Belastung kleinerer und mittlerer Unternehmen führen, die sich aus Marktdruck gezwungen sähen, den Zertifizierungsprozess zu durchlaufen. Die Deutsche Kreditwirtschaft sieht auch insbesondere für ihren Tätigkeitsbereich keinen Bedarf für ein „Datenschutz-Siegel“, da sich alle Banken und Sparkassen vertraglich zur Wahrung des Bankgeheimnisses verpflichtet haben, welches heute bereits höchstes Vertrauen der Kunden genießt. 3. Zu kritisieren ist, dass mit einer Zertifizierung bzw. der Vergabe eines Datenschutzsiegels in der hier vorgesehenen Art und Weise kein datenschutz-rechtlicher Mehrwert verbunden ist. Die Einführung eines Zertifizierungsverfahrens würde insbesondere kleiner und mittlere Unternehmen erheblich belasten, da diese die Kosten für ein solches Verfahren in der Regel nicht tragen können. Daher muss für die Unternehmen ein Anreiz geschaffen werden, sich einer Zertifizierung zu

	unterziehen oder ein Datenschutzsiegel zu erwerben. Ein solcher Anreiz könnte beispielsweise darin bestehen, dass eine Genehmigung eines Verarbeitungsvorgangs durch die Ausichtsbehörde entbehrlich ist, sich eine Datenschutzfolgenabschätzung erübrigt oder Informationspflichten, Dokumentationspflichten und eigene Prüfpflichten (z.B. gegenüber dem Auftragsdatenverarbeiter) entfallen. 4. Der in Erwägungsgrund 77 angedachte Aspekt der „Steuerung" der Verbraucher hin zur Nutzung datenschutzgepürfter Anbieter steht im Konflikt mit dem im UWG verorteten Grundsatz, dass mit der bloßen Einhaltung gesetzlicher Vorschriften nicht geworben werden darf. Schließlich ist festzuhalten, dass die Verantwortlichen zur Einhaltung datenschutzrechtlicher Vorgaben ohnehin verpflichtet sind.
~~2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen.~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
3. Die Kommission kann <u>unter Einbeziehung der betroffenen Kreise</u> technische <u>und organisatorische</u> Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -zeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -zeichen <u>entwickeln.</u>~~festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.~~	Unter Einbeziehung aller betroffenen Kreise sollte es möglich sein Standards einvernehmlich zu entwickeln.

KAPITEL V
ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

Artikel 40 ***Allgemeine Grundsätze der Datenübermittlung***	
Jedwede Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung in ein Drittland oder an eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der für die Verarbeitung Verantwortliche und der von ihm eingebundene~~der~~ Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weitergabe personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation.	Es sollte klargestellt werden, dass ein Auftragsverarbeiter keine eigenen Rechte an den Daten hat.
Artikel 41 ***Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses***	
1. Eine Datenübermittlung darf vorgenommen werden, wenn die Kommission festgestellt hat, dass das betreffende Drittland beziehungsweise ein Gebiet oder Behörde oder ein Verarbeitungssektor dieses Drittlands oder die betreffende internationale Organisation einen angemessenen Schutz bietet. Derartige Datenübermittlungen bedürfen keiner weiteren Genehmigung. Verbände und andere Einrichtungen, die Interessen von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in einem Mitgliedstaat vertreten, sind berechtigt, die Prüfung der Angemessenheit durch die Kommission zu beantragen.	Im Rahmen der Datenübermittlung zu beispielsweise steuerlichen Interessen von Drittstaaten könnte die Kommission die Angemessenheit einer im Drittstaat ansässigen Behörde feststellen. Durch ein Antragsrecht auf Prüfung der Angemessenheit können wirtschaftliche Belange angemessen berücksichtigt werden, um die Wettbewerbsfähigkeit der in der EU ansässigen Unternehmen zu sichern.
2. Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission	
a) die Rechtsstaatlichkeit, die geltenden allgemeinen und sektorspezifischen Vorschriften,	Folgeänderung zu Absatz 1.

insbesondere über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, die in dem betreffenden Land beziehungsweise der betreffenden internationalen Organisation und Behörde geltenden Standesregeln und Sicherheitsvorschriften sowie die Existenz wirksamer und durchsetzbarer Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen und insbesondere für in der Union ansässige betroffene Personen, deren personenbezogene Daten übermittelt werden;	
b) die Existenz und die Wirksamkeit einer oder mehrerer in dem betreffenden Drittland beziehungsweise in der betreffenden internationalen Organisation tätiger unabhängiger Aufsichtsbehörden, die für die Einhaltung der Datenschutzvorschriften, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Union und der Mitgliedstaaten zuständig sind, und	
c) die von dem betreffenden Drittland beziehungsweise der internationalen Organisation oder Behörde eingegangenen internationalen Verpflichtungen.	Folgeänderung zu Absatz 1.
3. Die Kommission kann durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor oder Behörde eines Drittlands oder eine internationale Organisation einen angemessenen Schutz im Sinne von Absatz 2 bietet. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	Folgeänderung zu Absatz 1.
4. In jedem Durchführungsrechtsakt werden der geografische und der sektorielle Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte Aufsichtsbehörde angegeben.	
5. Die Kommission kann durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor oder Behörde eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne von Absatz 2 dieses Artikels bietet; dies gilt insbesondere für Fälle, in denen die in dem betreffenden Drittland	Folgeänderung zu Absatz 1.

beziehungsweise der betreffenden internationalen Organisation oder Behörde geltenden allgemeinen und sektorspezifischen Vorschriften keine wirksamen und durchsetzbaren Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für in der Union ansässige betroffene Personen und insbesondere für betroffene Personen, deren personenbezogene Daten übermittelt werden, garantieren. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 oder – in Fällen, in denen es äußerst dringlich ist, das Recht natürlicher Personen auf den Schutz ihrer personenbezogenen Daten zu wahren – nach dem in Artikel 87 Absatz 3 genannten Verfahren angenommen.	
6. Wenn die Kommission die in Absatz 5 genannte Feststellung trifft, wird dadurch jedwede Übermittlung personenbezogener Daten an das betreffende Drittland beziehungsweise an ein Gebiet oder einen Verarbeitungssektor oder eine Behörde in diesem Drittland oder an die betreffende internationale Organisation unbeschadet der Bestimmungen der Artikel 42 bis 434 untersagt. Die Kommission nimmt zu unverzüglich ~~geeigneter Zeit~~ Beratungen mit dem betreffenden Drittland beziehungsweise mit der betreffenden internationalen Organisation oder der Behörde auf, um Abhilfe für die Situation, die aus dem gemäß Absatz 5 erlassenen Beschluss entstanden ist, zu schaffen.	Folgeänderung zu Absatz 1. Das Verbot der Übermittlung in einen Drittstaat nach Absatz 5 darf nicht die Ausnahmevorschrift des Artikel 44 umfassen. Ansonsten würde der betreffende Drittstaat u.a. vom Zahlungsverkehr abgeschnitten, denn der Bank wäre es verboten, die Überweisungsdaten in den betreffenden Staat zu übermitteln.
7. Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* eine Liste aller Drittländer beziehungsweise Gebiete und Verarbeitungssektoren und Behörde von Drittländern und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese einen beziehungsweise keinen angemessenen Schutz personenbezogener Daten bieten.	
8. Sämtliche von der Kommission auf der Grundlage von Artikel 25 Absatz 6 oder Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassenen Beschlüsse bleiben so lange in Kraft, bis sie von der Kommission geändert, ersetzt oder aufgehoben werden.	

Artikel 42 ***Datenübermittlung auf der Grundlage geeigneter Garantien***	
1. Hat die Kommission keinen Beschluss nach Artikel 41 erlassen, darf ein für die Verarbeitung Verantwortlicher oder ein von ihm eingebundener Auftragsverarbeiter personenbezogene Daten in ein Drittland oder an eine internationale Organisation oder Behörde übermitteln, sofern er in einem rechtsverbindlichen Instrument geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.	Folgeänderung zu Artikel 41 Absatz 1. Klarstellung, dass der Auftragsverarbeiter nur nach Weisung des Auftraggebers handelt.
2. Die in Absatz 1 genannten geeigneten Garantien können insbesondere bestehen in Form	
a) verbindlicher unternehmensinterner Vorschriften nach Artikel 43;	
b) von der Kommission angenommener Standarddatenschutzklauseln, diese Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen;	
c) von einer Aufsichtsbehörde nach Maßgabe des in Artikel 57 beschriebenen Kohärenzverfahren angenommener Standarddatenschutzklauseln, sofern diesen von der Kommission allgemeine Gültigkeit gemäß Artikel 62 Absatz 1 Buchstabe b zuerkannt wurde, oder	
d) von Vertragsklauseln, die zwischen dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter und dem Empfänger vereinbart und von einer Aufsichtsbehörde gemäß Absatz 4 genehmigt wurden.	
3. Datenübermittlungen, die nach Maßgabe der in Absatz 2 Buchstabe a, b und c genannten unternehmensinternen Vorschriften und Standarddatenschutzklauseln erfolgen, bedürfen keiner weiteren Genehmigung.	
4. Für Datenübermittlungen nach Maßgabe der in Absatz 2 Buchstabe d dieses Artikels genannten Vertragsklauseln holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die	

vorherige Genehmigung der Aufsichtsbehörde gemäß Artikel 34 Absatz 1 Buchstabe a ein. Falls die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche Personen in einem oder mehreren anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung.	
5. Wenn keine geeigneten Garantien für den Schutz personenbezogener Daten in einem rechtsverbindlichen Instrument vorgesehen werden und keine Ausnahme nach Artikel 44 vorliegt, holt der für die Verarbeitung Verantwortliche oder der von ihm eingebundene Auftragsverarbeiter die vorherige Genehmigung für die Übermittlung oder Kategorie von Übermittlungen oder für die Aufnahme von entsprechenden Bestimmungen in die Verwaltungsvereinbarungen ein, die die Grundlage für eine solche Übermittlung bilden. Derartige vorherige Genehmigungen der Aufsichtsbehörde müssen im Einklang mit Artikel 34 Absatz 1 Buchstabe a stehen. Falls die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche Personen in einem oder mehreren anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung. Sämtliche von einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilten Genehmigungen bleiben so lange in Kraft, bis sie von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden.	Klarstellung, dass bei Vorliegen eines Ausnahmefalls nach Artikel 44, keine Vorabgenehmigung der Aufsichtsbehörde erforderlich ist. Der Begriff „Verwaltungsvereinbarungen“ ist unverständlich. Die Bestandschutzregel ist sehr wichtig, damit bislang legale Datenübermittlungen nicht in Frage gestellt werden.
Artikel 43 ***Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften***	
1. Eine Aufsichtsbehörde kann nach Maßgabe des in Artikel 58 beschriebenen Kohärenzverfahrens verbindliche unternehmensinterne Vorschriften genehmigen, sofern diese	
a) rechtsverbindlich sind, für alle Mitglieder der Unternehmensgruppe des für die Verarbeitung	

Verantwortlichen oder des von ihm eingebundenen Auftragsverarbeiters sowie deren Beschäftigte gelten und von diesen Mitgliedern angewendet werden;	
b) die Durchsetzbarkeit der Rechte der ~~den~~ betroffenen Personen ausdrücklich regeln ~~durchsetzbare Rechte übertragen~~;	Klarstellung.
c) die in Absatz 2 festgelegten Anforderungen erfüllen.	
2. Alle verbindlichen unternehmensinternen Vorschriften enthalten mindestens folgende Informationen:	
a) Struktur und Kontaktdaten der Unternehmensgruppe und ihrer Mitglieder;	
b) die betreffenden Datenübermittlungen oder Datenübermittlungskategorien einschließlich der betreffenden Kategorien personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;	
c) interne und externe Rechtsverbindlichkeit der betreffenden unternehmensinternen Vorschriften;	
d) die allgemeinen Datenschutzgrundsätze, zum Beispiel Zweckbegrenzung, die Datenqualität, die Rechtsgrundlage für die Verarbeitung sowie die Bestimmungen für etwaige Verarbeitungen sensibler personenbezogener Daten, Maßnahmen zur Sicherstellung der Datensicherheit und die Anforderungen für die Datenweitergabe an nicht an diese Vorschriften gebundene Organisationen;	
e) soweit dies nach der Rechtsordnung des jeweiligen Drittstaats zulässig ist, die Rechte der betroffenen Personen nach dieser Verordnung und die diesen offen stehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, keiner einer Profilerstellung dienenden Maßnahme nach Artikel 20 unterworfen zu werden sowie des in Artikel 75 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen unternehmensinternen	1. Redundant zu Absatz 1b). 2. Die Rechtsordnungen des Drittstaates müssen Berücksichtigung finden.

Vorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;	
f) die von dem in einem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße von nicht in der Union niedergelassenen Mitgliedern der Unternehmensgruppe gegen die verbindlichen unternehmensinternen Vorschriften; der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;	
g) die Art und Weise, wie die betroffenen Personen gemäß Artikel 11 über die ihnen nach den verbindlichen unternehmensinternen Vorschriften übertragenen durchsetzbaren Rechte. ~~und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte~~ informiert werden~~;~~	Aus Transparenzgründen sollten den Betroffenen lediglich die Ihnen übertragenen durchsetzbaren Rechte mitgeteilt werden. Darüber hinausgehende Informationsverpflichtungen wären unverhältnismäßig und würden zu einer Überinformation des Betroffene führen.
(h) die Aufgaben des gemäß Artikel 35 benannten Datenschutzbeauftragten einschließlich der Überwachung der Einhaltung der verbindlichen unternehmensinternen Vorschriften in der Unternehmensgruppe sowie die Überwachung der Schulungsmaßnahmen und den Umgang mit Beschwerden;	
i) die innerhalb der Unternehmensgruppe bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen unternehmensinternen Vorschriften;	
~~j) die Verfahren für die Meldung und Erfassung von Änderungen der Unternehmenspolitik und ihre Meldung an die Aufsichtsbehörde~~;	Unternehmenspolitik ist kein relevanter Anknüpfungspunkt für datenschutzrechtliche Vorschriften.
k) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe gewährleisten, wie insbesondere die Offenlegung der Ergebnisse der Überprüfungen der unter Buchstabe i	

dieses Absatzes genannten Maßnahmen gegenüber der Aufsichtsbehörde.	
3. ~~Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels und insbesondere die Kriterien für deren Genehmigung und für die Anwendung von Absatz 2 Buchstaben b, d, e, und f auf verbindliche unternehmensinterne Vorschriften von Auftragsverarbeitern sowie weitere erforderliche Anforderungen zum Schutz der personenbezogenen Daten der betroffenen Personen festzulegen.~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
~~4. Die Kommission kann das Format und Verfahren für den auf elektronischem Wege erfolgenden Informationsaustausch über verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels zwischen für die Verarbeitung Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.~~	
Artikel 44 ***Ausnahmen***	
1. Falls <u>kein angemessenes Datenschutzniveau</u> ~~weder ein Angemessenheitsbeschluss~~ nach Artikel 41 ~~vorliegt noch geeignete Garantien nach~~ <u>oder</u> Artikel 42 besteht~~en~~, ist eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation <u>oder Behörde</u> nur zulässig, wenn <u>a) die Übermittlung zur Erfüllung einer gesetzlichen Verpflichtung oder Erlaubnis, einer aufsichtsrechtlichen Anforderung oder einer anderen Rechtsvorschrift erforderlich ist, der der für die Verarbeitung Verantwortliche unterliegt,</u>	Folgeänderung zu Artikel 41 Absatz 1. Klarstellung, dass die Ausnahmen einschlägig sind, wenn ein Nichtangemessenheitsbeschluss nach Artikel 41 Absatz 5 vorliegt. Vgl. Kommentierungen zu Artikel 6 Absatz 1 c).
<u>b~~a~~)</u> die betroffene Person der vorgeschlagenen Datenübermittlung zugestimmt hat, nachdem sie <u>darüber informiert worden ist, dass in dem Drittland, bei der internationalen Organisation oder bei der Behörde kein dem dieser Verordnung entsprechendes</u>	Eine Information des Betroffenen kann sich allenfalls auf den Umstand beschränken, dass in dem Drittland kein der Verordnung entsprechendes Datenschutzniveau

Datenschutzniveau besteht, ~~über die Risiken derartiger ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete durchgeführter Datenübermittlungen informiert wurde~~,	existiert. Darüber hinaus gehende Informationen sind dem Verantwortlichen unmöglich.
c~~b~~) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist,	
d~~c~~) die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist,	
e~~d~~) die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist,	
f~~e~~) die Übermittlung zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich ist,	
g~~f~~) die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,	
h~~g~~) die Übermittlung aus einem Register erfolgt, das gemäß dem Unionsrecht oder dem mitgliedstaatlichen Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die im Unionsrecht oder im mitgliedstaatlichen Recht festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind, oder	
(i~~h~~) die Übermittlung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder vom ~~Auftragsverarbeiter~~ Empfänger wahrgenommen wird, erforderlich ist und nicht als häufig oder massiv bezeichnet werden kann, und falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter alle Umstände beurteilt hat, die bei	In die vorzunehmende Interessensabwägung sollte auch das berechtigte Interesse des Empfängers der personenbezogenen Daten einbezogen werden, vgl. Kommentierung zu Artikel 6 Absatz 1 f) VO-E sowie Artikel 7f) der

einer Datenübermittlung oder bei einer Kategorie von Datenübermittlungen eine Rolle spielen, und gegebenenfalls auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat. Liegt ein Beschluss nach Artikel 41 Absatz 5 vor, ist regelmäßig davon auszugehen, dass die Interessen des Betroffenen einer Datenübermittlung entgegenstehen.	Richtlinie 95/46/EG.
2. Datenübermittlungen gemäß Absatz 1 Buchstabe hg dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.	
3. Bei Datenverarbeitungen gemäß Absatz 1 Buchstabe ih berücksichtigt der für die Verarbeitung Verantwortliche ~~oder der Auftragsverarbeiter~~ insbesondere die Art der Daten, die Zweckbestimmung und die Dauer der geplanten Verarbeitung, die Situation im Herkunftsland, in dem betreffenden Drittland und im Endbestimmungsland sowie ~~erforderlichenfalls~~ etwaige vorgesehene geeignete Garantien zum Schutz personenbezogener Daten, wenn erforderlich.	Folgeänderung zu Absatz 1 i). Was bedeutet „Endbestimmungsland“?
4. Absatz 1 Buchstaben cb, de und ih gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.	
5. Das in Absatz 1 Buchstabe ed genannte öffentliche Interesse muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein.	
6. Der für die Verarbeitung Verantwortliche oder der von ihm eingebundene Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die in Absatz 1 Buchstabe ih dieses Artikels genannten geeigneten Garantien in der Dokumentation gemäß Artikel 28 und setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis.	
~~7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die in Absatz 1 Buchstabe d genannten „wichtigen~~	Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und

~~Gründe des öffentlichen Interesses" zu präzisiseren und die Kriterien und Anforderungen für die geeigneten Garantien im Sinne des Absatzes 1 Buchstabe h festzulegen.~~	nicht auf die Kommission übertragen werden. Da sich die vielfältigen Lebenssachverhalte regelmäßig nicht regulatorisch erfassen lassen sollte die konkrete Bewertung im Einzelfall weiterhin maßgeblich sein.
Artikel 45 ***Internationale Zusammenarbeit zum Schutz personenbezogener Daten***	
1. In Bezug auf Drittländer und internationale Organisationen sowie Behörden treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur	
a) Entwicklung wirksamer Mechanismen der internationalen Zusammenarbeit, durch die die Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,	
b) gegenseitigen Leistung internationaler Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch Mitteilungen, Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und Grundfreiheiten bestehen,	
c) Einbindung maßgeblich Beteiligter in Diskussionen und Tätigkeiten, die zum Ausbau der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften über den Schutz personenbezogener Daten dienen,	
d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten.	
2. Zu den in Absatz 1 genannten Zwecken ergreift die Kommission geeignete Maßnahmen zur Förderung der Beziehungen zu Drittländern und internationalen Organisationen und insbesondere zu deren Aufsichtsbehörden, wenn sie gemäß Artikel 41 Absatz 3 durch Beschluss festgestellt hat, dass diese	

einen angemessenen Schutz bieten.	

KAPITEL VI
UNABHÄNGIGE AUFSICHTSBEHÖRDEN

ABSCHNITT 1
UNABHÄNGIGKEIT

Artikel 46 ***Aufsichtsbehörde***	
1. Jeder Mitgliedstaat trägt dafür Sorge, dass eine ~~oder mehrere~~ Behörde~~n~~ für die Überwachung der Anwendung dieser Verordnung zuständig ist~~sind~~ und einen Beitrag zur ihrer einheitlichen Anwendung in der gesamten Union leiste~~n~~, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer Daten geschützt und der freie Verkehr dieser Daten in der Union erleichtert werden. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.	Die Anpassungen sind unter Berücksichtigung der heutigen Situation in den anderen EU-Mitgliedstaaten, die nur eine einzige nationale Aufsichtsbehörde kennen, erforderlich, um eine einheitliche Rechts- und Verwaltungspraxis in den Mitgliedstaaten sicherzustellen und damit dem Vollharmonisierungs-ansatz der Verordnung Rechnung zu tragen. Beließe man in Deutschland die föderale Struktur auf Landesebene, müsste aus der Logik der Verordnung ein nationales Kohärenzverfahren etabliert werden.
~~2. Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die als zentrale Kontaktstelle für die wirksame Beteiligung dieser Behörden im Europäischen Datenschutzausschuss fungiert und führt ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 57 einhalten.~~	Folgeänderung zu Absatz 1.
2~~3~~. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften, die er aufgrund dieses Kapitels erlässt, sowie unverzüglich alle folgenden Änderungen dieser Vorschriften mit.	

Artikel 47 ***Unabhängigkeit***	Die Unabhängigkeit der jeweiligen Aufsichtsbehörde (Artikel 47) sollte nicht durch Zuweisung von Aufsichtsbefugnissen an die Europäische Kommission unterlaufen werden.
1. Die Aufsichtsbehörde nimmt die ihr zugewiesenen Aufgaben fachlich unabhängig wahr. ~~handelt bei der Erfüllung der ihr übertragenen Aufgaben und Befugnisse völlig unabhängig.~~	Vgl. Artikel 28 Absatz 1 der EU-Datenschutzrichtlinie.
~~2.~~ Die Mitglieder der Aufsichtsbehörde ersuchen in Ausübung ihres Amtes weder um Weisung noch nehmen sie Weisungen entgegen.	Es ist unklar, wie sich das Personal der Aufsichtsbehörde zusammensetzt. In der Verordnung werden die Begriffe „Mitglieder“, „Leiter der Aufsichtsbehörde“ und „Personal“ mit unterschiedlichen Bestellungsvoraussetzungen benannt. Eine völlige interne Weisungsfreiheit für Mitarbeiter einer Verwaltungsbehörde widerspricht rechtsstaatlichen Grundsätzen (vgl. Absatz 6, unten).
3. Die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.	
4. Die Mitglieder der Aufsichtsbehörde verhalten sich nach Ablauf ihrer Amtszeit im Hinblick auf die Annahme von Tätigkeiten und Vorteilen ehrenhaft und zurückhaltend.	
5. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde mit angemessenen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und mit der erforderlichen Infrastruktur ausgestattet wird, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Europäischen Datenschutzausschuss effektiv wahrnehmen zu können.	
6. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde über eigenes Personal verfügt, das	Unklar ist die Position des „Leiters der Aufsichtsbehörde“ im Verhältnis

vom Leiter der Aufsichtbehörde ernannt wird und seiner Leitung untersteht.	zu den „Mitgliedern“ der Aufsichtsbehörde.
7. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Die Mitgliedstaaten sorgen dafür, dass die Aufsichtsbehörde über einen eigenen jährlichen Haushalt verfügt. Die Haushaltspläne werden veröffentlicht.	
Artikel 48 ***Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde***	
1. Die Mitgliedstaaten tragen dafür Sorge, dass die Mitglieder der Aufsichtsbehörde entweder vom Parlament oder von der Regierung des betreffenden Mitgliedstaats ernannt werden.	
2. Die Mitglieder werden aus einem Kreis von Personen ausgewählt, an deren Unabhängigkeit kein Zweifel besteht, und die nachweislich über die für die Erfüllung ihrer Aufgaben erforderliche Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.	
3. Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder seiner Enthebung aus dem Amt gemäß Absatz 4.	
4. Ein Mitglied kann vom zuständigen nationalen Gericht seines Amtes enthoben oder seiner Ruhegehaltsansprüche oder an ihrer Stelle gewährten Vergünstigungen für verlustig erklärt werden, wenn es die Voraussetzungen für die Ausübung seines Amtes nicht mehr erfüllt oder eine schwere Verfehlung begangen hat.	
5. Endet die Amtszeit des Mitglieds oder tritt es zurück, übt es sein Amt so lange weiter aus, bis ein neues Mitglied ernannt ist.	
Artikel 49 ***Errichtung der Aufsichtsbehörde***	
Jeder Mitgliedstaat regelt durch Gesetz in den	

Grenzen dieser Verordnung	
a) die Errichtung der Aufsichtsbehörde und ihre Stellung,	
b) die Qualifikation, Erfahrung und fachliche Eignung, die für die Wahrnehmung der Aufgaben eines Mitglieds der Aufsichtsbehörde notwendig ist,	
c) die Vorschriften und Verfahren für die Ernennung der Mitglieder der Aufsichtsbehörde und zur Bestimmung der Handlungen und Tätigkeiten, die mit dem Amt unvereinbar sind,	
d) die Amtszeit der Mitglieder der Aufsichtsbehörde, die mindestens vier Jahre beträgt; dies gilt nicht für die erste Amtszeit nach Inkrafttreten dieser Verordnung, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist;	
e) ob die Mitglieder der Aufsichtsbehörde wiederernannt werden können,	
f) die Regelungen und allgemeinen Bedingungen für das Amt eines Mitglieds und die Aufgaben der Bediensteten der Aufsichtsbehörde,	
g) die Regeln und Verfahren für die Beendigung der Amtszeit der Mitglieder der Aufsichtsbehörde, auch für den Fall, dass sie die Voraussetzungen für die Ausübung ihres Amtes nicht mehr erfüllen oder eine schwere Verfehlung begangen haben.	
Artikel 50 ***Verschwiegenheitspflicht***	
Die Mitglieder, der Leiter und Bediensteten der Aufsichtsbehörde sind während ihrer Amts- beziehungsweise Dienstzeit und auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben bekannt geworden sind, Verschwiegenheit zu bewahren.	Die Verschwiegenheitspflicht sollte auch den Leiter umfassen.

ABSCHNITT 2
AUFGABEN UND BEFUGNISSE

Artikel 51 ***Zuständigkeit***	
1. Jede Aufsichtsbehörde übt im Hoheitsgebiet ihres Mitgliedstaats die ihr mit dieser Verordnung übertragenen Befugnisse aus.	
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 Aufsichtbehörde 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.	
3. Die Aufsichtsbehörde ist nicht zuständig für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen.	
Artikel 52 ***Aufgaben***	
1. Aufgaben der Aufsichtsbehörde sind	
a) die Überwachung und Gewährleistung der Anwendung dieser Verordnung,	
b) die Befassung mit Beschwerden betroffener Personen ~~oder von Verbänden, die diese Personen gemäß Artikel 73 vertreten~~, die Untersuchung der Angelegenheit in angemessenem Umfang und Unterrichtung der betroffenen Personen oder Verbände über den Fortgang und das Ergebnis der Beschwerde innerhalb einer angemessenen Frist, vor allem, wenn eine weitere Untersuchung oder	Folgeänderung zu Artikel 73. Verbände sollten nur dann Beschwerden vorbringen dürfen, wenn sie hierfür von den Betroffenen bevollmächtigt worden sind.

Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,	
c) der Informationsaustausch mit anderen Aufsichtsbehörden und die Amtshilfe sowie die Gewährleistung der einheitlichen Anwendung und Durchsetzung dieser Verordnung,	
d) die Durchführung von Untersuchungen auf eigene Initiative, aufgrund einer Beschwerde oder auf Ersuchen einer anderen Aufsichtsbehörde und, falls die betroffene Person eine Beschwerde bei dieser Aufsichtsbehörde eingereicht hat, deren Unterrichtung über die Ergebnisse der Untersuchungen innerhalb einer angemessenen Frist,	
e) die Verfolgung relevanter Entwicklungen, soweit als sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere der Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken,	
f) die Beratung der Organe und Einrichtungen der Mitgliedstaaten im Hinblick auf Rechts- und Verwaltungsmaßnahmen, die den Schutz der Rechte und Freiheiten der natürlichen Personen bei der Verarbeitung personenbezogener Daten zum Gegenstand haben,	
g) die Beratung in Bezug auf die in Artikel 34 genannten Verarbeitungsvorgänge und deren Genehmigung,	
h) die Abgabe von Stellungnahmen zu den Entwürfen von Verhaltensregeln gemäß Artikel 38 Absatz 2,	
i) die Genehmigung verbindlicher unternehmensinterner Vorschriften gemäß Artikel 43,	
j) die Mitwirkung im Europäischen Datenschutzausschuss.	
2. Jede Aufsichtsbehörde fördert die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder.	

3. Die Aufsichtsbehörde berät auf Antrag jede betroffene Person bei der Wahrnehmung der ihr nach dieser Verordnung zustehenden Rechte und arbeitet zu diesem Zweck gegebenenfalls mit den Aufsichtsbehörden anderer Mitgliedstaaten zusammen. 4. Die Aufsichtsbehörde berät auf Antrag jeden für die Verarbeitung Verantwortlichen sowie jeden Auftragsverarbeiter über die Erfüllung seiner Pflichten nach dieser Verordnung.	Neue Nummer 4: Auch verarbeitende Stellen sollten von den Aufsichtsbehörden beraten werden.
5~~4~~. Für die in Absatz 1 Buchstabe b genannten Beschwerden stellt die Aufsichtsbehörde ein Beschwerdeformular zur Verfügung, das elektronisch oder auf anderem Wege ausgefüllt werden kann.	
6~~5~~. Die Leistungen der Aufsichtsbehörde sind für die betroffene Person und im Falle des Absatzes 4 kostenlos.	
7~~6~~. Bei offensichtlich missbräuchlichen Anträgen, insbesondere bei wiederholt gestellten Anträgen, kann die Aufsichtsbehörde eine Gebühr verlangen oder davon absehen, die von der betroffenen Person beantragte Maßnahme zu treffen. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offensichtlich missbräuchlichen Charakter des Antrags.	
Artikel 53 ***Befugnisse***	
1. Jede Aufsichtsbehörde ist zur Einhaltung der Vorgaben dieser Verordnung befugt,	Klarstellung.
a) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter auf einen behaupteten Verstoß gegen die Vorschriften zum Schutz personenbezogener Daten hinzuweisen und ihn gegebenenfalls anzuweisen, diesem Verstoß in einer bestimmten Weise abzuhelfen, um den Schutz der betroffenen Person zu verbessern,	
b) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu	

entsprechen,	
c) den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den RepräsentantenVertreter anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich zweckdienlich sind,	Sprachliche Klarstellung. Zudem: Folgeänderung zu Artikel 4 Absatz 14.
d) die Befolgung der Genehmigungen und Auskünfte im Sinne von Artikel 34 sicherzustellen,	
e) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter zu ermahnen oder zu verwarnen,	
f) die Berichtigung, Löschung, Sperrung oder Vernichtung aller Daten, die unter Verletzung der Bestimmungen dieser Verordnung verarbeitet wurden, anzuordnen, und solche Maßnahmen Dritten, an die diese Daten weitergegeben wurden, mitzuteilen,	
g) die Verarbeitung teilweise oder ganz vorübergehend oder endgültig zu verbieten,	Die aufsichtsbehördliche Maßnahme soll sich nach dem Verhältnismäßigkeitsgrundsatz richten.
h) die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation oder Behörde teilweise oder ganz zu unterbinden,	
i) Stellungnahmen zu allen Fragen im Zusammenhang mit dem Schutz personenbezogener Daten abzugeben,	
j) das nationale Parlament, die Regierung oder sonstige politische Institutionen sowie die Öffentlichkeit über Fragen im Zusammenhang mit dem Schutz personenbezogener Daten zu informieren.	Sollte als allgemeine behördliche Aufgabe unter Artikel 52 Absatz 1 verortet werden.
2. Jede Aufsichtsbehörde kann kraft ihrer Untersuchungsbefugnis vom für die Verarbeitung Verantwortlichen oder von dem eingebundenen Auftragsverarbeiter Folgendes verlangen:	Klarstellung.
a) EinsichtZugriff auf alle personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben erforderlichnotwendig sind,	Der Begriff „Zugriff" ist problematisch, da dieser auch eine Veränderung bzw. Mitnahme der Daten umfassen könnte. Zur Ausübung der Kontrollrechte ist ein

	solch weitgehender Eingriff nicht erforderlich.
b) Zutrittgang während der Betriebs- und Geschäftszeiten zu den Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen und -geräte, sofern Grund zu der Annahme besteht, dass dort Tätigkeiten ausgeführt werden, die gegen diese Verordnung verstoßen.	Begrenzung des Zutrittsrechts auf das in § 38 im deutschen BDSG geregelte Maß.
Die Befugnisse nach Buchstabe b werden im Einklang mit dem Unionsrecht und dem Recht des der Mitgliedstaatesn ausgeübt, in dem die von der Maßnahme betroffenen Geschäftsräume liegen.	
3. Jede Aufsichtsbehörde ist insbesondere gemäß Artikel 74 Absatz 4 und Artikel 75 Absatz 2 befugt, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Klage zu erheben.	
4. Jede Aufsichtsbehörde ist befugt, verwaltungsrechtliche Sanktionen Vergehen, insbesondere solche nach Artikel 79 Absätze 4, 5 und 6, zu verhängen.ahnden.	Gleichlauf mit dem Regelungsgehalt in Artikel 79.
Artikel 54 ***Tätigkeitsbericht***	
Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit. Der Bericht wird dem nationalen Parlament vorgelegt und der Öffentlichkeit, der Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht.	

KAPITEL VII
ZUSAMMENARBEIT UND KOHÄRENZ

ABSCHNITT 1
ZUSAMMENARBEIT

Artikel 55 ***Amtshilfe***	
1. Die Aufsichtsbehörden übermitteln einander zweckdienliche Informationen und gewähren einander Amtshilfe, um diese Verordnung einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um vorherige Genehmigungen und eine vorherige Zurateziehung, die Vornahme von Nachprüfungen und die zügige Unterrichtung über die Befassung mit einer Angelegenheit und über weitere Entwicklungen in Fällen, in denen Personen in mehreren Mitgliedstaaten voraussichtlich von Verarbeitungsvorgängen betroffen sind.	
2. Jede Aufsichtsbehörde ergreift alle geeigneten Maßnahmen, um dem Ersuchen einer anderen Aufsichtsbehörde unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu können insbesondere auch die Übermittlung zweckdienlicher Informationen über den Verlauf einer Untersuchung oder Durchsetzungsmaßnahmen gehören, um die Einstellung oder das Verbot von Verarbeitungsvorgängen zu erwirken, die gegen diese Verordnung verstoßen.	
3. Das Amtshilfeersuchen enthält alle erforderlichen Informationen, darunter Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für die	

Angelegenheit verwendet, für die sie angefordert wurden.	
4. Die Aufsichtsbehörde, an die ein Amtshilfeersuchen gerichtet wird, kann dieses nur ablehnen, wenn	
a) sie für das Ersuchen nicht zuständig ist oder	
b) das Ersuchen gegen die Bestimmungen dieser Verordnung oder gegen Bestimmungen im Mitgl~~ei~~ied~~s~~staat der Aufsichtsbehörde verstoßen würde.	Klarstellung, dass die bestehenden Regelungen in den jeweiligen EU-Mitgliedstaaten zu beachten sind.
5. Die Aufsichtsbehörde, an die das Ersuchen gerichtet wurde, informiert die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um dem Ersuchen nachzukommen.	
6. Die Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, auf elektronischem Wege und so schnell wie möglich unter Verwendung eines standardisierten Formats, wobei sicherzustellen ist, dass die Informationen während ihrer Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Im Rahmen der Übermittlung von Informationen sind die schon heute geregelten Anforderungen an eine Weitergabekontrolle nach der Ziffer 4 der Anlage zu § 9 Satz 1 des deutschen BDSG zu beachten.
7. Maßnahmen, die aufgrund eines Amtshilfeersuchens getroffen werden, sind gebührenfrei.	
8. Wird eine ersuchte Aufsichtsbehörde nicht binnen eines Monats auf das Amtshilfeersuchen einer anderen Aufsichtsbehörde hin tätig, so ist die ersuchende Aufsichtsbehörde befugt, einstweilige Maßnahmen im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 Absatz 1 zu ergreifen und die Angelegenheit dem Europäischen Datenschutzausschuss gemäß dem Verfahren von Artikel 57 vorzulegen.	
9. Die Aufsichtsbehörde legt fest, wie lange diese einstweilige Maßnahme gültig ist. Dieser Zeitraum darf drei Monate nicht überschreiten. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss und die Kommission	

unverzüglich unter Angabe aller Gründe von diesen Maßnahmen in Kenntnis.	
10. Die Kommission kann Form und Verfahren der Amtshilfe nach diesem Artikel und die Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss, insbesondere das in Absatz 6 genannte standardisierte Format, festlegen. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	
Artikel 56 ***Gemeinsame Maßnahmen der Aufsichtsbehörden***	
1. Zur Stärkung der Zusammenarbeit und Amtshilfe erfüllen die Aufsichtsbehörden gemeinsame untersuchungsspezifische Aufgaben, führen gemeinsame Durchsetzungsmaßnahmen und andere gemeinsame Maßnahmen durch, an denen benannte Mitglieder oder Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten teilnehmen.	
2. In Fällen, in denen voraussichtlich Personen in mehreren Mitgliedstaaten von Verarbeitungsvorgängen betroffen sind, ist die Aufsichtsbehörde jedes dieser Mitgliedstaaten berechtigt, an den gemeinsamen untersuchungsspezifischen Aufgaben oder den gemeinsamen Maßnahmen teilzunehmen. Die zuständige Aufsichtsbehörde lädt die Aufsichtsbehörde jedes dieser Mitgliedstaaten zur Teilnahme an den betreffenden gemeinsamen untersuchungsspezifischen Aufgaben oder gemeinsamen Maßnahmen ein und antwortet unverzüglich auf das Ersuchen einer Aufsichtsbehörde um Teilnahme.	
3. Jede Aufsichtsbehörde kann als einladende Aufsichtsbehörde gemäß ihren nationalen Rechtsvorschriften und mit Genehmigung der unterstützenden Aufsichtsbehörde den an den gemeinsamen Maßnahmen beteiligten Mitgliedern oder Bediensteten der unterstützenden	

Aufsichtsbehörde Durchführungsbefugnisse einschließlich untersuchungsspezifischer Aufgaben übertragen oder, soweit dies nach dem Recht des Mitgliedstaats der einladenden Aufsichtsbehörde zulässig ist, den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestatten, ihre Durchführungsbefugnisse nach dem Recht der unterstützenden Aufsichtsbehörde auszuüben. Diese Durchführungsbefugnisse können nur unter der Leitung und in der Regel in Gegenwart der Mitglieder oder Bediensteten der einladenden Aufsichtsbehörde ausgeübt werden. Die Mitglieder oder Bediensteten der unterstützenden Aufsichtsbehörde unterliegen dem ~~nationalen~~ Recht des Mitgliedstaats der einladenden Aufsichtsbehörde. Die einladende Aufsichtsbehörde haftet für ihre Handlungen.	
4. ~~Die Aufsichtsbehörden regeln die praktischen Aspekte spezifischer Kooperationsmaßnahmen~~.	Es ist kein aus sich heraus verständlicher Regelungsgehalt erkennbar. Die Vorschrift ist daher zu streichen.
5. Kommt eine Aufsichtsbehörde binnen eines Monats nicht der Verpflichtung nach Absatz 2 nach, so sind die anderen Aufsichtsbehörden befugt, eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 Absatz 1 zu ergreifen.	
6. Die Aufsichtsbehörde legt fest, wie lange die einstweilige Maßnahme nach Absatz 5 gültig ist. Dieser Zeitraum darf drei Monate nicht überschreiten. Die Aufsichtsbehörde teilt dem Europäischen Datenschutzausschuss und der Kommission diese Maßnahmen unverzüglich unter Angabe aller Gründe mit und nimmt für diese Sache das in Artikel 57 genannte Verfahren in Anspruch.	

ABSCHNITT 2
KOHÄRENZ

Artikel 57 ***Kohärenzverfahren***	
Zu den in Artikel 46 Absatz 1 genannten Zwecken arbeiten die Aufsichtsbehörden im Rahmen des in	Die Unabhängigkeit der jeweiligen Aufsichtsbehörden (Artikel 47) sollte

diesem Abschnitt beschriebenen Kohärenzverfahrens untereinander und mit der Kommission im Europäischen Datenschutzausschuss gemäß Artikel 64 zusammen.	nicht durch Zuweisung von Aufsichtsbefugnissen an die Europäische Kommission unterlaufen werden. Vielmehr muss der vorgesehene Kohärenzprozess (Artikel 57 ff.) für ein abgestimmtes Handeln der nationalen Aufsichts-behörden sorgen. Dazu kommt dem Europäischen Datenschutzausschuss (Artikel 64 ff.) eine zentrale Rolle zu. Die Europäische Kommission sollte nicht getrennt neben diesem Ausschuss stehen, sondern dort selber Mitglied sein. Als „Gleicher unter Gleichen" kann dann die Kommission an den aufsichtsbehördlichen Entscheidungen des Ausschusses mitwirken. Ein Unterlaufen des Ausschusses durch eine Sonderzuständigkeit der Kommission neben dem Ausschuss wird damit vermieden.
Artikel 58 ***Stellungnahme des Europäischen Datenschutzausschusses***	
1. Bevor eine Aufsichtsbehörde eine Maßnahme nach Absatz 2 erlässt, übermittelt sie die geplante Maßnahme dem Europäischen Datenschutzausschuss ~~und der Kommission~~.	Die Streichung ist notwendig, um die Unabhängigkeit des Datenschutz-ausschusses nicht zu gefährden. Darüber sollte die Kommission ohnehin im Datenschutzausschuss vertreten sein. Verwaltungsrechtliche Maßnahmen sollten den Aufsichtsbehörden sowie dem unabhängigen Datenschutzausschuss obliegen, nicht jedoch der Kommission.
2. Die in Absatz 1 genannte Verpflichtung gilt für Maßnahmen, die Rechtswirkung entfalten sollen und	
a) sich auf Verarbeitungstätigkeiten beziehen, die mit dem zielgerichteten Angebot von Waren oder Dienstleistungen für eine erhebliche Zahl von betroffenen Personen in mehreren Mitgliedstaaten oder mit der Beobachtung des Verhaltens dieser	Es besteht die Gefahr, dass jede Verarbeitung in das recht aufwändige Kohärenzverfahren fallen könnte, weil im EU-Binnenmarkt grundsätzlich jede Ware oder

Personen im Zusammenhang stehen, oder	Dienstleistung EU-weit zugänglich sein sollte. Deshalb gilt es, den Anwendungsbereich einzugrenzen. Einschränkende Merkmale sollten sein: • Zielgerichtete Ausrichtung auf mehrere Mitgliedstaaten. Vgl. Artikel 6 Absatz 1 b) der VERORDNUNG (EG) Nr. 593/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I). • Relevanz für eine Vielzahl von Betroffenen.
b) den freien Verkehr personenbezogener Daten in der Union wesentlich beeinträchtigen können oder	
~~c) der Annahme einer Liste der Verarbeitungsvorgänge dienen, die der vorherigen Zurateziehung gemäß Artikel 34 Absatz 5 unterliegen oder~~	Folgeänderung zur Streichung von Artikel 34 Absatz 5.
d) der Festlegung von Standard-Datenschutzklauseln gemäß Artikel 42 Absatz 2 Buchstabe c dienen oder	Siehe Kommentierung dort.
e) der Genehmigung von Vertragsklauseln gemäß Artikel 42 Absatz 2 Buchstabe d dienen oder	Siehe Kommentierung dort.
f) der Annahme verbindlicher unternehmensinterner Vorschriften im Sinne von Artikel 43 dienen.	Siehe Kommentierung dort.
3. Jede Aufsichtsbehörde und der Europäische Datenschutzausschuss können beantragen, dass eine Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird, insbesondere, wenn eine Aufsichtsbehörde die in Absatz 2 genannte geplante Maßnahme nicht vorlegt oder den Verpflichtungen zur Amtshilfe gemäß Artikel 55 oder zu gemeinsamen Maßnahmen gemäß Artikel 56 nicht	

nachkommt.	
~~4. Um die ordnungsgemäße und kohärente Anwendung dieser Verordnung sicherzustellen, kann die Kommission beantragen, dass eine Sache im Rahmen des Kohärenzverfahrens behandelt wird.~~	Die Kommission sollte im Ausschuss vertreten sein und kann dann dort ihre Rechte wahrnehmen.
5. Die Aufsichtsbehörden ~~und die Kommission~~ übermitteln auf elektronischem Wege unter Verwendung eines standardisierten Formats zweckdienliche Informationen, darunter je nach Fall eine kurze Darstellung des Sachverhalts, die geplante Maßnahme und die Gründe, warum eine solche Maßnahme ergriffen werden muss, wobei sicherzustellen ist, dass die Informationen während ihrer Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Im Rahmen der Übermittlung von Informationen sind die schon heute geregelten Anforderungen an eine Weitergabekontrolle nach der Ziffer 4 der Anlage zu § 9 Satz 1 BDSG zu beachten.
6. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet unverzüglich auf elektronischem Wege unter Verwendung eines standardisierten Formats die Mitglieder des Datenschutzausschusses ~~und die Kommission~~ über zweckdienliche Informationen, die ihm zugegangen sind. Soweit erforderlich stellt der Vorsitz des Europäischen Datenschutzausschusses Übersetzungen der zweckdienlichen Informationen zur Verfügung.	
7. Wenn der Europäische Datenschutzausschuss dies mit der einfachen Mehrheit seiner Mitglieder entscheidet oder eine Aufsichtsbehörde ~~oder die Kommission~~ dies binnen einer Woche nach Übermittlung der zweckdienlichen Informationen nach Absatz 5 ~~beantragen~~beantragt, gibt der Europäische Datenschutzausschuss eine Stellungnahme zu der Angelegenheit ab. Die Stellungnahme wird binnen einem Monat mit der einfachen Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet je nach Fall die in Absatz 1 oder Absatz 3 genannte Aufsichtsbehörde~~, die Kommission~~ und die gemäß Artikel 51 zuständige Aufsichtsbehörde unverzüglich über die Stellungnahme und veröffentlicht sie.	
8. Die in Absatz 1 genannte Aufsichtsbehörde und die gemäß Artikel 51 zuständige	

Aufsichtsbehörde tragen der Stellungnahme des Europäischen Datenschutzausschusses Rechnung und teilen dessen Vorsitz ~~und der Kommission~~ binnen zwei Wochen nach ihrer Unterrichtung über die Stellungnahme elektronisch unter Verwendung eines standardisierten Formats mit, ob sie die geplante Maßnahme beibehält oder ändert; gegebenenfalls übermittelt sie die geänderte geplante Maßnahme.	
Artikel 59 ***Stellungnahme der Kommission***	
~~1. Binnen zehn Wochen, nachdem eine Angelegenheit nach Artikel 58 vorgebracht wurde, oder spätestens binnen sechs Wochen im Fall des Artikels 61, kann die Kommission hierzu eine Stellungnahme abgeben, um die ordnungsgemäße und einheitliche Anwendung dieser Verordnung sicherzustellen.~~	Vollständig streichen, da die Überwachung der einheitlichen Auslegung dieser VO dem Datenschutzausschuss obliegt, vgl. Art. 66, in dem die Kommission vertreten ist und Stellung nehmen kann.
~~2. Hat die Kommission eine Stellungnahme gemäß Absatz 1 angenommen, so die betroffene Aufsichtsbehörde der Kommission und dem Europäischen Datenschutzausschuss mit, ob sie ihre geplante Maßnahme beizubehalten oder abzuändern beabsichtigt.~~	Streichung erforderlich, um die Unabhängigkeit der Aufsichtsbehörden (vgl. auch Art. 47 VO-E) sicherzustellen.
~~3. Während des in Absatz 1 genannten Zeitraums erlässt die Aufsichtsbehörde nicht die geplante Maßnahme.~~	
~~4. Beabsichtigt die Aufsichtsbehörde, der Stellungnahme der Kommission nicht zu folgen, teilt sie dies der Kommission und dem Europäischen Datenschutzausschuss innerhalb des in Absatz 1 genannten Zeitraums mit und begründet dies. In diesem Fall darf die geplante Maßnahme während eines weiteren Monats nicht angenommen werden.~~	
Artikel 60 ***Aussetzung einer geplanten Maßnahme***	
~~1. Binnen eines Monats nach der Mitteilung nach Artikel 59 Absatz 4 kann die Kommission, wenn sie ernsthaft bezweifelt, dass die geplante Maßnahme die ordnungsgemäße Anwendung dieser Verordnung sicherstellt, oder befürchtet, dass sie zu~~	Folgeänderung zur Streichung von Artikel 59.

~~einer uneinheitlichen Anwendung der Verordnung führt, unter Berücksichtigung der Stellungnahme des Europäischen Datenschutzausschusses gemäß Artikel 58 Absatz 7 oder Artikel 61 Absatz 2 einen begründeten Beschluss erlassen, mit dem die Aufsichtsbehörde aufgefordert wird, die Annahme der geplanten Maßnahme auszusetzen, sofern dies erforderlich ist, um~~	
~~a) voneinander abweichende Meinungen der Aufsichtsbehörde und des Europäischen Datenschutzausschusses miteinander in Einklang zu bringen, falls dies möglich erscheint oder~~	
~~b) eine Maßnahme gemäß Artikel 62 Absatz 1 Buchstabe zu erlassen.~~	
~~2. Die Kommission legt fest, wie lange die Maßnahme ausgesetzt wird, wobei die Aussetzung 12 Wochen nicht überschreiten darf.~~	
~~3. Während des in Absatz 2 genannten Zeitraums darf die Aufsichtsbehörde die geplante Maßnahme nicht annehmen.~~	
Artikel 61 ***Dringlichkeitsverfahren***	
1. Unter außergewöhnlichen Umständen kann eine Aufsichtsbehörde abweichend vom Verfahren nach Artikel 58 sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer treffen, wenn sie zu der Auffassung gelangt, dass dringender Handlungsbedarf besteht, um die Interessen ~~von~~ betroffener Personen, vor allem, wenn die Durchsetzung ihrer Rechte durch eine Veränderung der bestehenden Lage erheblich behindert zu werden droht, zu schützen, um größere Nachteile abzuwenden oder aus anderen Gründen. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss ~~und die Kommission~~ unverzüglich unter Angabe aller Gründe von diesen Maßnahmen in Kenntnis.	
2. Hat eine Aufsichtsbehörde eine Maßnahme nach Absatz 1 ergriffen und ist sie der Auffassung, dass dringend endgültige Maßnahmen erlassen werden müssen, kann sie unter Angabe von Gründen,	

auch für die Dringlichkeit der endgültigen Maßnahmen, im Dringlichkeitsverfahren um eine Stellungnahme des Europäischen Datenschutzausschusses ersuchen.	
3. Jede Aufsichtsbehörde kann unter Angabe von Gründen, auch für den dringenden Handlungsbedarf, im Dringlichkeitsverfahren um eine Stellungnahme ersuchen, wenn die zuständige Aufsichtsbehörde trotz dringenden Handlungsbedarfs keine geeignete Maßnahme getroffen hat, um die Interessen von betroffenen Personen zu schützen.	
4. Abweichend von Artikel 58 Absatz 7 wird die Stellungnahme im Dringlichkeitsverfahren nach den Absätzen 2 und 3 binnen zwei Wochen durch einfache Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen.	
Artikel 62 ***Durchführungsrechtsakte***	
~~1. Die Kommission kann zu folgenden Zwecken Durchführungsrechtsakte erlassen:~~	
~~a) Beschluss über die ordnungsgemäße Anwendung dieser Verordnung gemäß ihren Zielen und Anforderungen im Hinblick auf Angelegenheiten, die ihr gemäß Artikel 58 oder Artikel 61 von einer Aufsichtsbehörde übermittelt wurden, zu denen gemäß Artikel 60 Absatz 1 ein begründeter Beschluss erlassen wurde oder zu denen eine Aufsichtsbehörde keine geplante Maßnahme übermittelt und mitgeteilt hat, dass sie der Stellungnahme der Kommission gemäß Artikel 59 nicht zu folgen beabsichtigt,~~	
~~b) Beschluss innerhalb des in Artikel 59 Absatz 1 genannten Zeitraums darüber, ob Standard-Datenschutzklauseln nach Artikel 58 Absatz 2 Buchstabe d allgemeine Gültigkeit zuerkannt wird,~~	
~~c) Festlegung der Form und der Verfahren für die Anwendung des in diesem Abschnitt beschriebenen Kohärenzverfahrens,~~	
~~d) Festlegung der Ausgestaltung des elektronischen Informationsaustauschs zwischen den~~	

~~Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss, insbesondere des standardisierten Formats nach Artikel 58 Absätze 5, 6 und 8.~~	
~~Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.~~	
~~2. In hinreichend begründeten Fällen äußerster Dringlichkeit im Zusammenhang mit den Interessen betroffener Personen gemäß Absatz 1 Buchstabe a erlässt die Kommission gemäß dem Verfahren von Artikel 87 Absatz 3 sofort geltende Durchführungsrechtsakte. Diese gelten für einen Zeitraum von höchstens 12 Monaten.~~	Mit der Unabhängigkeit der Aufsichtsbehörden nicht zu vereinbaren und daher zu streichen, vgl. Art. 47!
~~3. Unabhängig davon, ob die Kommission eine Maßnahme nach Maßgabe dieses Abschnitts erlassen hat, kann sie auf der Grundlage der Verträge andere Maßnahmen erlassen.~~	
Artikel 63 ***Durchsetzung***	
1. Folgt die Aufsichtsbehörde der Stellungnahme des Europäischen Datenschutzauschusses gemäß Artikel 58 Abs. 8 so wird f~~F~~ür die Zwecke dieser Verordnung ~~wird~~ eine durchsetzbare Maßnahme der Aufsichtsbehörde eines Mitgliedstaats in allen anderen betroffenen Mitgliedstaaten durchgesetzt.	Klarstellung der Rechtsfolge von Artikel 58 Absatz 8.
2. Nimmt eine Aufsichtsbehörde für eine geplante Maßnahme entgegen Artikel 58 Absätze 1 bis 5 nicht das Kohärenzverfahren in Anspruch oder folgt die Aufsichtsbehörde der Stellungnahme des Europäischen Datenschutzauschusses gemäß Artikel 58 Abs. 8 nicht oder nur teilweise, so ist die Maßnahme der Aufsichtsbehörde nicht europaweit rechtsgültig und durchsetzbar.	Klarstellung der Rechtsfolge von Artikel 58 Absatz 8.

ABSCHNITT 3
EUROPÄISCHER DATENSCHUTZAUSSCHUSS

Artikel 64 ***Europäischer Datenschutzausschuss***	
1. Hiermit wird ein Europäischer Datenschutzausschuss eingerichtet.	
2. Der Europäische Datenschutzausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats, ~~und~~ dem Europäischen Datenschutzbeauftragten sowie einem Vertreter der Europäischen Kommission.	Folgeänderung: Die Kommission sollte Mitglied im Ausschuss sein. Dann bedarf es für diese keiner gesonderten Regelung.
~~3. Ist in einem Mitgliedstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe dieser Richtlinie erlassenen Vorschriften zuständig, so wird der Leiter einer diese Aufsichtsbehörden zum gemeinsamen Vertreter ernannt.~~	Streichen: Folgeänderung Artikel 46 Absatz 1.
~~4. Die Kommission ist berechtigt, an den Tätigkeiten und Sitzungen des Europäischen Datenschutzausschusses teilzunehmen und bestimmt einen Vertreter. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet die Kommission unverzüglich von allen Tätigkeiten des Europäischen Datenschutzausschusses.~~	
Artikel 65 ***Unabhängigkeit***	
1. Der Europäische Datenschutzausschuss handelt bei der Erfüllung seiner Aufgaben gemäß den Artikeln 66 und 67 unabhängig.	
~~2. Unbeschadet der Ersuchen der Kommission gemäß Artikel 66 Absatz 1 Buchstabe b und Artikel 67 Absatz 2 ersucht der Europäische Datenschutzausschuss bei der Erfüllung seiner Aufgaben weder um Weisung noch nimmt er Weisungen entgegen.~~	Die Weisungsungebundenheit des Ausschusses gegenüber der Kommission steht im Widerspruch zu der in Abs. 1 der Vorschrift normierten Unabhängigkeit des Ausschusses.

Artikel 66 ***Aufgaben des Europäischen Datenschutzausschusses***	
1. Der Europäische Datenschutzausschuss stellt sicher, dass diese Verordnung einheitlich angewandt wird. Zu diesem Zweck geht der Europäische Datenschutzausschuss ~~von sich aus oder auf Ersuchen der Kommission~~ insbesondere folgenden Tätigkeiten nach:	Folgeänderung zu Artikel 64 Absatz 2.
a) Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, darunter auch etwaige Vorschläge zur Änderung dieser Verordnung;	
b) von sich aus, auf Antrag eines seiner Mitglieder ~~oder auf Ersuchen der Kommission~~ vorgenommene Prüfung von die Anwendung dieser Verordnung betreffenden Fragen und Ausarbeitung von Leitlinien, Empfehlungen und bewährten Praktiken für die Aufsichtsbehörden zwecks Sicherstellung einer einheitlichen Anwendung dieser Verordnung;	Folgeänderung zu Artikel 64 Absatz 2.
c) Überprüfung der praktischen Anwendung der unter Buchstabe b genannten Leitlinien, Empfehlungen und bewährten ~~Praktiken und regelmäßige Berichterstattung über diese an die Kommission~~;	Folgeänderung zu Artikel 64 Absatz 2.
d) Abgabe von Stellungnahmen zu Beschlussentwürfen von Aufsichtsbehörden gemäß dem in Artikel 57 genannten Kohärenzverfahren;	
e) Förderung der Zusammenarbeit und eines effizienten bilateralen und multilateralen Austausches von Informationen und Praktiken zwischen den Aufsichtsbehörden;	
f) Förderung von Schulungsprogrammen und Erleichterung des Personalaustausches zwischen Aufsichtsbehörden sowie gegebenenfalls mit Aufsichtsbehörden von Drittländern oder mit Aufsichtsstellen internationaler Organisationen;	
g) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzvorschriften und –praktiken mit	

Datenschutzaufsichtsbehörden in aller Welt.	
2. Die Kommission kann, wenn sie den Europäischen Datenschutzausschuss um Rat ersucht, unter Berücksichtigung der Dringlichkeit des Sachverhalts eine Frist setzen.	
3. Der Europäische Datenschutzausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Praktiken an die Kommission und an den in Artikel 87 genannten Ausschuss weiter und veröffentlicht sie.	
4. Die Kommission setzt den Europäischen Datenschutzausschuss von allen Maßnahmen in Kenntnis, die sie im Anschluss an die vom Europäischen Datenschutzausschuss herausgegebenen Stellungnahmen, Leitlinien, Empfehlungen und bewährten Praktiken ergriffen hat.	
Artikel 67 ***Berichterstattung***	
1. Der Europäische Datenschutzausschuss informiert die Kommission regelmäßig und zeitnah über die Ergebnisse seiner Tätigkeiten. Er erstellt einen jährlichen Bericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Union und in Drittländern.	
Der Bericht enthält eine Überprüfung der praktischen Anwendung der in Artikel 66 Absatz 1 Buchstabe c genannten Leitlinien, Empfehlungen und bewährten Praktiken.	
2. Der Bericht wird veröffentlicht und dem Europäischen Parlament, dem Rat und der Kommission übermittelt.	
Artikel 68 ***Verfahrensweise***	
1. Der Europäische Datenschutzausschuss trifft seine Beschlüsse mit der einfachen Mehrheit seiner Mitglieder.	

2. Der Europäische Datenschutzausschuss gibt sich eine Geschäftsordnung und legt seine Arbeitsweise fest. Er sieht insbesondere vor, dass bei Ablauf der Amtszeit oder Rücktritt eines seiner Mitglieder die Aufgaben kontinuierlich weitererfüllt werden, dass für spezifische Fragen oder Sektoren Untergruppen eingesetzt werden, und dass seine Verfahrensvorschriften im Einklang mit dem in Artikel 57 genannten Kohärenzverfahren stehen.	
Artikel 69 ***Vorsitz***	
1. Der Europäische Datenschutzausschuss wählt aus dem Kreis seiner Mitglieder einen Vorsitzenden und zwei stellvertretende Vorsitzende. Der Europäische Datenschutzbeauftragte, bekleidet, sofern er nicht zum Vorsitzenden gewählt wurde, einen der beiden Stellvertreterposten.	
2. Die Amtszeit des Vorsitzenden und seiner beiden Stellvertreter beträgt fünf Jahre; ihre Wiederwahl ist zulässig.	
Artikel 70 ***Aufgaben des Vorsitzenden***	
1. Der Vorsitzende hat folgende Aufgaben:	
a) Einberufung der Sitzungen des Europäischen Datenschutzausschusses und Erstellung der Tagesordnungen;	
b) Sicherstellung einer rechtzeitigen Erfüllung der Aufgaben des Europäischen Datenschutzausschusses, insbesondere der Aufgaben im Zusammenhang mit dem Kohärenzverfahren nach Artikel 57.	
2. Der Europäische Datenschutzausschuss legt die Verteilung der Aufgaben auf den Vorsitzenden und dessen zwei Stellvertreter in seiner Geschäftsordnung fest.	

Artikel 71 ***Sekretariat***	
1. Der Europäische Datenschutzausschuss erhält ein Sekretariat. Dieses wird vom Europäischen Datenschutzbeauftragten gestellt.	
2. Das Sekretariat leistet dem Europäischen Datenschutzausschuss unter Leitung von dessen Vorsitzendem analytische, administrative und logistische Unterstützung.	
3. Das Sekretariat ist insbesondere verantwortlich für	
a) das Tagesgeschäft des Europäischen Datenschutzausschusses;	
b) die Kommunikation zwischen den Mitgliedern des Europäischen Datenschutzausschusses, seinem Vorsitz und der Kommission sowie die Kommunikation mit anderen Organen und mit der Öffentlichkeit;	
c) den Rückgriff auf elektronische Mittel für die interne und die externe Kommunikation;	
d) die Übersetzung sachdienlicher Informationen;	
e) die Vor- und Nachbereitung der Sitzungen des Europäischen Datenschutzausschusses;	
f) Vorbereitung, Entwurf und Veröffentlichung von Stellungnahmen und sonstigen vom Europäischen Datenschutzausschuss angenommenen Dokumenten.	
Artikel 72 ***Vertraulichkeit***	
1. Die Beratungen des Europäischen Datenschutzausschusses sind vertraulich.	
2. Den Mitgliedern des Europäischen Datenschutzausschusses, Sachverständigen und den Vertretern von Dritten vorgelegte Dokumente sind vertraulich, sofern sie nicht gemäß der Verordnung (EG) Nr. 1049/2001 offengelegt oder <u>auf der Grundlage einer anderen Rechtsvorschrift</u> ~~andere~~	Klarstellung.

~~Weise~~ vom Europäischen Datenschutzausschuss der Öffentlichkeit zugänglich gemacht werden.	
3. Die Mitglieder des Europäischen Datenschutzausschusses, die Sachverständigen und die Vertreter von Dritten beachten die Verpflichtung zur Wahrung der Vertraulichkeit gemäß diesem Artikel. Der Vorsitzende stellt sicher, dass die Sachverständigen und die Vertreter von Dritten von der ihnen auferlegten Vertraulichkeitspflicht in Kenntnis gesetzt werden.	

KAPITEL VIII
RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

Artikel 73 ***Recht auf Beschwerde bei einer Aufsichtsbehörde***	Die EU-Verordnung sollte keine neuen Instrumente kollektiver Rechtsdurchsetzung (vgl. Artikel 73) schaffen. Dem Recht auf informationelle Selbstbestimmung ist immanent, dass jedes Individuum entscheiden kann, welche Informationen es wem gegenüber wie preisgeben möchte. Folgerichtig wird es allgemein als ein höchstpersönliches Recht begriffen. Darum sollte auch die Rechtsdurchsetzung individuell erfolgen. Einer Verbandsklage – etwa nach amerikanischem Vorbild – bedarf es zudem deswegen nicht, weil hierzulande jeder Verbraucher die Möglichkeit hat, sich auf Basis der Verordnung an die für ihn zuständige Behörde zu wenden, welche mit den zur Durchsetzung der Vorschriften dieser Verordnung notwendigen Befugnissen ausgestattet ist, über eine hohe Fachkompetenz verfügt und welche insbesondere keine sachfremden wirtschaftlichen Eigeninteressen verfolgt. Ergänzend kann die Hilfe eines Rechtsanwalts in Anspruch genommen werden.
1. Jede betroffene Person hat unbeschadet eines anderweitigen administrativen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht mit dieser Verordnung vereinbar ist.	
~~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~~	Streichen, da Verstoß gegen das Rechtsberatungsgesetz. Siehe auch Änderungsvorschläge zu Absatz 3. Schutz des Betroffenen ist über

~~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.~~	Absatz 3 sichergestellt.
~~3. Unabhängig von der Beschwerde einer betroffenen Person haben 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, im Sinne des Absatzes 2 das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde, wenn sie der Ansicht sind, dass der Schutz personenbezogener Daten verletzt wurde.~~	Das Beschwerderecht sollte nur den tatsächlich Betroffenen zustehen. Der Betroffene kann sich hierbei nach den nationalen Rechtsvorschriften zur Rechtsberatung von Dritten vertreten lassen.
Artikel 74 ***Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde***	
1. Jede natürliche oder juristische Person hat das Recht auf einen gerichtlichen Rechtsbehelf gegen sie betreffende Entscheidungen einer Aufsichtsbehörde.	
2. Jede betroffene Person hat das Recht auf einen gerichtlichen Rechtsbehelf, um die Aufsichtsbehörde zu verpflichten, im Fall einer Beschwerde tätig zu werden, wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist oder wenn die Aufsichtsbehörde sie nicht gemäß Artikel 52 Absatz 1 Buchstabe b innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.	
3. Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.	
4. Eine betroffene Person, die von einer Entscheidung einer Aufsichtsbehörde betroffen ist, die ihren Sitz in einem anderen Mitgliedstaat hat als dem, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, kann die Aufsichtsbehörde in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts ersuchen,	

in ihrem Namen gegen die zuständige Aufsichtsbehörde in dem anderen Mitgliedstaat Klage zu erheben.	
5. Die endgültigen Entscheidungen der Gerichte im Sinne dieses Artikels werden von den Mitgliedstaaten vollstreckt.	Unklar ist, ob in einem Mitgliedstaat auch Gerichtsentscheidungen aus einem anderen Mitgliedstaat vollstreckbar sind.
Artikel 75 ***Recht auf gerichtlichen Rechtsbehelf gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter***	
1. Jede natürliche Person hat unbeschadet eines verfügbaren administrativen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde nach Artikel 73 das Recht auf einen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht verordnungskonformen Verarbeitung ihrer personenbezogenen Daten verletzt wurden.	
~~2. Für Klagen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, es sei denn, es handelt sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.~~	In Deutschland gilt für Klagen gegen die verarbeitende Stelle der Zivilrechtsweg. Die bestehenden europäischen wie nationalen Regelungen zum Gerichtsstand (u.a. Brüssel-I-VO) dürfen durch die angedachten Regelungen nicht konterkariert werden.
3. Ist dieselbe Maßnahme, Entscheidung oder Vorgehensweise Gegenstand des Kohärenzverfahrens gemäß Artikel 58, kann das Gericht das Verfahren, mit dem es befasst wurde, aussetzen, es sei denn, es ist aufgrund der Dringlichkeit des Schutzes der Rechte der betroffenen Person nicht möglich, den Ausgang des Kohärenzverfahrens abzuwarten.	
~~4. Die endgültigen Entscheidungen der Gerichte im Sinne dieses Artikels werden von den Mitgliedstaaten vollstreckt.~~	Streichen, da nicht erforderlich. Die gerichtliche Vollstreckung von Urteilen der Zivilgerichtsbarkeit ist bereits im nationalen Zivilprozessrecht sowie in der sog.

	Brüssel I VO (EG 44/2001) geregelt.
Artikel 76 ***Gemeinsame Vorschriften für Gerichtsverfahren***	
~~1. Einrichtungen, Organisationen oder Verbände im Sinne des Artikels 73 Absatz 2 haben das Recht, die in Artikel 74 und 75 genannten Rechte im Namen einer oder mehrerer betroffenen Personen wahrzunehmen.~~	Ein Sammel- oder Verbandsklagerecht ist auf Grund der Beschwerdemöglichkeit bei der Aufsichtsbehörde nicht erforderlich. Zudem obliegt es dem Betroffenen, sein Recht auf informationelle Selbstbestimmung eigenständig wahrzunehmen. Sollte gleichwohl an einem Klagerecht der Verbände festgehalten werden, sind zumindest die Regelungen der Richtlinie EG/98/27 „EU-Unterlassungsklagenrichtlinie“ einzuhalten; d.h., das Klagerecht kann nur von einer qualifizierten und staatlich anerkannten Stelle in Anspruch genommen werden, vgl. § 4 UKlaG.
~~2. Jede Aufsichtsbehörde hat das Recht, Klage zu erheben, um die Bestimmungen dieser Verordnung durchzusetzen oder um einen einheitlichen Schutz der personenbezogenen Daten innerhalb der Union sicherzustellen.~~	Die Regelung hat das Verwaltungshandeln in den einzelnen Mitgliedstaaten zu beachten. Nach deutschem Verwaltungsrecht hat eine Behörde kein Klagerecht gegen nicht-öffentliche Stellen.
3. Hat ein zuständiges mitgliedstaatliches Gericht Grund zu der Annahme, dass in einem anderen Mitgliedstaat ein Parallelverfahren anhängig ist, setzt es sich mit dem zuständigen Gericht in diesem anderen Mitgliedstaat in Verbindung, um sich zu vergewissern, ob ein solches Parallelverfahren besteht.	
4. Betrifft das Parallelverfahren in dem anderen Mitgliedstaat dieselbe Maßnahme, Entscheidung oder Vorgehensweise, kann das Gericht sein Verfahren aussetzen.	
~~5. Die Mitgliedstaaten stellen sicher, dass mit den nach innerstaatlichem Recht verfügbaren~~	Streichen, da Maßnahmen des einstweiligen Rechtsschutzes bei-

~~Klagemöglichkeiten rasch Maßnahmen einschließlich einstweilige Maßnahmen erwirkt werden können, um mutmaßliche Rechtsverletzungen abzustellen und zu verhindern, dass den Betroffenen weiterer Schaden entsteht.~~	spielsweise in Deutschland ausreichend geregelt sind (einstweiliger Rechtsschutz nach ZPO).
Artikel 77 ***Haftung und Recht auf Schadenersatz***	
1. Jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen mit dieser Verordnung nicht zu vereinbarenden Handlung ein Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.	
2. Ist mehr als ein für die Verarbeitung Verantwortlicher oder mehr als ein Auftragsverarbeiter an der Verarbeitung beteiligt, haftet jeder für die Verarbeitung Verantwortliche oder jeder Auftragsverarbeiter gesamtschuldnerisch für den gesamten Schaden. <u>Regressansprüche im Innenverhältnis bleiben hiervon unberührt.</u>	Folge der gemeinsamen Verantwortung (Art. 24)
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass ihm der Umstand, durch den der Schaden eingetreten ist, nicht zur Last gelegt werden kann.	

Artikel 78 ***Sanktionen***	Die Differenzierung zwischen „Sanktionen“ (Artikel 78) und „verwaltungsrechtlichen Sanktionen“ (Artikel 79) ist nicht nachvollziehbar. Es darf nicht zu einer doppelten Sanktionierung eines Verstoßes kommen. Zudem sind Bußgeldvorschriften originärer Bestandteil des Strafrechts und entziehen sich damit der Regelungszuständigkeit der Europäischen Union. Diese kollisionsrechtliche Regel würde umgangen, wenn man – wie in Artikel 79 Absätze 4 bis 6 angedacht – nun ein bis dato dem europäischen Recht fremdes „verwaltungsrechtliches Bußgeld“ einführte.
1. Die Mitgliedstaaten legen fest, welche Sanktionen bei einem Verstoß gegen diese Verordnung zu verhängen sind, und treffen die zu ihrer Durchsetzung erforderlichen Maßnahmen; dies gilt auch für den Fall, dass der für die Verarbeitung Verantwortliche seiner Pflicht zur Benennung eines Repräsentanten~~Vertreters~~ nach Artikel 25 nicht nachgekommen ist. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.	Folgeänderung zu Artikel 4 Absatz 14; vgl. auch Artikel 80 Absatz 6 f).
2. Hat der für die Verarbeitung Verantwortliche einen Repräsentanten nach Artikel 25 ~~Vertreter~~ benannt, wirken die Sanktionen gegen den Repräsentanten~~Vertreter~~ unbeschadet etwaiger Sanktionen, die gegen den für die Verarbeitung Verantwortlichen verhängt werden könnten.	Folgeänderung zu Artikel 4 Absatz 14; vgl. auch Artikel 80 Absatz 6 f).
3. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.	

~~*Artikel 79*~~ ~~***Verwaltungsrechtliche Sanktionen***~~	Artikel 79 ist insgesamt zu streichen, da dieser Sachverahlt bereits in Artikel 78 abschließend geregelt ist. Darüber hinaus fehlt es an der Kompetenz der Regelung strafrechtlicher Bußgeldvorschriften, wie sie in Artikel 79 Absätze 4 bis 6 angedacht sind.
~~1. Jede Aufsichtsbehörde ist befugt, nach Maßgabe dieses Artikels verwaltungsrechtliche Sanktionen zu verhängen.~~	
~~2. Die verwaltungsrechtlichen Sanktionen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Die Höhe der Geldbuße bemisst sich nach der Art, Schwere und Dauer des Verstoßes, seinem vorsätzlichen oder fahrlässigen Charakter, dem Grad der Verantwortung der natürlichen oder juristischen Person und früheren Verstößen dieser Person, den nach Artikel 23 eingeführten technischen und organisatorischen Maßnahmen und Verfahren und dem Grad der Zusammenarbeit mit der Aufsichtsbehörde zur Abstellung des Verstoßes.~~	
~~3. Handelt es sich um einen ersten, unabsichtlichen Verstoß gegen diese Verordnung, kann anstatt einer Sanktion eine schriftliche Verwarnung erfolgen. Fällen, in denen~~	
~~eine natürliche Person personenbezogene Daten ohne eigenwirtschaftliches Interesse verarbeitet oder~~	Die Voraussetzungen sind zu streichen, da sich bereits aus dem Verhältnismäßigkeitsgebot des Absatzes 2 zwingend ergibt, dass eine vorangehende Verwarnung immer zulässig sein muss.
~~ein Unternehmen oder eine Organisation mit weniger als 250 Beschäftigten personenbezogene Daten nur als Nebentätigkeit zusätzlich zu den Haupttätigkeiten verarbeitet.~~	
~~4. Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 250 000 EUR oder im Fall eines Unternehmens bis in Höhe von 0,5 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder~~	Die Sanktionen sind unverhältnismäßig und könnten die Existenz der Unternehmen bedrohen. Die Einführung eines kartellrechtsähnlichen Bußgeld-

~~fahrlässig~~	rahmens ist auf Grund des Schutzzwecks des Datenschutzrechts (Individualschutz) nicht gerechtfertigt. Zudem ist im deutschen Verwaltungs- und Strafrecht eine Gewinnabschöpfung nur unter bestimmten Voraussetzungen möglich. Weiter ist die Abstufung nach den unterschiedlichen Strafgraden bei etlichen Tatbeständen nicht nachvollziehbar.
~~(a) keine Vorkehrungen für Anträge betroffener Personen gemäß Artikel 12 Absätze 1 und 2 trifft oder den Betroffenen nicht unverzüglich oder nicht dem verlangten Format entsprechend antwortet;~~	
~~(b) unter Verstoß gegen Artikel 12 Absatz 4 eine Gebühr für die Auskunft oder die Beantwortung von Anträgen betroffener Personen verlangt.~~	
5. ~~Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 500 000 EUR oder im Fall eines Unternehmens bis in Höhe von 1 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig~~	Die Sanktionen sind unverhältnismäßig und könnten die Existenz der Unternehmen bedrohen. Die Einführung eines kartellrechtsähnlichen Bußgeldrahmens ist auf Grund des Schutzzwecks des Datenschutzrechts (Individualschutz) nicht gerechtfertigt.
~~(a) der betroffenen Person die Auskünfte gemäß Artikel 11, Artikel 12 Absatz 3 und Artikel 14 nicht oder nicht vollständig oder in nicht hinreichend transparenter Weise erteilt;~~	
~~(b) der betroffenen Person keine Auskunft gemäß Artikel 15 erteilt, personenbezogene Daten nicht gemäß Artikel 16 berichtigt oder einen Empfänger nicht gemäß Artikel 13 benachrichtigt;~~	
~~(c) das Recht auf Vergessenwerden oder auf~~	

~~Löschung nicht beachtet, keine Vorkehrungen trifft, um die Einhaltung der Fristen zu gewährleisten, oder nicht alle erforderlichen Schritte unternimmt, um Dritte von einem Antrag der betroffenen Person auf Löschung von Links zu personenbezogenen Daten sowie Kopien oder Replikationen dieser Daten gemäß Artikel 17 zu benachrichtigen;~~	
~~(d) keine Kopie der personenbezogenen Daten in elektronischem Format bereitstellt oder die betroffene Person unter Verstoß gegen Artikel 18 daran hindert, personenbezogene Daten auf eine andere Anwendung zu übertragen;~~	
~~(e) die jeweilige Verantwortung der für die Verarbeitung Mitverantwortlichen nicht oder nicht hinreichend gemäß Artikel 24 bestimmt hat;~~	
~~(f) die Dokumentation gemäß Artikel 28, Artikel 31 Absatz 4 und Artikel 44 Absatz 3 nicht oder nicht hinreichend gewährleistet;~~	
~~(g) in Fällen, in denen keine besonderen Kategorien von Daten verarbeitet werden, die Vorschriften im Hinblick auf die freie Meinungsäußerung gemäß Artikel 80, die Datenverarbeitung im Beschäftigungskontext gemäß Artikel 82 oder die Bedingungen für die Verarbeitung zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung gemäß Artikel 83 nicht beachtet.~~	
~~6. Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 1 000 000 EUR oder im Fall eines Unternehmens bis in Höhe von 2 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig~~	Die Sanktionen sind unverhältnismäßig und könnten die Existens der Unternehmen bedrohen. Die Einführung eines kartellrechtsähnlichen Bußgeldrahmens ist auf Grund des Schutzzwecks des Datenschutz-rechts (Individualschutz) nicht

	gerechtfertigt.
~~(a) personenbezogene Daten ohne oder ohne ausreichende Rechtsgrundlage verarbeitet oder die Bedingungen für die Einwilligung gemäß den Artikeln 6, 7 und 8 nicht beachtet;~~	
~~(b) unter Verstoß gegen die Artikel 9 und 81 besondere Kategorien von Daten verarbeitet;~~	
~~(c) das Recht auf Widerspruch gemäß Artikel 19 oder eine damit verbundene Bedingung nicht beachtet;~~	
~~(d) die Bedingungen gemäß Artikel 20 in Bezug auf Maßnahmen, die auf Profiling basieren, nicht beachtet;~~	
~~(e) keine internen Datenschutzstrategien festlegt oder keine geeigneten Maßnahmen gemäß den Artikeln 22, 23 und 30 anwendet, um die Beachtung der Datenschutzvorschriften sicherzustellen und nachzuweisen;~~	
~~(f) keinen Vertreter gemäß Artikel 25 benennt;~~	
~~(g) unter Verstoß gegen die mit der Datenverarbeitung im Namen eines für die Verarbeitung Verantwortlichen verbundenen Pflichten gemäß den Artikeln 26 und 27 personenbezogene Daten verarbeitet oder deren Verarbeitung anordnet;~~	
~~(h) die Aufsichtsbehörde bei einer Verletzung des Schutzes personenbezogener Daten nicht alarmiert oder sie oder die betroffene Person gemäß den Artikeln 31 und 32 nicht oder nicht rechtzeitig oder nicht vollständig von einer solchen Verletzung benachrichtigt;~~	
~~(i) keine Datenschutz-Folgenabschätzung nach Artikel 33 vornimmt oder~~	

~~personenbezogene Daten entgegen Artikel 34 ohne vorherige Genehmigung oder ohne Zuratezichung der Aufsichtsbehörde verarbeitet;~~	
~~(j) keinen Datenschutzbeauftragten nach Artikel 35 benennt oder nicht die Voraussetzungen für die Erfüllung seiner Aufgaben gemäß Artikel 35, 36 und 37 schafft;~~	
~~(k) ein Datenschutzsiegel oder -zeichen im Sinne des Artikels 39 missbraucht;~~	
~~(l) eine mangels eines Angemessenheitsbeschlusses oder mangels geeigneter Garantien oder einer Ausnahme gemäß den Artikeln 40 bis 44 unzulässige Datenübermittlung in ein Drittland oder an eine internationale Organisation vornimmt oder anordnet;~~	
~~(m) einer Anweisung oder einem vorübergehenden oder endgültigen Verarbeitungsverbot oder einer Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 53 Absatz 1 nicht Folge leistet;~~	
~~(n) entgegen den Pflichten gemäß Artikel 28 Absatz 3, Artikel 29, Artikel 34 Absatz 6 und Artikel 53 Absatz 2 die Aufsichtsbehörde nicht unterstützt, nicht mit ihr zusammenarbeitet, ihre keine einschlägigen Auskünfte erteilt oder keinen Zugang zu seinen Räumlichkeiten gewährt;~~	
~~(o) die Vorschriften über die Wahrung des Berufsgeheimnisses gemäß Artikel 84 nicht einhält.~~	
~~7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Beträge der in den Absätzen 4, 5 und 6 genannten Geldbußen unter Berücksichtigung der in Absatz 2 aufgeführten Kriterien zu aktualisieren.~~	

KAPITEL IX
VORSCHRIFTEN FÜR BESONDERE DATENVERARBEITUNGSSITUATIONEN

Artikel 80 ***Verarbeitung personenbezogener Daten und freie Meinungsäußerung***	
1. Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen oder Ausnahmen von den allgemeinen Grundsätzen des Kapitels II, von den Rechten der betroffenen Person in Kapitel III, von den Bestimmungen über den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter in Kapitel IV, von der Übermittlung personenbezogener Daten in Drittländer und an internationale Organisationen in Kapitel V, von den Vorschriften über die Aufsichtsbehörden in Kapitel VI sowie von den Vorschriften über Zusammenarbeit und Kohärenz in Kapitel VII vor, um das Recht auf Schutz der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen.	
2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlassen hat, und setzt sie unverzüglich von allen weiteren Änderungsgesetzen oder diese Rechtsvorschriften betreffenden Änderungen in Kenntnis.	
Artikel 81 ***Verarbeitung personenbezogener Gesundheitsdaten***	
1. Die Verarbeitung personenbezogener Gesundheitsdaten erfolgt in den Grenzen dieser Verordnung nach Maßgabe von Artikel 9 Absatz 2 Buchstabe h auf der Grundlage des Unionsrechts oder des mitgliedstaatlichen Rechts, das geeignete, besondere Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht; sie muss notwendig sein	

a) für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten, sofern die Verarbeitung dieser Daten durch dem Berufsgeheimnis unterliegendes ärztliches Personal erfolgt oder durch sonstige Personen, die nach mitgliedstaatlichem Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, einer entsprechenden Geheimhaltungspflicht unterliegen;	
b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit unter anderem zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards unter anderem für Arzneimittel oder Medizinprodukte oder	
c) aus anderen Gründen des öffentlichen Interesses in Bereichen wie der sozialen Sicherheit, insbesondere um die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Krankenversicherungsleistungen sicherzustellen.	
2. Die Verarbeitung personenbezogener Gesundheitsdaten, die zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung unter anderem zur Erstellung von Patientenregistern zur Verbesserung der Diagnose sowie zur Unterscheidung zwischen ähnlichen Krankheitsarten und zur Vorbereitung von Studien zu Therapiezwecken erforderlich ist, unterliegt den Bedingungen und Garantien gemäß Artikel 83.	
~~3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit im Sinne des Absatzes 1 Buchstabe b näher auszuführen und um die Kriterien und Anforderungen in Bezug auf die Garantien für die Verarbeitung personenbezogener Daten für die in Absatz 1 genannten Zwecke festzulegen.~~	

Artikel 82 ***Datenverarbeitung im Beschäftigungskontext***	Ausnahmeregelungen für Datenverarbeitungen im Beschäftigungsverhältnis sollten nicht zugelassen werden, das sonst das von der Verordnung verfolgte Ziel der Schaffung eines einheitlichen Datenschutzniveaus in der EU in Frage gestellt wird. Wettbewerbsverzerrungen wären die Folge. Fraglich darüber hinaus: Verhältnis von Art. 82 zu Erwägungsgrund 34 i. V. m. Art. 7 Abs. 4. Denn aus Art. 7 Abs. 4 könnte folgen, dass Einwilligungserklärungen in Beschäftigungsverhältnissen nicht wirksam sein sollen. Dies widerspricht der Intention von Art. 82, wonach die Mitgliedstaaten Regelungen für die Datenverarbeitung im Beschäftigungsverhältnis erlassen sollen.
~~1. Die Mitgliedstaaten können in den Grenzen dieser Verordnung per Gesetz die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext unter anderem für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von gesetzlich oder tarifvertraglich festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses regeln.~~	
~~2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.~~	
~~3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Garantien für die Verarbeitung personenbezogener Daten für die in Absatz 1 genannten Zwecke~~	

~~festzulegen.~~	
Artikel 83 ***Datenverarbeitung zu historischen oder statistischen Zwecken sowie zum Zwecke der wissenschaftlichen Forschung***	
1. In den Grenzen dieser Verordnung dürfen personenbezogene Daten nur dann zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung verarbeitet werden, wenn	
a) diese Zwecke nicht auf andere Weise durch die Verarbeitung von Daten erfüllt werden können, die eine Bestimmung der betroffenen Person nicht oder nicht mehr ermöglichen;	
b) Daten, die die Zuordnung von Informationen zu einer bestimmten oder bestimmbaren betroffenen Person ermöglichen, von den übrigen Informationen getrennt aufbewahrt werden, sofern diese Zwecke in dieser Weise erfüllt werden können.	
2. Einrichtungen, die Arbeiten für historische oder statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung durchführen, dürfen personenbezogene Daten nur dann veröffentlichen oder auf andere Weise bekannt machen, wenn	
a) die betroffene Person nach Maßgabe von Artikel 7 ihre Einwilligung erteilt hat,	
b) die Veröffentlichung personenbezogener Daten für die Darstellung von Forschungsergebnissen oder zur Unterstützung der Forschung notwendig ist, soweit die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person diese Interessen nicht überwiegen oder	
c) die betroffene Person die Daten veröffentlicht hat.	
~~3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Verarbeitung personenbezogener Daten für die Zwecke der Absätze 1 und 2, etwaige erforderliche Beschränkungen der Rechte der betroffenen Person auf~~	

~~Unterrichtung und Auskunft sowie die unter diesen Umständen geltenden Bedingungen und Garantien für die Rechte der betroffenen Person festzulegen.~~	
Artikel 84 ***Geheimhaltungspflichten***	
1. Die Mitgliedstaaten können in den Grenzen dieser Verordnung die Untersuchungsbefugnisse der Aufsichtsbehörden im Sinne des Artikels 53 Absatz 2 gegenüber den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeitern, die nach einzelstaatlichem Recht oder nach von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen, regeln, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Diese Vorschriften gelten nur in Bezug auf personenbezogene Daten, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei einer Tätigkeit erlangt oder erhoben hat, die einer solchen Geheimhaltungspflicht unterliegt.	
2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Vorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.	
Artikel 85 ***Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften***	
1. Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten an, dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.	
2. Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, richten eine unabhängige Datenschutzaufsicht im Sinne des Kapitels VI ein.	

KAPITEL X
DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE

Artikel 86 ***Befugnisübertragung***	
~~1. Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.~~	Der Europäischen Kommission soll an 26 Stellen der Verordnung (vgl. Artikel 86) die Kompetenz zum Erlass von die Verordnung ergänzenden Vorschriften gegeben werden. Hierbei werden die in Artikel 290 des „Vertrages über die Arbeitsweise der Europäischen Union“ (AEUV) gesetzten Grenzen für sog. „delegierte Rechtsakte“ deutlich überschritten. Zwar sind die in Artikel 289 ff. AEUV genannten inhaltlichen oder formalen Anforderungen für delegierte Rechtsakte weit gefasst. Aus dem Zusammenspiel der Artikel 289 und 290 AEUV ergibt sich aber, dass eine Verordnung als Basisrechtsakt die wesentlichen materiellen Festlegungen nicht auf den abgeleiteten Rechtsakt übertragen darf. Dagegen beschränkt sich die Rechtsetzungsermächtigung des Verordnungsvorschlags vielfach nicht auf die Übertragung einer solchen „Konkretisierungskompetenz“, sondern überlässt der Kommission weitgehend die Befugnis, den Regelungsgehalt eigenständig festzulegen. Damit erhält die Kommission die Befugnis, im Bereich des Datenschutzes die Normen, deren einheitliche Anwendung sie nach der bisherigen Konzeption des Entwurfs überwachen soll, weitestgehend eigenständig zu schaffen. In dieser Kumulation von Rechtsetzungskompetenz und Verwaltungshandeln liegt aus unserer Sicht eine Durchbrechung des Gewaltenteilungsprinzips, die erheblichen rechtsstaatlichen Bedenken begegnet.
~~2. Die Befugnis zum Erlass delegierter~~	

~~Rechtsakte gemäß Artikel 6 Absatz 5, Artikel 8 Absatz 3, Artikel 9 Absatz 3, Artikel 12 Absatz 5, Artikel 14 Absatz 7, Artikel 15 Absatz 3, Artikel 17 Absatz 9, Artikel 20 Absatz 6, Artikel 22 Absatz 4, Artikel 23 Absatz 3, Artikel 26 Absatz 5, Artikel 28 Absatz 5, Artikel 30 Absatz 3, Artikel 31 Absatz 5, Artikel 32 Absatz 5, Artikel 33 Absatz 6, Artikel 34 Absatz 8, Artikel 35 Absatz 11, Artikel 37 Absatz 2, Artikel 39 Absatz 2, Artikel 43 Absatz 3, Artikel 44 Absatz 7, Artikel 79 Absatz 6, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 wird der Kommission auf unbestimmte Zeit ab Inkrafttreten dieser Verordnung übertragen.~~	
~~3. Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 6 Absatz 5, Artikel 8 Absatz 3, Artikel 9 Absatz 3, Artikel 12 Absatz 5, Artikel 14 Absatz 7, Artikel 15 Absatz 3, Artikel 17 Absatz 9, Artikel 20 Absatz 6, Artikel 22 Absatz 4, Artikel 23 Absatz 3, Artikel 26 Absatz 5, Artikel 28 Absatz 5, Artikel 30 Absatz 3, Artikel 31 Absatz 5, Artikel 32 Absatz 5, Artikel 33 Absatz 6, Artikel 34 Absatz 8, Artikel 35 Absatz 11, Artikel 37 Absatz 2, Artikel 39 Absatz 2, Artikel 43 Absatz 3, Artikel 44 Absatz 7, Artikel 79 Absatz 6, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Der Beschluss wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Er berührt nicht die Gültigkeit von bereits in Kraft getretenen delegierten Rechtsakten.~~	
~~4. Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.~~	
~~5. Ein delegierter Rechtsakt, der gemäß Artikel 6 Absatz 5, Artikel 8 Absatz 3, Artikel 9 Absatz 3, Artikel 12 Absatz 5, Artikel 14 Absatz 7, Artikel 15 Absatz 3, Artikel 17 Absatz 9, Artikel 20 Absatz 6, Artikel 22 Absatz 4, Artikel 23 Absatz 3, Artikel 26 Absatz 5, Artikel 28 Absatz 5, Artikel 30 Absatz 3, Artikel 31 Absatz 5, Artikel 32 Absatz 5, Artikel 33 Absatz 6, Artikel 34 Absatz 8, Artikel 35~~	

~~Absatz 11, Artikel 37 Absatz 2, Artikel 39 Absatz 2, Artikel 43 Absatz 3, Artikel 44 Absatz 7, Artikel 79 Absatz 6, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 erlassen worden ist, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb von zwei Monaten nach Übermittlung des Rechtsakts Einwände erhoben haben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.~~	
Artikel 87 ***Ausschussverfahren***	
1. Die Kommission wird von einem Ausschuss unterstützt. Bei diesem Ausschuss handelt es sich um einen Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.	
2. Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.	
3. Wird auf diesen Absatz Bezug genommen, so gilt Artikel 8 der Verordnung (EU) Nr. 182/2011 in Verbindung mit deren Artikel 5.	

KAPITEL XI

SCHLUSSBESTIMMUNGEN

Artikel 88 ***Aufhebung der Richtlinie 95/46/EG***	
1. Die Richtlinie 95/46/EG wird aufgehoben.	
2. Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser	

Verordnung errichteten Europäischen Datenschutzausschuss.	
Artikel 89 ***Verhältnis zur Richtlinie 2002/58/EG und Änderung dieser Richtlinie***	
1. Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/85/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.	
2 Artikel 1 Absatz 2 der Richtlinie 2002/58/EG wird gestrichen.	
Artikel 90 ***Bewertung***	
Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig einen Bericht zur Bewertung und Überprüfung dieser Verordnung vor. Der erste Bericht wird spätestens vier Jahre nach Inkrafttreten dieser Verordnung vorgelegt. Danach wird alle vier Jahre ein weiterer Bericht vorgelegt. Die Kommission legt geeignete Vorschläge zur Änderung dieser Verordnung und zur Anpassung anderer Rechtsinstrumente vor, die sich insbesondere unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen können. Die Berichte werden veröffentlicht.	
Artikel 91 ***Inkrafttreten und Anwendung***	
1. Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.	
2. Ihre Anwendung beginnt <u>für nach dem in Absatz 1 genannten Zeitpunkt verarbeiteten</u>	Die Regelung sollte für Bestandsdaten eine

personenbezogenen Daten [*zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt*]. Für vor dem in Absatz 1 genannten Zeitpunkt verarbeiteten personenbezogenen Daten beginnt die Anwendung fünf Jahre nach dem in Absatz 1 genannten Zeitpunkt. 3. Ergibt sich die Rechtmäßigkeit der Verarbeitung aus einer vor dem in Absatz 1 genannten Zeitpunkt erteilten Einwilligung der betroffenen Person, so behält diese Einwilligung ihre Gültigkeit.	längere Übergangsvorschrift vorsehen. Darüber hinaus bedarf für bestehende Einwilligungserklärungen eines Bestandschutzes. Es wäre ein erheblicher administrativer Aufwand, bestehende Einwilligungserklärungen, wie z.B. die SCHUFA-Klausel, nach dem Inkrafttreten der Verordnung neu einholen zu müssen.
Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.	