

Deutsche Kreditwirtschaft Stand: 21.3.2012

Anmerkungen zu einzelnen Regelungen (Artikel 1 bis 21)

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
<i>Artikel 1</i> <i>Gegenstand und Ziele</i>	
1. Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.	<p>Das Rechtsinstrument der Verordnung führt in begrüßenswerter Weise zu einer Rechtsvereinheitlichung im Binnenmarkt. Jedoch müssen folgende Spannungsfelder angemessen geklärt werden:</p> <ul style="list-style-type: none">• 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

	<p>Geldwäsche-, Korruptions- und Betrugsbekämpfung, bankaufsichtsrechtliche Regeln zum Scoring, Datenschutzvorschriften im Telemediengesetz),</p> <ul style="list-style-type: none"> • Verhältnis zu den in einigen Staaten geltenden gesetzlichen Regelungen zum Bankgeheimnis. <p>Positiv zu bewerten ist, dass sich die Regelungen des Verordnungsvorschlags (VO) auf den Schutz personenbezogener Daten von <u>natürlichen</u> Personen beschränken sollen, vgl. auch Erwägungsgrund 12. Dies entspricht dem bisherigen Ansatz der EU-Datenschutzrichtlinie und des Bundesdatenschutzgesetzes. Daten juristischer Personen sollten weiterhin nicht in den Anwendungsbereich der VO aufgenommen werden.</p>
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.	
<p><i>Artikel 2</i></p> <p><i>Sachlicher Anwendungsbereich</i></p>	-
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 sollen.	Entspricht dem Anwendungsbereich des BDSG. Erwägungsgrund 13 verdeutlicht, dass Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, nicht in den Anwendungsbereich der VO fallen.
2. Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird	

a) im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt, etwa im Bereich der nationalen Sicherheit,	Fraglich ist die Relevanz dieser EU-rechtlich geprägten Abgrenzung für nicht-öffentliche Stellen. Überlagert die Verordnung Datenschutzvorschriften beispielsweise im Sozialrecht, Betriebsverfassungsgesetz, Strafrecht, Gesellschaftsrecht und Telekommunikationsrecht? Diese Gesetze fallen entweder gar nicht oder nur teilweise in die Zuständigkeit des EU-Gesetzgebers.
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 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.	Zwar wird eine Abgrenzung zur E-Privacy-Richtlinie vorgenommen. Jedoch dürfte die Regelung in der Praxis wegen ihrer Unschärfe zu Anwendungsproblemen führen.
	<p>Wie schon zu Artikel 1 dargelegt, fehlt eine Abgrenzungsregelung zu bereichsspezifischen Datenschutzregelungen in anderen EU-RiL (z.B. EU-Verbraucherkredit-RiL). Weiter ist klärungsbedürftig, wiesich die Regelungen auf bestehende nationale, bereichsspezifische datenschutzrechtliche Regelungen aus wirken (z. B. im Telemediengesetz, Telekommunikationsgesetz).</p> <p>Zudem stellt sich die Frage, wie sich die VO auf bestehende Spezialgesetze auswirkt, wie diese z. B. im Bankaufsichtsrecht in § 10 Abs. 1 Satz 3ff. Kreditwesengesetz, § 25c</p>

	Abs. 2 Kreditwesengesetz geregelt sind.
<i>Artikel 3</i> 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 ist zu bedenken, dass die Exterritorialitätsvorschrift auch für Töchter deutscher Kreditinstitute in Drittstaaten relevant (z.B. Bank in den USA) ist, 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 wird. 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 hoheitliche Eingriffen (z.B. strafrechtlichen Beschlagnahmen) unterliegt.
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.	
<i>Artikel 4</i> 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;	<p>Positiv zu bewerten ist, dass nach Erwägungsgrund 23 die VO keine Anwendung auf anonymisierte Daten findet, so dass die betroffene Person nicht mehr identifiziert werden kann. Offen bleibt auch nach Erwägungsgrund 24, ob IP-Adressen oder Cookie-Kennungen personenbezogen sind.</p> <p>Insgesamt ist mit der Regelung wohl eine Erweiterung des Anwendungsbereichs verbunden, weil maßgeblich auf die objektive Bestimmbarkeit abgestellt wird: Schon die Kombination Kontonummer und Bankleitzahl (zukünftig IBAN) dürfte damit ein personenbezogenes Datum sein, auch wenn der Empfänger dieser Daten über kein Zusatzwissen verfügt, welche Person sich hinter diesem Pseudonym verbirgt. Bisher 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 zu setzen.</p> <p>WICHTIG: Es sollte die Pseudonymisierung sowie die Anonymisierung unmittelbar in Artikel 4 definiert werden und dieses Vorgehen als datenschutzfreundliche Vorgehensweise privilegiert werden.</p>
(2) „personenbezogene Daten“ alle Informationen, die sich auf eine betroffene Person beziehen;	
(3) „Verarbeitung“ jeden mit oder ohne	Entspricht grundsätzlich Artikel 2 Abs. b der

<p>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 <u>an Empfänger</u>, der Abgleich oder die Verknüpfung sowie das Löschen, <u>Sperren</u>—oder Vernichten der Daten;</p>	<p>EU-Datenschutzrichtlinie. Es ist aber nicht ersichtlich, warum das „Sperren“ aus dem Katalog der Verarbeitungstatbestände gestrichen worden ist. Das „Sperren“ sollte in die Definition aufgenommen werden.</p> <p>Zudem sollte der Begriff „Löschen“ wie in § 3 Abs. 4 Nr. 5 BDSG definiert werden als: „<i>das Unkenntlichmachen gespeicherter personenbezogener Daten</i>“. Dies ist insbesondere zur Erfüllung der Anforderungen in Artikel 17 VO notwendig.</p> <p>Das Tatbestandsmerkmal der Übermittlung sollte auf Datenweiterleitungen an „Empfänger“ beschränkt werden, vgl. insoweit auch die folgende Kommentierung zu Abs. 7.</p>
<p>(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;</p>	
<p>(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;</p>	<p>Neu ist die gemeinsame Verantwortung von datenverarbeitenden Stellen (vgl. auch Art. 24). Beispiel SWIFT als joint controller. Ansatz „share dataprocessing“ und „joint controller“.</p>

(6) "Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;	Abgrenzung zur gemeinsamen Verantwortung (Ausnahme Art. 26 Abs. 4 bei Verstoß).
(7) "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, <u>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;</u>	Im Unterschied zur EU-Datenschutzrichtlinie unterscheidet der Verordnungsentwurf nicht mehr zwischen „Dritter“ und „Empfänger“. Stattdessen wird die Definition des „Dritten“ aus Artikel 2 f) der EU-Datenschutzrichtlinie für den Begriff „Empfänger“ verwendet. Allerdings sollte gem. Artikel 2 f) der EU-Datenschutzrichtlinie beim Begriff „Empfänger“ klargestellt werden, dass dies nur Stellen außerhalb der verantwortlichen Stelle sind. Vgl. insoweit auch oben die Ergänzung in 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;	Angesichts der Rahmenbedingungen gerade im elektronischen Geschäftsverkehr ist positiv zu bewerten, dass die Einwilligung nicht der Schriftform bedarf, wie dies aktuell - in Abweichung von der EU-Datenschutzrichtlinie - nach § 4a BDSG der Fall ist. Wie auch das BDSG wird eine informierte Einwilligungserklärung vorausgesetzt, vgl. Erwägungsgrund 25. Kritisch zu hinterfragen ist jedoch Erwägungsgrund 33, der vorgibt, dass 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 Anforderungen dürften über die aktuellen Anforderungen an die Freiwilligkeit einer Einwilligungserklärung hinausgehen, so dass Erwägungsgrund 33 besser wie § 4a Abs. 1 BDSG formuliert werden sollte, wonach „die Einwilligung nur wirksam ist, wenn sie auf der freien Entscheidung des Betroffenen beruht.“
(9) "Verletzung des Schutzes personenbezogener Daten" eine	Die Definition ist im Zusammenspiel der in der VO geregelten Meldepflicht eine

	<p>schwerwiegende Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder widerrechtlich, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;</p>	<p>erhebliche Erweiterung zu § 42a BDSG.. Um eine unsinnige Meldeflut zu vermeiden, sollte schon auf Definitionsebene die Meldepflicht auf schwerwiegende Beeinträchtigungen wie in § 42a BDSG beschränkt werden.</p> <p>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.</p>
(10)	<p>„genetische Daten“ Daten <u>- mit Ausnahme des Geschlechts -</u> jedweder Art zu den ererbten oder während der vorgeburtlichen Entwicklung erworbenen Merkmalen eines Menschen;</p>	<p>Es ist zu weitgehend, auch das Geschlecht eines Menschen als genetisches Datum zu erfassen, da dieses häufig schon aus dem Namen bzw. der Anrede erkennbar ist.</p>
(11)	<p>„biometrische Daten“ Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die dessen eindeutige Identifizierung ermöglichen, wie Gesichtsbilder oder daktyloskopische Daten <u>(;die Unterschrift des Betroffenen ist ausgenommen);</u></p>	<p>Siehe auch Art. 33 Abs. 2 d).</p> <p>Die neue Datenart kann Relevanz bekommen bei biometrischen Authentifizierungsverfahren (Iriserkennung, Fingerabdruck, etc.). Jedenfalls sollte definitorisch festgehalten werden, dass die Unterschrift eines Menschen nicht unter den Begriff fällt, weil damit viele Lebenssachverhalte in den Anwendungsbereich einer Folgenabschätzung nach Art. 33 fallen würden.</p>
(12)	<p>„Gesundheitsdaten“ Informationen, die sich auf den körperlichen oder geistigen Gesundheitszustand einer Person oder auf die Erbringung von Gesundheitsleistungen für die betreffende Person beziehen;</p>	<p>Relevant bei Mitarbeiterdaten sowie ggf. bei Betreuungs-sachverhalten (Führung von Konten für unter gesetzlicher Betreuung stehender Personen).</p>
(13)	<p>„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</p>	

	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“ 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;	
(15)	„Unternehmen“ jedes Gebilde, das eine <u>selbständige</u> wirtschaftliche Tätigkeit ausübt, unabhängig von seiner Rechtsform, das heißt vor allem natürliche und juristische Personen sowie Personengesellschaften oder Vereinigungen, die regelmäßig einer <u>selbständigen</u> wirtschaftlichen Tätigkeit nachgehen;	= juristische Person, Gewerbetreibende, Einzelkaufleute, Freiberufler (<u>nicht</u> Verbraucher), Klarstellung, dass nicht Mitarbeiter eines Unternehmens erfasst sind.
(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
<i>Artikel 5</i> 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 für die betroffene Person nachvollziehbaren Weise verarbeitet werden;	Es sollte nicht auf die subjektive Nachvollziehbarkeit jeder einzelnen betroffenen Person abgestellt werden, da diese kaum bestimmbar sein dürfte. Vielmehr sollte im Rahmen des Rechtmäßigkeitsprinzips auf eine allgemeine Nachvollziehbarkeit für den Durchschnitt der 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 <u>Maß ausgerichtet sein</u> Mindestmaß beschränkt sein; sie dürfen nur verarbeitet werden, wenn	Der Zweckbindungsgrundsatz sollte nicht mit dem Grundsatz der Datensparsamkeit und -vermeidung vermischt werden. Zudem könnte eine Kollision mit

<p>und solange die Zwecke der Verarbeitung nicht durch die Verarbeitung von anderen als personenbezogenen Daten erreicht werden können;</p>	<p>Datenverarbeitungen aufgrund vom Betroffenen freiwillig erteilten Angaben auftreten.</p>
<p>d) sachlich richtig und, <u>wenn nötig</u>, 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;</p>	<p>Die Einschränkung „wenn nötig“ aus Art. 6 Abs. 1 d) EU-Datenschutzrichtlinie sollte beibehalten werden, um die Überprüfungszyklen von der tatsächlichen Notwendigkeit abhängig machen zu können, die sich nach Datenart und Verarbeitungszweck erheblich unterscheiden kann.</p> <p>Es sollte überlegt werden, eine Mitwirkungspflicht des Betroffenen zu normieren, die verantwortliche Stelle über Änderungen in seiner Sphäre zu informieren.</p>
<p>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 Einklang mit den Vorschriften und Modalitäten des Artikels 83 verarbeitet werden und die Notwendigkeit ihrer weiteren Speicherung in regelmäßigen Abständen überprüft wird;</p>	<p>Zu begrüßen ist, dass im Gegenschluß bei Zweckablauf die Daten noch in anonymisierter Form weiterverarbeitet werden dürfen.</p> <p>Es sollten die besonderen Anforderungen der gesetzlichen handels- und steuerrechtlichen sowie bankaufsichtsrechtlichen Aufbewahrungspflichten, u. a. § 146 AO, §§ 256, 257 HGB, § 34 Abs. 3 WpHG, § 8 Abs. 3 GwG, Berücksichtigung finden.</p>
<p>f) unter der Gesamtverantwortung des für die Verarbeitung Verantwortlichen verarbeitet werden, der dafür haftet, dass bei <u>jedem Verarbeitungsverfahren</u> jedem Verarbeitungsvorgang die Vorschriften dieser Verordnung eingehalten werden, und der den Nachweis hierfür erbringen muss.</p>	<p>Die deutsche Fassung weicht deutlich von der englischen Fassung ab, die lautet:</p> <p><i>“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”</i></p> <p>So ist insbesondere der Begriff „Gesamtverantwortung“ unklar und dieser deckt sich nicht mit der englischen Fassung.</p> <p>Die Rechtsnatur der Vorschrift ist unklar. Gilt diese nur in Bezug auf eine zivilrechtliche Haftung oder auch verwaltungsrechtlich gegenüber der Aufsichtsbehörde oder im</p>

	<p>Sanktionsverfahren (Strafrecht, Ordnungswidrigkeit)? Diese müsste vom Anwendungsbereich auf eine zivilrechtliche Haftung beschränkt werden, da eine mit der Nachweispflicht einhergehende Beweislastumkehr nicht mit rechtsstaatlichen Grundsätzen im Verwaltungs- und Strafrecht vereinbar wäre.</p> <p>Es sollte nicht an einzelne Verarbeitungsvorgänge, sondern an Verarbeitungsverfahren angeknüpft werden.</p>
<p><i>Artikel 6</i> Rechtmäßigkeit der Verarbeitung</p>	
<p>1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:</p>	
<p>a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben.</p>	.
<p>b) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die <u>im Interesse auf Antrag</u> der betroffenen Person erfolgen.</p>	<p>Entspricht Art. 7 Abs. b der EU-Datenschutzrichtlinie.</p> <p>Das Tatbestandsmerkmal „auf Antrag“ ist zu formal und bildet nicht ein vorvertragliches Schuldverhältnis ab.</p>
<p>c) Die Verarbeitung ist zur Erfüllung einer gesetzlichen <u>Verpflichtung oder Erlaubnis, einer aufsichtsrechtlichen Anforderung oder einer anderen Rechtsvorschrift</u> erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.</p>	<p>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.“</p>
<p>d) Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person zu schützen.</p>	

<p>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.</p>	
<p>f) Die Verarbeitung ist <u>erforderlich zur Wahrung des berechtigten Interesses</u>, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, 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.</p>	<p>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</p> <p>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.</p> <p>Sofern eine Datenverarbeitung nach Art. 6 Abs. 1 f legitimiert ist, wäre es bloßer Formalismus, wenn der Betroffene, wie es in Erwägungsgrund 38 vorgesehen ist, vom Verantwortlichen über sein Widerspruchsrecht informiert werden muss und er seine berechtigten Interessen gegenüber dem Betroffenen ausdrücklich darlegen muss.</p> <p>Über die Interessenabwägung müsste auch die Verarbeitung öffentlich zugänglicher Daten erfasst sein (vgl. § 28 Absatz 3 BDSG).</p>
<p>2. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke unterliegt den Bedingungen und Garantien des Artikels 83.</p>	
<p>3. Die Verarbeitungen gemäß Absatz 1 Buchstaben c und e <u>müssen einer gesetzlichen Verpflichtung oder Erlaubnis, einer aufsichtsrechtlichen Anforderung oder einer anderen Rechtsvorschrift eine</u></p>	<p>Gleichlauf mit Kommentierung zu Art. 6 Abs. 1c.</p>

Rechtsgrundlage haben im	
a) Unionsrecht oder	
b) Recht des Mitgliedstaats <u>unterliegen</u> , 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.	Die Anforderungen dürfen nur dem nationalen Gesetzgeber auferlegt werden. Der Datenverarbeiter darf auf die Legalität der Gesetzgebung vertrauen dürfen.
4. Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e <u>f</u> genannten Gründe zutreffen. Dies gilt insbesondere bei Änderungen von Geschäfts- und allgemeinen Vertragsbedingungen.	Satz 1: Eine Änderung des Verarbeitungszwecks sollte grundsätzlich im Rahmen einer Interessenabwägung nach Artikel 7 Absatz 1 f VO-E möglich bleiben. Satz 2: Streichung des zweiten Satzes, da aus der mit dem Betroffenen vereinbarten Vertragsänderung bereits eine Veränderung des Verarbeitungszwecks folgt und vom Betroffenen 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.	Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch erfassen.
<i>Artikel 7 Einwilligung</i>	
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	

<p>schriftliche Erklärung erfolgen, die noch einen anderen Sachverhalt betrifft, muss das Erfordernis der Einwilligung äußerlich erkennbar von dem anderen Sachverhalt getrennt werden.</p>	
<p>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.</p>	
<p>4. Die Einwilligung bietet keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht.</p>	<p>Gemäß Artikel 7 Absatz 4 der Verordnung 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“ 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.</p> <p>Folglich sollte Absatz 4 gestrichen werden. Die Einwilligung muss stets einen Datenverarbeitungsvorgang legitimieren können.</p>
<p><i>Artikel 8</i> <i>Verarbeitung personenbezogener Daten eines Kindes</i></p>	
<p>1. Für die Zwecke dieser Verordnung ist die Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten dreizehnten Lebensjahr, dem direkt Dienste der Informationsgesellschaft angeboten werden,</p>	

<p>nur rechtmäßig, wenn und insoweit die Einwilligung hierzu durch die Eltern oder den Vormund des Kindes oder mit deren Zustimmung erteilt wird. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen, um eine nachprüfbare Einwilligung zu erhalten.</p>	
<p>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.</p>	
<p>3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten und Anforderungen in Bezug auf die Art der Erlangung einer nachprüfbaren Einwilligung gemäß Absatz 1 näher zu regeln. Dabei zieht die Kommission spezifische Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen in Betracht.</p>	<p>Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch erfassen.</p>
<p>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.</p>	<p>Die Entwicklung von Vordrucken und Formularen sollte den Verwendern und nicht der Kommission obliegen. Eine gesetzliche Standardisierung würde zu einer erheblichen Bürokratisierung führen.</p>
<p style="text-align: center;"><i>Artikel 9</i> Verarbeitung besonderer Kategorien von personenbezogenen Daten</p>	
<p>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 Sicherungsmaßnahmen ist untersagt.</p>	<p>Bislang sind in Artikel 8 der Datenschutzrichtlinie Daten über Strafurteile keine sensible Daten:</p> <p>„Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.“</p> <p>Die Aufnahme dieser Datenart wäre für –</p>

	<p>auch bankaufsichtsrechtlich erforderlichen – Sicherheitsüberprüfungen ein problematisches Verarbeitungshindernis. Deshalb sollte diese Datenkategorie aus dem Katalog der sensiblen Daten gestrichen werden.</p> <p>Es sollte besser bei der autonomen Sonderregelung in Artikel 8 Absatz 5 der Richtlinie bleiben und dort die besonderen Aspekte heutiger Complianceanforderungen berücksichtigt werden. Artikel 8 Absatz 5 der Richtlinie lautet:</p> <p>Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen 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.</p> <p>Die Mitgliedstaaten können vorsehen, daß Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.</p>
<p>2. Absatz 1 gilt nicht in folgenden Fällen:</p>	
<p>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</p>	
<p>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</p>	

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 <u>oder eine zivilrechtliche Pflicht gegenüber dem Betroffenen</u> zu erfüllen, oder	<p>Hierüber dürfen alle gesetzlichen Verarbeitungspflichten einer Bank mit öffentlichen Bezug (z.B. im Rahmen des Steuerrechts, der Geldwäschebekämpfung, 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.</p> <p>Nicht abgedeckt wird hingegen die Erfüllung gesetzlicher Pflichten aus dem Zivilrecht. So wird nach dem Zahlungsdiensterecht (das auf</p>

	der EU-Zahlungsdiensterichtlinie beruht) ein Zahlungsdienstleister z.B. verpflichtet, die Daten, die vom Kunden im Verwendungszweck 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 Sicherungsmaßnahmen 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.	<p>Siehe oben, Übernahme des bisherigen Artikel 8 Absatz 5 der Richtlinie:</p> <p>Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen 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.</p> <p>Die Mitgliedstaaten können vorsehen, daß Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.</p>
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	Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch

2 genannten Ausnahmen näher zu regeln.	erfassen.
<i>Artikel 10</i> 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
<i>Artikel 11</i> Transparente Information und Kommunikation	
<p>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.</p> <p><u>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.</u></p>	<p>Die deutsche Fassung weicht erheblich von der englischen Fassung ab, diese lautetet:</p> <p><i>"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."</i></p> <p>Die englische Fassung ist verständlicher und eher umsetzbar als die deutsche Fassung. Gleichwohl darf nicht verkannt werden, dass gerade für kleine und mittlere Unternehmen, die Aufstellung von Datenschutzgrundsätze eine neue bürokratische Belastung darstellen kann.</p>
<p>2. Der für die Verarbeitung Verantwortliche stellt der betroffenen Person alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten für den Betroffenen hat in verständlicher Form unter Verwendung einer klaren, und einfachen und adressatengerechten Sprache zu erfolgenr Verfügung, besonders dann,</p>	<p>Die Vorgabe „adressatengerecht“ ist kaum umsetzbar, denn sie würde in der Konsequenz bedeuten, eine Vielzahl unterschiedlicher Informationsangebote bedeuten. Es reicht das Transparenzgebot.</p>

wenn die Information an ein Kind gerichtet ist.	
<p><i>Artikel 12</i></p> <p><i>Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann</i></p>	
<p>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 <u>ermöglichen</u>erleichtern. Im Falle, dass der für die Verarbeitung Verantwortliche gegenüber dem Betroffenen ausschließlich auf elektronischem Wege kommuniziert, der automatisierten Verarbeitung personenbezogener Daten sorgt der für die Verarbeitung Verantwortliche dafür, dass die Maßnahme elektronisch beantragt werden kann.</p>	<p>Satz 1: Der erste Satz ist eigentlich nicht notwendig, da jede gesetzliche Anforderung vollzogen werden muss.</p> <p>Satz 2: Die Formulierung „erleichtern“ in Satz 2 ist unbestimmt und bereitet nur Raum für nicht zielführende Diskussionen, ob ein Unternehmen diese Anforderungen erfüllt hat. Besser ist darauf abzustellen, dass die verantwortliche Stelle</p> <p>Satz 3: Zudem folgt nicht zwingend aus dem Umstand, dass Daten automatisiert verarbeitet werden, dass das Unternehmen auch über die technischen Mittel verfügt, dass „die Maßnahme elektronisch beantragt werden kann“. 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.</p>
<p>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 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 <u>der für die Verarbeitung Verantwortliche darlegen kann,</u></p>	<p>Satz 2: Eine Möglichkeit der Verlängerung der Reaktionsfrist ist sowohl bei massenhaften Anfragen als auch bei komplexen Sachverhalten erforderlich.</p> <p>Satz 3: Auskünfte sollen nach der englischen Fassung „in writing“ erteilt werden. Die Schriftform geht darüber hinaus, so dass das Tatbestandsmerkmal „in Textform“ vorzugswürdig ist.</p> <p>Satz 4: Zudem muss es dem Verantwortlichen obliegen, zu entscheiden, in welcher Form er</p>

<p>dass die Bearbeitung innerhalb der Frist nach <u>Satz 1 nicht mit verhältnismäßigem Aufwand möglich ist, oder die</u> ihre Zusammenarbeit <u>der Betroffenen</u> 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 <u>schriftlich in Textform</u> zu erfolgen. Stellt die betroffene Person den Antrag in elektronischer Form, ist sie auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.</p>	<p>dem Betroffenen Auskunft erteilt. Eine elektronische Auskunftserteilung kann auch im Interesse des Betroffenen nur erfolgen, wenn der Auskunftssuchende sich eindeutig authentifiziert hat (z.B. mittels elektronischem Identitätsnachweis des Personalausweises) und der Auskunftssuchende eine technisch sicher Übertragung technisch unterstützen kann (z.B. verschlüsselte Datenübermittlung).</p> <p>Die Antwortfrist von einem Monat sollte wie bereits vorgesehen Ausnahmen zulassen, beispielsweise bei Massenauskunftersuchen, die eine längere Bearbeitungszeit bedeuten können. Dabei sollte eine „geeignete“ Fristverlängerung akzeptiert werden.</p>
<p>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.</p>	
<p>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.</p>	
<p>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.</p>	<p>Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch erfassen.</p>
<p>6. Die Kommission kann Standardvorlagen und Standardverfahren für</p>	<p>Die Entwicklung von Vordrucken und Formularen sollte den Verwendern obliegen.</p>

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.	Eine Standardisierung würde zu einer erheblichen Bürokratisierung führen.
<i>Artikel 13</i> Rechte gegenüber Empfängern	
Sofern ein berechtigtes Interesse des Betroffenen besteht, teilt dDer 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
<i>Artikel 14</i> Information der betroffenen Person	
1. Einer Person, von der personenbezogene Daten erhoben werden, stellt teilt der für die Verarbeitung Verantwortliche zumindest <u>folgende</u>	1. Grundsätzliches Transparenz für den von der Datenverarbeitung Betroffenen ist sicherlich

<p><u>Informationen Folgendes zur Verfügung mit:</u></p>	<p>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:</p> <p>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).</p> <p>2. Berücksichtigung des Umweltschutzes bei Art und Weise der Informationserteilung</p> <p>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.÷</p>
<p>a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters <u>und auf Nachfrage die für Datenschutz zuständige</u></p>	<p>Die Nennung des Namens und die Kontaktdaten des für die Verarbeitung Verantwortlichen ist ausreichend, damit der Betroffene den für die Verarbeitung</p>

<p>Stelle und des Datenschutzbeauftragten,</p>	<p>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.</p>
<p>b) die Zwecke, für die Daten verarbeitet werden, einschließlich der Geschäfts- und allgemeinen Vertragsbedingungen, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe b gründet, beziehungsweise auf Nachfrage die von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen, wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht,</p>	<p>Die Regelung sollte wie Art. 10 Abs. b der EU-Datenschutzrichtlinie gefasst werden, um zusätzlichen bürokratischen Aufwand zu vermeiden.</p> <p>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.</p> <p>Eine Darstellung der von der verantwortlichen Stelle verfolgten berechtigten Interessen ist ein unnötiger Formalismus und bringt keinen Informationsgewinn. Nur in den Fällen, in denen der Betroffene hierzu ausdrücklich nachfragt, sollte diese Information bedarfsgerecht erfolgen.</p>
<p>c) die Dauer, für die die personenbezogenen Daten gespeichert werden,</p>	<p>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. Insofern muss eine generische Beschreibung ausreichen.</p>
<p>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</p>	<p>Diese Information ist redundant, da diese bereits von Artikel 11 Absatz 1 abgedeckt ist. Zudem kann es nicht alleine die Aufgabe der verantwortlichen Stelle sein, den Betroffenen über seine gesetzlichen Pflichten aufzuklären.</p>

dieser Daten,	
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 <u>zur Verfügung gestellten</u> genannten Informationen außerdem mit, ob die Bereitstellung der Daten obligatorisch oder fakultativ ist und welche mögliche Folgen die Verweigerung der Daten hätte.	Folgeänderung zu Absatz 1
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 <u>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.</u>	Entspricht weitgehend Art. 11 der EU-DSR. 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 <u>stellt</u> die Informationen gemäß den Absätzen 1, 2 und 3 <u>zur Verfügung</u>	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 <u>hat bereits auf andere Weise Kenntnis</u> verfügt bereits über die Informationen gemäß den Absätzen 1, 2 und 3 <u>erlangt</u> , oder	Die praxisgerechte Formulierung in § 4 Abs. 3 Satz 1 BDSG sollte übernommen werden, um unnötige Formalismen bei 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 <u>erfolgt ist zur Erfüllung einer gesetzlichen Pflicht oder im Rahmen einer gesetzlichen Erlaubnis, einer aufsichtsrechtlichen Anordnung oder einer sonstigen Rechtsvorschrift</u> , 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 <u>des für die Verarbeitung Verantwortlichen oder anderer Personen</u> ein.	Die Regelung ist ein Korrektiv beim Aufeinandertreffen unterschiedlicher Grundrechtspositionen. Auch die Rechte der verantwortlichen Stelle müssen daher einbezogen werden.
6. Im Fall des Absatzes 5 Buchstabe b ergreift der für die Verarbeitung	

Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person.	
<p>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 Kleinunternehmen sowie mittlere Unternehmen.</p>	<p>Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch erfassen.</p>
<p>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 verschiedenen Sektoren und Verarbeitungssituationen berücksichtigt. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.</p>	<p>Die Entwicklung von Vordrucken und Formularen sollte den Verwendern obliegen. Eine Standardisierung würde zu einer erheblichen Bürokratisierung führen.</p>
<p><i>Artikel 15</i> Auskunftsrecht der betroffenen Person</p>	
<p>1. Die betroffene Person <u>kann</u> 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, <u>informiert</u> teilt der für die Verarbeitung Verantwortliche <u>über</u> Folgendes, <u>soweit dem Betroffenen die Informationen nicht bereits erteilt wurden</u> mit:</p>	<p>Zu Satz 1: Vermeidung, dass der Auskunftsanspruch von Dritten instrumentalisiert wird (z.B. Missbrauch der „Selbstauskunft“ des Mieters auf Veranlassung des Vermieters zur Bonitätsprüfung).</p> <p>Klarstellung, dass der dargestellte Anspruch nur zu Zwecken von datenschutzrechtlichen Rechten geltend gemacht werden darf und nicht einen allgemeinen Ausforschungsanspruch gegen den Verantwortlichen im Zivilprozess darstellt oder zur Verwendung in Strafprozessen</p>

	<p>zweckentfremdet werden darf.</p> <p>Zu Satz 2: Redaktionelle Anpassung. Sind dem Betroffenen bereits die Informationen erteilt worden (beispielsweise mit den Vertragsunterlagen oder im Wege der Erfüllung von Rechnungslegungspflichten) besteht kein datenschutzrechtlicher – kostenloser - Auskunftsbedarf.</p>
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 Widerspruchsrechts 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,	Über das Bestehen gesetzlicher Ansprüche sollte im Rahmen einer Vertragsbeziehung nicht noch zusätzlich informiert werden müssen
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 adressatengerechte Aufbereitung der beim Verantwortlichen verarbeiteten Daten.
h) die Tragweite der Verarbeitung und die mit ihr angestrebten Auswirkungen,	Artikel 20 könnte auch Scoring-Verfahren betreffen. Insofern ist es notwendig, dass das

<p>zumindest im Fall der Maßnahmen gemäß Artikel 20.</p>	<p>Auskunftsrecht sich nicht auch auf die Art und Weise der Funktion von Scoring-Verfahren bezieht. Vorzugswürdig erscheint es, wenn der im Erwägungsgrund 51 angedachte Schutz des Geschäftsgeheimnisses, des geistigen Eigentums und des Urheberrechts unmittelbar in Artikel 14 der VO verortet wird.</p>
<p>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.</p>	<p>Satz 1 ist redundant siehe Abs. 1 g). Zu Satz 2: Es muss dem Verantwortlichen obliegen, zu entscheiden, in welcher Form er dem Betroffenen Auskunft erteilt. Ggf. sprechen Sicherheitsaspekte gegen eine Beauskunftung in elektronischer Form. Dies betrifft die ggf. nicht mögliche Identifizierung des Anfragenden sowie die Sicherheit der Übertragungswege.</p>
<p>3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten zu den Kriterien und Anforderungen in Bezug auf die Mitteilung über den Inhalt der personenbezogenen Daten gemäß Absatz 1 Buchstabe g an die betroffene Person festzulegen.</p> <p><u>Eine Auskunftspflicht besteht nicht, wenn</u></p> <p><u>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,</u></p> <p><u>b. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,</u></p> <p><u>c. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,</u></p> <p><u>d. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat,</u></p>	<p>Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch erfassen.</p> <p>Stattdessen sollten analog zu § 33 Abs. 2 BDSG in der Verordnung Beschränkungen des Auskunftsrechts normiert werden, die sich insbesondere auf Geschäftsgeheimnisse und Eigentumsrechte des Verantwortlichen beziehen, vgl. dazu auch Erwägungsgrund 51 der VO. Darüber hinaus sind für die Kreditwirtschaft insbesondere auch Beschränkungen aufgrund gesetzlicher Schweigepflichten wie z.B. § 12 GwG relevant.</p>

<p><u>dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden würde,</u> <u>e. die Daten für eigene Zwecke gespeichert sind und</u> <u>aa) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder</u> <u>bb) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,</u></p>	
<p>4. Die Kommission kann Standardvorlagen und -verfahren für 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.</p>	<p>Die Entwicklung von Vordrucken und Formularen sollte den Verwendern obliegen. Eine Standardisierung würde zu einer erheblichen Bürokratisierung führen.</p>

ABSCHNITT 3

BERICHTIGUNG UND LÖSCHUNG

Regelung ggf. mit Änderungsvorschlag	Anmerkungen
<p style="text-align: center;"><i>Artikel 16</i> <i>Recht auf Berichtigung</i></p>	
<p>Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Berichtigung von unzutreffenden personenbezogenen Daten zu verlangen. Die betroffene Person hat das Recht, die Vervollständigung unvollständiger personenbezogener Daten, auch in Form eines Korrigendums, zu verlangen, soweit dies für</p>	<p>Der Fall der Strittigkeit der Richtigkeit von Daten ist nicht bedacht.</p> <p>Ein Ergänzungsanspruch – auch in Form des Korrigendums - sollte nur dann bestehen, wenn dies für den Verarbeitungszweck erforderlich ist.</p>

den Verarbeitungszweck erforderlich ist.	
<p style="text-align: center;"><i>Artikel 17</i></p> <p style="text-align: center;">Recht auf Vergessenwerden und auf Löschung</p>	
<p>1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten zu verlangen, speziell wenn es sich um personenbezogene Daten handelt, die die betroffene Person im Kindesalter öffentlich gemacht hat, sofern einer der folgenden Gründe zutrifft:</p>	
<p>a) Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.</p>	<p>Wir gehen davon aus, dass die „Verarbeitung auf sonstige Weise“ auch zulässige Zweckänderungen umfasst. Bei Beendigung eines Vertrages kann es noch nachvertragliche Pflichten geben, die einer Datenlöschung bzw. –sperrung entgegenstehen können.</p>
<p>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.</p>	
<p>c) Die betroffene Person legt gemäß Artikel 19 Widerspruch gegen die Verarbeitung ein.</p>	
<p>d) Die Verarbeitung der Daten ist aus anderen Gründen nicht mit der Verordnung vereinbar.</p>	<p>Eine generelle Auffangbestimmung für einen Löschungsanspruch ist unpraktikabel. Die Verordnung muss die Fälle genau bestimmen, in den der Betroffene einen Löschungsanspruch hat.</p>
<p>2. Hat der in Absatz 1 genannte für die Verarbeitung Verantwortliche die personenbezogenen Daten öffentlich gemacht, unternimmt er in Bezug auf die</p>	

<p>Daten, für deren Veröffentlichung er verantwortlich zeichnet, alle vertretbaren Schritte, auch technischer Art, um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt. Hat der für die Verarbeitung Verantwortliche einem Dritten die Veröffentlichung personenbezogener Daten gestattet, liegt die Verantwortung dafür bei dem für die Verarbeitung Verantwortlichen.</p>	
<p>3. Der für die Verarbeitung Verantwortliche sorgt <u>unter den Voraussetzungen des Absatzes 1</u> für eine umgehende Löschung der personenbezogenen Daten, soweit deren Speicherung nicht erforderlich ist</p>	<p>Das Verhältnis zu Absatz 1 ist klarzustellen.</p>
<p>(a) zur Ausübung des Rechts auf freie Meinungsäußerung gemäß Artikel 80;</p>	
<p>(b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 81;</p>	
<p>(c) für historische und statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung gemäß Artikel 83;</p>	
<p>(d) zur Erfüllung einer gesetzlichen <u>oder aufsichtsrechtlichen</u> 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</p>	<p>Ergänzung um aufsichtsrechtliche Vorgaben. Es obliegt nicht dem Verantwortlichen, die Zielsetzung nationalen Rechts zu prüfen.</p>

angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen muss;	
(e) in den in Absatz 4 genannten Fällen.	
4. Anstatt die personenbezogenen Daten zu löschen, kann der für die Verarbeitung Verantwortliche <u>diese Daten sperren</u> deren Verarbeitung beschränken , wenn	Statt der Formulierung „beschränken“ sollte 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 Beweis Zwecke oder <u>zur Erfüllung gesetzlicher Aufbewahrungsvorschriften</u> 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) <u>eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.</u>	Übernahme des Sperrgrundes in § 35 Absatz 3 Nr. 3 BDSG, um in der Praxis auch Sachverhalte berücksichtigen zu können, in denen eine Löschung aus technischen Gründen (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 Beweis Zwecke <u>und zur Erfüllung gesetzlicher Aufbewahrungspflichten</u> erforderlich sind, wenn die betroffene Person ihre Einwilligung gegeben	Klarstellung, dass auch die Erfüllung von gesetzliche Aufbewahrungspflichten bei der Sperre zu berücksichtigen ist.

hat oder die Rechte einer anderen natürlichen oder juristischen Person geschützt werden müssen oder wenn dies im öffentlichen Interesse liegt.	
6. Unterliegt die Verarbeitung 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 <u>Sperrung</u> Beschränkung aufgehoben werden soll.	Unklar ist, in welchen Fällen eine Sperrung 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 <u>vorher</u> nicht auf sonstige Weise verarbeiten, <u>außer sie sind anonymisiert</u> .	Eine Weiternutzung von anonymen Daten sollte statthaft sein.
9. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten festzulegen in Bezug auf	Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch erfassen.
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.	

<p style="text-align: center;"><i>Artikel 18</i> Recht auf Datenübertragbarkeit</p>	
<p>1. <u>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 weiterverwendbaren strukturierten gängigen elektronischen Format oder deren Überführung in ein anderes System zu verlangen.</u></p>	<p>Ein Recht auf Datenportabilität 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.</p> <p>Für „konventionelle Datenverarbeitungen“ in unternehmensinternen Datenbanken ist der Anspruch auf Datenportabilität nicht sachgerecht und würde unverhältnismäßig in die Grundrechtsposition von Unternehmen eingreifen:</p> <p>Zum einen ist es nicht der Betroffene, der in unternehmensinterne Datenbanken „seine“ Daten einstellt, sondern die Datenverarbeitung wird verfahrenstechnisch alleine von dem Unternehmen gesteuert.</p> <p>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.</p> <p>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</p>

	<p>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.</p> <p>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.</p>
<p>2. Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und basiert die Verarbeitung auf einer Einwilligung oder einem Vertrag, hat die betroffene Person das Recht, diese personenbezogenen Daten sowie etwaige sonstige von ihr zur Verfügung gestellte Informationen, die in einem automatisierten Verarbeitungssystem gespeichert sind, in einem gängigen elektronischen Format in ein anderes System zu überführen, ohne dabei von dem für die Verarbeitung Verantwortlichen, dem die personenbezogenen Daten entzogen werden, behindert zu werden.</p>	<p>Siehe Kommentierung zu Art. 18 Abs. 1.</p>
<p>3. Die Kommission kann das</p>	<p>Insbesondere stellt die Möglichkeit der</p>

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.	Festlegung des elektronischen Formats nach Absatz 1 durch die Kommission einen erheblicher Eingriff in die verfassungsrechtlich geschützte Betriebsorganisationsfreiheit.
---	---

ABSCHNITT 4

WIDERSPRUCHSRECHT UND PROFILING

Regelung ggf. mit Änderungsvorschlag	Anmerkungen
<i>Artikel 19</i> 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 nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.	
2. Werden personenbezogene Daten verarbeitet, um Direktwerbung für nicht kommerzielle Zwecke zu betreiben, hat die betroffene Person das Recht, dagegen unentgeltlich Widerspruch einzulegen. Die betroffene Person muss ausdrücklich in einer verständlichen und von anderen Informationen klar abgegrenzten Form auf dieses Recht hingewiesen werden.	Vgl. Erwägungsgrund 57 der deutschen Fassung.
3. Im Falle eines Widerspruchs gemäß <u>Absatz 1</u> und 2 darf der für die Verarbeitung Verantwortliche die betreffenden personenbezogenen Daten nicht weiter nutzen oder anderweitig verarbeiten. <u>Im Falle eines Widerspruchs gemäß Absatz 2 darf der für die Verarbeitung Verantwortliche die betreffenden personenbezogenen Daten nicht</u>	Mit einem neuen zweiten Satz wird klargestellt, dass bei einem Widerspruch gegen Verarbeitungen zu Werbezwecken die Verarbeitung zur Erfüllung eines Vertrages unberührt bleibt.

für Zwecke der Direktwerbung weiter nutzen.	
<i>Artikel 20</i> 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.	Erfasst sind wohl insbesondere auch Scoring-Verfahren (Antragsscoring sowie Verhaltensscoring), die für Entscheidungen im Kundenverhältnis relevant sind. Nicht vom Anwendungsbereich erfasst sind wohl Ratingverfahren, die lediglich bankinternen Zwecken wie z.B. der Risikosteuerung dienen.
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	z. B. § 10 Abs. 1 Sätze 3 ff. KWG. Es kann nicht Aufgabe von Unternehmen sein, zu prüfen, ob die gesetzliche Bestimmung, die die Maßnahme erlaubt oder fordert, dem Datenschutz angemessen Rechnung trägt. Vielmehr muss sich das Unternehmen auf dies gesetzliche Vorschrift verlassen können.
c) mit Einwilligung der betroffenen Person nach Maßgabe von Artikel 7 und vorbehaltlich entsprechender Garantien erfolgt.	Einwilligung muss als Legitimation der Datenverarbeitung ausreichen. Zudem: Abgrenzungs- oder Beweisschwierigkeiten in der Praxis.

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.	Streichen: Die Kodifizierung von Zulässigkeitstatbeständen sollte Rat und Parlament vorbehalten sein und nicht auf Kommission übertragen werden. Die Bewertung sollte dem Einzelfall überlassen bleiben. Die vielfältigen Lebenssachverhalte lassen sich regelmäßig nicht regulatorisch erfassen.

ABSCHNITT 5 BESCHRÄNKUNGEN

Regelung ggf. mit Änderungsvorschlag	Anmerkungen
<i>Artikel 21 Beschränkungen</i>	
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	<p>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).</p> <p>Solche Beschränkungen sollten insbesondere Geschäftsgeheimnisse und Eigentumsrechte der Verantwortlichen schützen, vgl. z.B. Erwägungsgrund 51 der VO in Bezug auf die dort bereits angedachte Beschränkung von</p>

	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.	