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

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.