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

mit grundsätzlichen Anmerkungen 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:
Christian Koch
Telefon: +49 30 2021- 2321
E-Mail: c.koch@bvr.de

Berlin, 22. März 2012

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-VO

Die Europäische Kommission hat am 25. Januar 2012 ihren Vorschlag für eine europäische Datenschutzverordnung vorgelegt. Die Deutsche Kreditwirtschaft unterstützt die damit verbundene Zielsetzung, das Datenschutzrecht weiter zu vereinheitlichen, um im Europäischen Binnenmarkt ein „einheitliches Spielfeld" für alle Wirtschaftsunternehmen zu schaffen, Hindernisse im EU-Binnenmarkt zu beseitigen und Wettbewerbsverzerrungen zu vermeiden. Das Bestreben der Europäischen Kommission, bürokratische Regelungen abzubauen und das Datenschutzrecht zu vereinfachen, wird begrüßt. Allerdings besteht bei etlichen Regelungen noch Klarstellungs- und Verbesserungsbedarf, damit diese in der Praxis mit verhältnismäßigem Aufwand umsetzbar sind und ein ausgewogener Interessenausgleich zwischen Betroffenen und den Verantwortlichen der Verarbeitung erreicht wird. Zudem sollte nicht jede durch die Herausforderungen des Internets motivierte Verschärfung des Datenschutzrechts zu pari für „konventionelle" Datenverarbeitungen übernommen werden, für die das bislang geltende Datenschutzrecht einen ausreichenden Schutz der Interessen der Betroffenen gewährleistet.

Im Vorgriff auf eine derzeit in der Deutschen Kreditwirtschaft in Vorbereitung befindliche detaillierte Stellungnahme zu den einzelnen Regelungen im Verordnungsvorschlag bestehen bislang folgende grundsätzliche Anmerkungen zu dem Gesetzesvorhaben:

1. Vor- und Nachteile der Verordnung als Rechtsinstrument

Eine Harmonisierung des EU-Datenschutzrechts und die Beseitigung von EU-Binnenmarkthindernissen werden grundsätzlich unterstützt (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 der Verordnungslösung müssen daher 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 Staaten geltenden gesetzlichen Regelungen zum Bankgeheimnis.

2. 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. Der Kommissionsvorschlag geht dabei über die in Artikel 290 des „Vertrages über die Arbeitsweise der Europäischen Union" (AEUV) gesetzten Grenzen für „delegierte Rechtsakte" weit hinaus, weil sich die Rechtsetzungsermächtigung vielfach nicht auf eine Konkretisierung der Vorschriften der Verordnung beschränkt, sondern eine eigenständige Normsetzung erlaubt. Auch ist diese Übertragung der Rechtsetzungskompetenz auf die Exekutive

wegen der Durchbrechung des Gewaltenteilungsprinzips und rechtsstaatlicher Bedenken abzulehnen. Insbesondere darf die Kommission nicht strafbewährte Vorschriften konkretisieren (z. B. die Zulässigkeitsregel in Artikel 6 Absatz 1f durch Artikel 6 Absatz 5) und damit erst den Bestimmtheitsgrundsatz strafrechtlicher Normen erfüllen. Die Rechtsetzungsbefugnis sollte weiter alleine bei Rat und Europäischem Parlament bleiben. Soweit Konkretisierungsbedarf bei einzelnen Regelungen der Verordnung besteht, sollte dies sogleich durch Präzisierung der Normen in der Verordnung oder durch zusätzlich von Rat und Parlament erlassene Rechtsakte erfolgen.

Aus gleichen Gründen ist auch die in der Verordnung vorgesehene Delegierung auf die Europäische Kommission abzulehnen, Vorgaben für Datenformate (z. B. Artikel 18 Absatz 3) und Muster für die Erfüllung von Transparenzpflichten (z. B. Artikel 14 Absatz 8) vorzuschreiben. Die konkrete Umsetzung und Ausgestaltung bestimmter datenschutzrechtlicher Pflichten sollte weiter in der Selbstverantwortung der Unternehmen liegen.

3. Vorschriften auf Regelungsziele beschränken

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" nicht immer sachgerecht sind. „Konventionelle Datenverarbeitungen" in Unternehmen würden damit unnötig bürokratisiert, eingeschränkt und/oder beeinträchtigt. Diese Probleme treten bei den – in der „virtuellen Welt" des Internet durchaus nachvollziehbaren und ausweislich der Erwägungsgründe 52, 54 sowie 55 und deswegen 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) auf.

4. Rechte datenverarbeitender Unternehmen angemessen berücksichtigen

Der Verordnungsvorschlag berücksichtigt in einigen Regelungen nicht die verfassungsmäßig geschützten Rechte von datenverarbeitenden Unternehmen. 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 Artikel 2, 12 und 14 des Grundgesetzes garantierte Recht am eingerichteten und ausgeübten Gewerbebetrieb oder Grundrechte im Verwaltungs- und Gerichtsverfahren. Insgesamt gilt es, einen angemessenen Ausgleich zwischen den verfassungsrechtlich geschützten Rechtspositionen 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.

5. Doppelregulierung bzw. widersprüchliche Regulierung für Kreditwirtschaft 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 Pflichten überlappen und unnötigen Bürokratieaufwand 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 Verordnung Doppelregulierungen und Widersprüche zum Bankaufsichtsrecht zu vermeiden. Erfüllt eine Bank bereits ihre bankaufsichtsrechtlichen Pflichten zur Unternehmensführung, dann müssen damit auch vergleichbare datenschutzrechtliche Vorgaben als erfüllt anerkannt werden. Ordnen bankaufsichtsrechtliche Normen die Verarbeitung personenbezogener Daten an oder erlauben sie diese, muss die Verordnung das Bankaufsichtsrecht akzeptieren.

Überdies kollidieren einige Vorgaben der Verordnung mit zivilrechtlichen Regelungen 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.

6. Keine Reduzierung der Zulässigkeitstatbestände

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 faktisch 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.

7. Übermäßige Formalisierung und Bürokratisierung vermeiden

Zwar verfolgt die Kommission das Ziel der Entlastung von Unternehmen von überflüssigen Formalien. Gleichzeitig werden den Unternehmen bei der Organisation der Datenverarbeitung und bei der Information der Betroffenen erheblich erweiterte Pflichten auferlegt (vgl. Artikel 11 bis 14), die im Ergebnis zu einer Ausweitung von Formalien und Bürokratie führt. Auch führt die Erweiterung der Informationspflichten schnell zu einer für den Betroffenen nicht verständlichen Informationsflut. Folglich sollte eine übermäßige Formalisierung und Bürokratisierung vermieden werden.

8. Informationspflichten bedarfsgerecht ausgestalten

Transparenz für den von der Datenverarbeitung Betroffenen ist sicherlich eine Grundvoraussetzung dafür, dass der Betroffene seine Rechte wahrnehmen kann. Doch schon im Verbraucherschutzrecht ist die Tendenz zu verzeichnen, dass durch gesetzliche Vorgaben die Menge der dem Bankkunden zu erteilenden Informationen ein Ausmaß erreicht hat, bei dem man sich fragt, ob der Bankkunde dies möchte und verstehen kann. Insofern ist der mit Artikel 14 verfolgte Ansatz einer „umfassenden" Informationspflicht fragwürdig, wenn er letztlich in einer für den Kunden nicht mehr verarbeitbaren „Informationsflut" mündet. Zielführender ist ein zweistufiger Ansatz: Auf der ersten Stufe muss es ausreichen, dem Kunden allgemeine Informationen erteilen zu können. Erst bei dessen konkreter Nachfrage 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 weitere Informationen dem Kunden geben).

9. Unbeabsichtigte Effekte vermeiden

Einige Regelungen werden eher zu einer Minderung als zur Stärkung des Datenschutzes beitragen. Beispiele:

- Eine Auskunftspflicht dem Unternehmen auf elektronischem Wege aufzuerlegen (Artikel 15 Absatz 2), gefährdet den Datenschutz, wenn eine Auskunftserteilung nicht von einer sicheren Authentifizierung des Auskunftsersuchenden und einem sicheren elektronischen Transportweg abhängig gemacht werden kann (vgl. auch Erwägungsgrund 52).
- Das Recht auf Datenportabilität (Artikel 18) fördert nur scheinbar die Rechte der Betroffenen, denn der Betroffene wird in vielen Fällen von Dritten zur Geltendmachung dieses Rechts instrumentalisiert werden, mit der Folge, dass der Zugriff auf personenbezogene Daten bei Unternehmen erleichtert und einmal erhaltene Dateikopien unbegrenzt zum Handelsgut werden.

10. Datenschutzrecht darf nicht zweckentfremdet werden können

Das Datenschutzrecht sollte nicht zweckentfremdet werden können, sondern sich auf den Schutz des informationellen Selbstbestimmungsrechts beschränken. Hierzu zwei Beispiele:

- Das Recht auf Datenportabilität (Artikel 18) ist 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.
- Die Auskunftspflichten eines Unternehmens (Artikel 15) sollten 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 müssen unberührt bleiben.

11. Arbeitsteilige Strukturen in der Wirtschaft berücksichtigen

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