

# Stellungnahme

zu den Änderungsvorschlägen von Europäischem  
Parlament und Rat zum Vorschlag der  
EU-Kommission für eine  
Datenschutz-Grundverordnung

Kontakt:

Daniel Selig

Telefon: +49 30 20225- 5356

Telefax: +49 30 20225-5345

E-Mail: [daniel.selig@dsgv.de](mailto:daniel.selig@dsgv.de)

Berlin, 03. September 2015

Federführer:

Deutscher Sparkassen- und Giroverband e. V.

Charlottenstraße 47 | 10117 Berlin

Telefon: +49 30 20225-0

Telefax: +49 30 20225-250

[www.die-deutsche-kreditwirtschaft.de](http://www.die-deutsche-kreditwirtschaft.de)

**1. EG 134 (Rat) - Gewährleistung von Rechtssicherheit und Bestandschutz für Datenverarbeitungsvorgänge vor Inkrafttreten der Verordnung**

Die Geschäftsbeziehung zwischen Bank und Kunde ist durch langjährige Dauerschuldverhältnisse geprägt. Banken sind daher insbesondere darauf angewiesen, dass für vor dem Inkrafttreten begonnene Datenverarbeitungen (z.B. zur Erfüllung eines Immobilienkredits) Rechtssicherheit und in gewissem Maße Bestandschutz gilt. Diesem Bedürfnis trägt der vom Rat vorgeschlagene Erwägungsgrund 134 mit Übergangsbestimmungen Rechnung. Da es sich um eine dem materiellen Recht zuzuordnende Übergangsbestimmung handelt, sollte diese unmittelbar in den Schlussvorschriften der Verordnung (z.B. in Artikel 91) Eingang finden.

**2. Artikel 4 Absatz 7a (EP) - Datenaustausch zwischen Auftraggeber und Auftragsdatenverarbeiter ist keine gesondert erlaubnispflichtige Datenübermittlung**

Banken nutzen in erheblichem Umfang Auftragsdatenverarbeiter. Nach geltendem Recht ist der Datenaustausch mit dem Auftragnehmer keine gesondert erlaubnispflichtige Datenübermittlung, da die Bank nach außen verantwortliche Stelle bleibt. Um dies klarzustellen, sollte die vom EP mit Artikel 4 Absatz 7a vorgeschlagene Definition des „Dritten“ übernommen werden. Im Zusammenhang mit Artikel 26 wird damit deutlich, dass ein Auftragsdatenverarbeiter zwar ein „Empfänger“ von Daten, aber kein „Dritter“ ist. Die Weitergabe von Daten an den Auftragsdatenverarbeiter ist damit keine gesondert nach Artikel 6 erlaubnispflichtige Datenübermittlung.

**3. Artikel 4 Absatz 16 (Rat) und Artikel 22 Absatz 3a (EP) - Datenverarbeitung in der Unternehmensgruppe berücksichtigen**

Gerade im Finanzdienstleistungsbereich arbeiten Unternehmen in Konzern- oder Verbundstrukturen zusammen, um ihren Kunden ein breites Spektrum an Dienstleistungen „aus einer Hand“ anbieten zu können. Deshalb ist die vom EP mit Artikel 22 Absatz 3a vorgeschlagene Erleichterung der Verarbeitung von Daten innerhalb einer Unternehmensgruppe sehr zu begrüßen.

In Anknüpfung an den Ratsvorschlag zu Artikel 4 Absatz 17 sollte die Definition der Unternehmensgruppe in Artikel 4 Absatz 16 erweitert werden. Zumindest sollte diese Regelung auch für gleichgeordnete Unternehmen in einem Konzern gelten (vgl. § 18 Absatz 2 AktG). Zudem sollte eine Gruppe von Unternehmen auch dann vorliegen, wenn diese im Sinne des anwendbaren nationalen Rechts wegen der Ausübung einer gemeinsamen Wirtschaftstätigkeit als solche anerkannt wird.

**4. Artikel 6 Absatz 1c - Zulässigkeitstatbestand der Datenverarbeitung zur Erfüllung von rechtlichen Pflichten muss auch bankaufsichtsrechtliche Vorgaben umfassen**

Banken müssen vielfach personenbezogene Daten aufgrund von rechtlichen Vorgaben des jeweiligen EU-Mitgliedstaats verarbeiten (z. B. zur Geldwäsche- und Betrugsbekämpfung). Rechtsgrundlage sind dabei sowohl Gesetze als auch „untergesetzliche Instrumente“ wie Rechtsverordnungen, Verwaltungsakte oder bankaufsichtsrechtliche Vorgaben. Die Formulierung „rechtliche Verpflichtung“ im Ratstext zu Artikel 6 Absatz 1c ist deshalb vorzugswürdig gegenüber der EP-Fassung „gesetzliche Verpflichtung“, da damit alle für Banken relevanten hoheitlichen Rechtsakte erfasst werden. Dies steht auch im Einklang mit den Ausführungen im Erwägungsgrund 31a des Ratsvorschlags, wonach auch untergesetzliche Rechtsakte erfasst sein sollen.

Des Weiteren ist in diesem Zusammenhang der Ratsvorschlag zu Artikel 1 Absatz 2a und Artikel 6 Absatz 3 zu unterstützen. Denn dieser gewährleistet für die Kreditinstitute einen zwingend erforderlichen Gleichlauf zwischen Bankaufsichtsrecht und Datenschutzrecht. Bereichsspezifische Normen im Bankaufsichtsrecht beispielsweise zur Identifikation von Bankkunden, zum Scoring/Rating sowie zur Geldwäsche- und

Betrugsbekämpfung können weiter unter Beachtung von Artikel 6 Absatz 3 durch den jeweiligen EU-Mitgliedstaat getroffen werden.

Im Vergleich zur bisherigen Rechtslage in Deutschland fehlt es allerdings noch an einer Regelung, wonach auch Tarifverträge und Betriebsvereinbarungen als „sonstige“ Rechtsvorschriften eine Datenverarbeitung legitimieren können. Dem nationalen Gesetzgeber sollte diese Anerkennung von Tarifverträgen und Betriebsvereinbarungen als Legitimation der Datenverarbeitung weiterhin offen stehen. Dies sollte zumindest in Artikel 82 noch zum Ausdruck gebracht werden.

#### **5. Artikel 6 Absatz 1f - Datenverarbeitung im Drittinteresse erlauben**

Rat und Parlament haben in Artikel 6 Absatz 1f die Ergänzung des Drittinteresses vorgeschlagen. Diese Ergänzung ist notwendig, um beispielsweise die Arbeit von Kreditauskunfteien weiter zu legitimieren. Der Ratsvorschlag ist gegenüber der EP-Fassung vorzugswürdig, da er klarer formuliert ist.

#### **6. Artikel 6 Absatz 4 - Flexibilität bei Zweckbindung erhalten**

Der Vorschlag des Rats in Artikel 6 Absatz 4 Satz 2 lässt unter bestimmten Voraussetzungen eine Zweckänderung zu und ist daher zu unterstützen. Denn die technischen Möglichkeiten der Datenverarbeitung und die Kundenbedürfnisse haben sich im Vergleich zur EU-Datenschutzrichtlinie erheblich weiter entwickelt. Der Vorschlag des Rates erlaubt mehr Flexibilität und ist für die Erhaltung der Wettbewerbsfähigkeit der europäischen Wirtschaft gegenüber Wettbewerbern aus Drittstaaten erforderlich.

#### **7. Artikel 9 - Verarbeitung sensibler Daten im Zahlungsverkehr vereinfachen**

Damit weiterhin vom Betroffenen in Zahlungsaufträgen angegebene sensible Daten (z. B. Spende an Partei A oder Mitgliedsbeitrag an Gewerkschaft B) ohne eine zusätzliche Einwilligung des Kunden verarbeitet werden können, sollte der EP-Vorschlag für Artikel 9 Absatz 2 aa) übernommen werden, wonach sensible Daten auch im Rahmen der Erfüllung eines Vertrages verarbeitet werden dürfen.

#### **8. Artikel 13a (EP) - Aussagekraft von Informationspiktogrammen prüfen**

Einfache und leicht wahrnehmbare Informationen sind sinnvoll. Doch sind die vom Parlament mit Artikel 13a vorgeschlagenen Informationspiktogramme zu sehr als „Warnschilder“ ausgestaltet und bergen die Gefahr von Missverständnissen beim Bürger. So sollte z. B. das Warnzeichen zur Verschlüsselung sich nicht auf diesen Aspekt fokussieren, sondern positiv auf die Gesamtheit der Datensicherungsmaßnahmen des Unternehmens abstellen (Datensicherheitspiktogramm). Zudem sollten die vom EP vorgeschlagenen Piktogramme noch hinsichtlich Aussagekraft und Eindeutigkeit verbessert werden.

#### **9. Artikel 14 - Informationsumfang abstufen und Wiederholungen vermeiden**

Bankkunden erhalten aufgrund verschiedener gesetzlicher Vorgaben umfangreiche Informationspakete. Im Datenschutzrecht hier noch weiter drauf zu satteln ist der falsche Weg, weil dies nur zu einer teuren und ineffektiven Informationsflut führt. Der Ratsvorschlag zu Artikel 14 Absatz 1 und Absatz 1a ist daher vorzugswürdig, da er den Informationsumfang nach Erforderlichkeit abstuft, um eine Informationsüberflutung des Betroffenen zu vermeiden. Auf der ersten Stufe reicht es, die verantwortliche Stelle und die Datenverarbeitungszwecke zu benennen. Nur wenn es zum Zweck der Transparenz und der Risikolage erforderlich ist, müssen weitere Informationen erteilt werden.

Stellungnahme zu den Änderungsvorschlägen von Europäischem Parlament und Rat zum Vorschlag der EU-Kommission für eine Datenschutz-Grundverordnung vom 03. September 2015

Zudem ist der Ratsvorschlag zu Artikel 14 Absatz 5 sachgerecht, um redundante Informationen zu vermeiden. Gerade bei Verarbeitungen zur Erfüllung eines Vertrages erfährt der Betroffene die wesentlichen Informationen aus den Vertragsunterlagen (z.B. aus dem Kreditvertrag). Diese müssen nicht wiederholt werden.

#### **10. Artikel 15 - Anspruch auf Kopie der Datenverarbeitung ist nicht sachgerecht**

Die aus der Diskussion um die Datenportabilität (Artikel 18) resultierende Erweiterung des Auskunftsrechts des Betroffenen von einem Informationsrecht in einen Anspruch auf Herausgabe der Kopie der Daten (vgl. Artikel 15 Absatz 1) ist abzulehnen. Für die Gewährleistung der Datenschutzrechte des Betroffenen reicht der bisherige Auskunftsanspruch völlig aus. Wie schon bei der Datenportabilität kritisiert, birgt ein Kopieherausgabeanspruch gegenüber konventionellen Unternehmen auch ein hohes Potential der Zweckentfremdung durch Dritte, die den Betroffenen instrumentalisieren, um damit Ziele außerhalb des Datenschutzes zu verfolgen (z. B. Vermieter verlangt vom Mieter Unterlagen aus der Geschäftsverbindung mit seiner Bank, Umgehung von Zivilprozessregeln zur Beweiserhebung). Sollte an dem Kopieherausgabeanspruch festgehalten werden, müsste zur Vermeidung einer Zweckentfremdung geregelt werden, dass diese Kopien nicht von Dritten genutzt werden dürfen. Zudem: Um in jedem Fall Geschäftsgeheimnisse der Unternehmen, Datenschutzrechte Dritter und das geistige Eigentum von Unternehmen zu wahren, muss der Kopie-Herausgabeanspruch entsprechend eingeschränkt werden, wie der Rat mit Artikel 15 Absatz 2a vorschlägt.

#### **11. Artikel 18 - Anspruch auf Datenportabilität auf soziale Netzwerke und Internetplattformen begrenzen**

Der Anspruch auf Datenportabilität passt nur für soziale Netzwerke und sonstige Internetplattformen und nicht für konventionelle Unternehmen, wie Banken. Außerhalb des Internetbereichs ist von einer hohen Zweckentfremdungsgefahr (s. o.) und enormen Implementierungsaufwänden und -kosten auszugehen. Basierend auf den vom Rat zu Artikel 18 Absatz 2 vorgeschlagenen Einschränkungen, sollte der Anspruch auf „Dienste der Informationsgesellschaft“ (vgl. Definition in Artikel 4 Absatz 20 des Ratsvorschlags) beschränkt werden. Ansonsten müssten konventionelle Unternehmen beispielsweise alle Schreiben des Kunden an das Unternehmen jederzeit (in Kopie) herausgeben.

Formulierungsvorschlag:

*„Die betroffene Person hat gegenüber einem Dienst der Informationsgesellschaft das Recht, die sie betreffenden personenbezogenen Daten, (...)“*

#### **12. Artikel 20 - Profilbildungsvorschrift auf automatisierte Einzelentscheidungen beschränken**

Die Regelungen zur Profilbildung sollten sich gemäß dem Ratsvorschlag zu Artikel 20 auf die automatisierte Einzelentscheidung beschränken, womit der Ansatz der EU-Datenschutzrichtlinie fortgeführt würde. Um den Gleichlauf zwischen Bankaufsichtsrecht und Datenschutzrecht zu gewährleisten, ist der Ratsvorschlag zu Artikel 20 Absatz 1a lit. b) zu unterstützen.

#### **13. Artikel 31 – Erheblichkeitsschwelle bei Datenschutzpannenmeldepflicht**

Der Ratstext zu Artikel 31 ist vorzugswürdig, da damit eine Erheblichkeitsschwelle eingeführt wird und Meldungen von Bagatellen vermieden werden.

#### **14. Artikel 33 – Datenschutzfolgenabschätzung nur fakultativ regeln**

In der Kreditwirtschaft bestehen bereits Erfahrungen mit dem Instrument der Datenschutzfolgeabschätzung bei Einsatz der NFC-Technik auf Zahlungskarten. Dieses Verfahren ist – wenn man es ernst nimmt – aufwändig, teuer und langwierig. Die von EP und Rat in Artikel 33 Absatz 1 beschriebene Schwelle der Erforderlichkeit einer Datenschutzfolgenabschätzung läuft Gefahr, dass dieses verfahrenstechnisch recht aufwändige Instrument übermäßig zum Einsatz kommen müsste und gerade kleinere und mittlere Unternehmen völlig überfordert. Denn beispielsweise die Risikoindikatoren „Identitätsdiebstahl“ oder „finanzielle Verluste“ könnten beispielweise bei jedem im E-Commerce tätigen Anbieter erfüllt sein. Die Datenschutzfolgenabschätzung wird damit faktisch zu einer Markteintrittsschranke für Unternehmen. Das Instrument sollte deshalb weiter freiwillig bleiben.

Zumindest sollte der Ratsvorschlag weiter verfolgt werden, dass die Aufsichtsbehörde ermächtigt wird, die Pflicht einzugrenzen (vgl. Artikel 33 Absatz 2a bis 2b). Zudem sollte die Pflicht eines Unternehmens zur Datenschutzfolgenabschätzung nicht bestehen, wenn es aufgrund einer rechtlichen Pflicht gemäß Artikel 6 Absatz 1c handelt. Denn dann hat das Unternehmen selber keinen Gestaltungsspielraum und eine Folgenabschätzung macht keinen Sinn.

Faktisch unmöglich ist die Konsultationspflicht der Marktgegenseite nach Artikel 33 Absatz 4, da beispielsweise Verbraucherschutzverbände gar nicht die Ressourcen haben, sich mit der zu erwartenden hohen Zahl von Gutachten inhaltlich zu befassen. Die Konsultationspflicht sollte daher gestrichen werden.

#### **15. Artikel 79 – Angemessenheit der Sanktionen**

Der Ratsvorschlag zur Streichung von Artikel 78 und zur Änderung von Artikel 79 ist vorzugswürdig, da damit eine mit dem Verfassungsrecht unvereinbare Doppelbestrafung ausgeschlossen wird und der Sanktionsrahmen eingeschränkt wird. Jedoch bleibt der Strafrahmen noch unangemessen hoch und muss auf ein verhältnismäßiges Maß reduziert werden.