Z E N T R A L E R K R E D I T A U S S C H U S S

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)239

Deutscher Bundestag
Innenausschuss
Platz der Republik 1
11011 Berlin

10178 Berlin, den 15. April 2011
Burgstraße 28
AZ ZKA: BDSG
AZ BdB: RE.30 - Ht/Bl

Stellungnahme des Zentralen Kreditausschusses zu dem Gesetzentwurf der Bundesregierung für ein „Gesetz zur Regelung des Beschäftigtendatenschutzes“ (BT-Drs. 17/4230 vom 15. Dezember 2010)

Sehr geehrte Damen und Herren,

in seiner Sitzung am 13. April 2011 (Top 2) hat der Innenausschuss des Deutschen Bundestages die Beratungen zu dem von der Bundesregierung vorgelegten Entwurf eines „Gesetzes zur Regelung des Beschäftigtendatenschutzes“ (BT-Drs. 17/4230) aufgenommen. Zugleich sind die Gesetzentwürfe der Fraktion der SPD (BT-Drs. 17/69) und der Fraktion BÜNDNIS90/DIE GRÜNEN (BT-Drs. 17/4853) zum Beschäftigtendatenschutz beraten worden.

Anbei leiten wir Ihnen unsere Stellungnahme zum Regierungsentwurf zu, mit der wir uns vor allem dafür aussprechen, das geplante Beschäftigtendatenschutzrecht in Einklang mit bankaufsichtsrechtlichen Vorgaben zur Betrugs-, Geldwäsche- und Korruptionsbekämpfung und zu Compliance-Maßnahmen zu bringen. Auch der Bundesrat hält es für erforderlich, die beabsichtigten datenschutzrechtlichen Regelungen im weiteren Gesetzgebungsverfahren mit den bankenaufsichtlichen Vorschriften in Einklang zu bringen (vgl. BT-Drs. 17/4230, S. 26 f., Anlage 3 Nr. 1 f.).

. . .

Für die Beachtung unserer Stellungnahme bei den weiteren Beratungen wären wir Ihnen sehr verbunden.

Mit freundlichen Grüßen
Für den Zentralen Kreditausschuss
Bundesverband deutscher Banken

Thorsten Höche Wulf Hartmann

Anlage

Z E N T R A L E R K R E D I T A U S S C H U S S

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN • BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN • DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

Stellungnahme des Zentralen Kreditausschusses zu dem Gesetzentwurf der Bundesregierung für ein „Gesetz zur Regelung des Beschäftigtendatenschutzes“ (BT-Drs. 17/4230 vom 15. Dezember 2010)

15. April 2011

Gliederung:

A. Vorbemerkung

Die im Zentralen Kreditausschuss zusammenwirkenden Spitzenverbände des deutschen Kreditgewerbes möchten im Folgenden die Gelegenheit wahrnehmen, zu dem Gesetzesentwurf der Bundesregierung zur Regelung des Beschäftigtendatenschutzes Stellung zu nehmen. Dabei konzentrieren wir uns auf diejenigen Datenschutzvorschriften, die für Kreditinstitute eine besondere Bedeutung haben, insbesondere weil sie in einem Spannungsverhältnis zum Bankaufsichtsrecht stehen oder gerade bei Kreditinstituten zu Anwendungsproblemen führen würden. Die allgemeinen, für alle Unternehmensarten gleichermaßen geltenden Anmerkungen zum Gesetzesvorhaben werden Gegenstand der Stellungnahmen der Arbeitgeberverbände sein.

B. Beschäftigtendatenschutz in Einklang mit bankaufsichtsrechtlichen Vorgaben zur Betrugs-, Geldwäsche- und Korruptionsbekämpfung und zu Compliance-Maßnahmen bringen

1. Verbesserungsbedarf, auch aus Sicht des Bundesrates

Wir begrüßen grundsätzlich den mit den neuen Regelungen, insbesondere in § 32d Abs. 3 BDSG-E, verfolgten Ansatz, einen datenschutzrechtlichen Rahmen für die Betrugs-, Geldwäsche- und Korruptionsbekämpfung sowie für Compliance-Maßnahmen in Unternehmen zu schaffen, um mehr Rechtsklarheit und Rechtssicherheit zu schaffen. Jedoch sehen wir die Gefahr, dass die vorgeschlagenen Vorschriften nicht im vollen Umfang den Besonderheiten in der Kreditwirtschaft Rechnung tragen und bankaufsichtsrechtlich gebotene Maßnahmen zur Bekämpfung von Straftaten und zur Compliance in Frage stellen. Die bankaufsichtsrechtlichen Vorgaben sollen die Integrität von Kreditinstituten gewährleisten und sind damit für die Reputation des Finanzplatzes Deutschland von erheblicher Bedeutung. Ein neues Beschäftigtendatenschutzrecht muss dieser Besonderheit Rechnung tragen.

Auch der Bundesrat hält es für erforderlich, die beabsichtigten datenschutzrechtlichen Regelungen im weiteren Gesetzgebungsverfahren mit den bankenaufsichtlichen Vorschriften in Einklang zu bringen (Stellungnahme vom 5. November 2011, BR-Drs. 535/10, Nr. 1 f.; BT-Drs. 17/4230, S. 26 f., Anlage 3 Nr. 1 f.). Die Bundesregierung hat in ihrer Gegenäußerung (BT-Drs. 17/4230, S. 38, Anlage 4 zu Nr. 1 f.) ausgeführt, die Anregungen des Bundesrates zum Anlass zu nehmen, die weitere Ergänzung finanzmarktaufsichtsrechtlicher Regelungen im Hinblick auf § 32 ff. im Rahmen des Gesetzgebungsverfahrens zu prüfen.

2. Konkrete Probleme

a. Bisher über Spezialnormen oder § 28 Absatz 1 Nr. 2 BDSG zulässige Datenverarbeitungen werden in Frage gestellt

Korruptions-, Betrugs- und Geldwäschebekämpfung sowie Compliance spielen in der Kreditwirtschaft eine besonders wichtige Rolle. Diese Maßnahmen unterliegen einer umfassenden gesetzlichen Regulierung unter anderem im Kreditwesengesetz, im Geldwäschegesetz und im Wertpapierhandelsgesetz. An die Kreditwirtschaft werden dabei hohe Anforderungen an die Überwachung von Transaktionen und Geschäftsbeziehungen sowie an die Aufdeckung von Interessenkonflikten und Insidergeschäften sowie von Fehlverhalten der eigenen Mitarbeiter gestellt. In diesem aufsichtsrechtlichen Rahmen dürfen und müssen personenbezogene Daten von Beschäftigten erhoben, verarbeitet und genutzt werden und zwar auch verdachts- und anlassunabhängig. Diese Vorgänge sind bislang datenschutzrechtlich entweder aufgrund einer Spezialnorm (z.B. § 25c Abs. 2 Satz 3 KWG) oder nach § 28 Abs. 1 Nr. 2 BDSG zulässig.

Der Gesetzentwurf der Bundesregierung stellt diese Rechtslage in Frage, weil bislang übersehen wird, dass die bankaufsichtsrechtlichen Vorgaben zu bankinternen Sicherungsmaßnahmen nicht erst bei Bestehen eines konkreten Anlasses, wie in § 32d Abs. 3 und § 32e BDSG-E als Voraussetzung formuliert, greifen, sondern grundsätzlich anlassfrei und flächendeckend bestehen. Mit anderen Worten: Unabhängig von dem Vorliegen oder dem Verdacht auf eine konkrete Straftat durch einen Mitarbeiter im Unternehmen, muss die Bank aufgrund bankaufsichtsrechtlicher Vorgaben routinemäßig Prüfungen und Kontrollen vornehmen, die auch einzelpersonenbezogene Beschäftigtendaten erfassen können und sich nicht mit anonymisierten Daten durchführen lassen. Um nicht die aufsichtsrechtlichen Vorgaben zu konterkarieren, ist es daher von besonderer Bedeutung, dass diese Kontroll- und Schutzmaßnahmen auch nach Inkrafttreten der neuen Beschäftigtendatenschutzvorschriften nach Maßgabe des Bankaufsichtsrechts weiter zulässig bleiben und effektiv ausgeführt werden können.

b. § 32d Abs. 3 BDSG-E greift im Vergleich mit § 25c Abs. 2 S. 1 KWG viel zu kurz und stellt damit bankinterne Sicherungsmaßnahmen in Frage

Laut der Gesetzesbegründung soll § 32d Abs. 3 BDSG-E auch für die Kreditwirtschaft die Grundlage für die Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen darstellen. **§ 32d Abs. 3 BDSG-E** erlaubt jedoch nur den **automatisierten**

Abgleich von Beschäftigtendaten in **anonymisierter oder pseudonymisierter Form** und setzt zudem eine Datenverarbeitung **zur Aufdeckung von bestimmten Straftaten** oder anderen schwerwiegenden Pflichtverletzungen durch Beschäftigte voraus.

Anhand des Vergleichs mit der bankaufsichtsrechtlichen Vorgabe des § 25c Abs. 2 Satz 1 KWG zu „internen Sicherungsmaßnahmen" der Kreditinstitute wird deutlich, dass § 32d Abs. 3 BDSG-E als alleinige Compliance-Norm im Beschäftigtendatenschutzrecht für Kreditinstitute viel zu kurz greifen würde, weil das Bankaufsichtsrecht unberücksichtigt bliebe. Die Regelung wäre in der kreditwirtschaftlichen Praxis kaum umsetzbar.

§ 25c Abs. 2 Satz 1 KWG n. F.[1] verpflichtet Kreditinstitute, *„angemessene Datenverarbeitungssysteme zu betreiben und zu aktualisieren, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die auf Grund des öffentlich und im Kreditinstitut verfügbaren Erfahrungswissens über die Methoden der Geldwäsche, der Terrorismusfinanzierung und sonstigen strafbaren Handlungen im Sinne des Absatzes 1 Satz 1 als zweifelhaft oder ungewöhnlich anzusehen sind."*. Dabei dürfen laut § 25c Abs. 2 Satz 2 KWG n. F. die Kreditinstitute *„personenbezogene Daten erheben, verarbeiten und nutzen, soweit dies zur Erfüllung dieser Pflicht erforderlich ist"*. Aufgrund der Vielzahl von Zahlungsverkehrsvorgängen werden i. d. R. spezielle EDV-basierte Geldwäsche-Researchprogramme eingesetzt, die – eingestellt nach bestimmten Parametern – ein Monitoring des gesamten Zahlungsverkehrs durchführen. Die von der Überwachung betroffenen Kontoinhaber können dabei gleichzeitig Beschäftigte des Kreditinstituts sein, wenn sie z. B. ihr Gehaltskonto bei dem Arbeitgeber-Institut führen. Zur Erfüllung des § 32d Abs. 3 BDSG-E müssten nun sämtliche Kontodaten anonymisiert oder pseudonymisiert werden, bevor das Monitoring durchgeführt werden könnte. Dies kann praktisch kaum dargestellt werden, da es zu einem kosten- und zeitintensiven Mehraufwand (Umstellung der Systeme, zusätzliche Schritte bei der Verarbeitung einer immensen Datenmenge, Schaffung von Rechenkapazitäten, etc.) führen würde, der von jedem Kreditinstitut zu tragen wäre. Außerdem ist nicht einsichtig, warum Beschäftigte des Kreditinstituts, welches für sie ein Konto führt, einen höheren Schutz genießen sollten als „bloße" Kunden dieses Kreditinstituts. Darüber hinaus verlangt § 25c Abs. 2 KWG eine verdachtsunabhängige, also anlassfreie Überprüfung des Zahlungsverkehrs, wohingegen § 32d Abs. 3 BDSG-E zumindest nach seinem Wortlaut („zur Aufdeckung von Straftaten") einen konkreten Straftatverdacht voraussetzt. Der **§ 32d Abs. 3 BDSG-E ist daher auf die Besonderheiten in der Kreditwirtschaft nicht zugeschnitten und somit für sie nicht praktikabel**.

[1] "Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), das durch Artikel 2 des Gesetzes vom 1. März 2011 (BGBl. I S. 288) geändert worden ist".

3. Lösungsvorschläge

a. Allgemein

Wie aus der Stellungnahme des Bundesrates und der Gegenäußerung der Bundesregierung folgt, gibt es zur Vermeidung der aufgezeigten Probleme und zur Herstellung eines Einklangs zwischen dem Datenschutz- und Bankaufsichtsrecht zwei Wege: Ein – pragmatischer – Weg ist die Anpassung der Vorschriften in dem Gesetzentwurf, die wir im Folgenden beschreiben. Alternativ könnten aber auch – wie wohl von der Bundesregierung vor allem aus gesetzessystematischen Überlegungen angedacht – die bankaufsichtsrechtlichen Vorschriften dahin gehend ergänzt werden, dass in diese jeweils eine eigenständige datenschutzrechtliche Erlaubnisnorm aufgenommen wird. Dazu würde es sich anbieten, in das derzeit als Referentenentwurf der Bundesregierung vorliegende „Gesetz zur Optimierung der Geldwäscheprävention“ vom 30. März 2011 entsprechende Gesetzesänderungen aufzunehmen.

b. Einklang von Bankaufsichtsrecht und Beschäftigtendatenschutz durch Ergänzung von § 32c Abs. 1 Satz 2 Nr. 1 BDSG-E um „Kontroll- und Prüfpflichten“ aufgrund gesetzlicher Vorschriften

Um Bankaufsichtsrecht und Beschäftigtendatenschutz für die Kreditwirtschaft in Einklang zu bringen, muss im vorliegenden Gesetzesvorhaben eine **Grundlage für anlassfreie Kontrollen** von Mitarbeitern zur Durchführung der bankaufsichtsrechtlich gebotenen Betrugs-, Geldwäsche- und Korruptionsbekämpfung, zur Wertpapier-Compliance und zur Vermeidung von strafbaren Handlungen, die zu einer Gefährdung des Vermögens des Institutes führen können, geschaffen werden. Eine solche Grundlage für die Datenerhebung, –verarbeitung und –nutzung bieten die **§ 32c Abs. 1 Satz 2 Nr. 1 und Nr. 3 i. V. m. § 32d Abs. 1 BDSG-E**, wenn von diesem Erlaubnistatbestand zusätzlich auch gesetzlich oder aufgrund eines Gesetzes – hier durch das Bankaufsichtsrecht (z. B. § 25c KWG) – gebotene Kontroll- und Prüfungsmaßnahmen umfasst sind. Mithin würde das Bankaufsichtsrecht, wie bisher, die Kontroll- und Prüfungsmaßnahmen und damit verbundene Erhebungen, Verarbeitungen und Nutzungen von Mitarbeiterdaten determinieren.

Wir schlagen daher vor, § 32c Abs. 1 Satz 2 Nr. 1 BDSG-E um **„Kontroll- und Prüfpflichten“ zur Erfüllung von (bank-)aufsichtsrechtlichen Anforderungen** zu ergänzen. Die Vorschrift würde dann wie folgt lauten:

„Beschäftigtendaten dürfen vorbehaltlich der §§ 32e bis 32i erhoben werden, wenn dies für die Durchführung, Beendigung oder die Abwicklung des Beschäftigtenverhältnisses erforderlich ist. Dies ist insbesondere der Fall, soweit die Kenntnis dieser Daten für den Arbeitgeber erforderlich ist, um

1. *gesetzliche oder auf Grund eines Gesetzes bestehende Erhebungs-, Melde-, Auskunfts-, Offenlegungs-,* ***Kontroll-, Prüf-*** *oder Zahlungspflichten zu erfüllen,*
2. *… .“*

Die Erläuterungen zur Compliance in der Kreditwirtschaft in der Gesetzesbegründung zu § 32d Abs. 3 BDSG-E sollten dann auch in den erläuternden Gesetzesmaterialien zu § 32c Abs. 1 Satz 2 Nr. 1 BDSG-E übernommen werden. Dazu bietet es sich an, Kontroll- und Prüfpflichten als *„Pflichten von z. B. Kreditinstituten, Zahlungsinstituten, Finanzdienstleistungsunternehmen oder Wertpapierdienstleistungsunternehmen aus aufsichtsrechtlichen Vorgaben zur Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten oder Straftaten durch den Beschäftigten im Beschäftigungsverhältnis“* zu beschreiben. So wäre sichergestellt, dass die deutsche Kreditwirtschaft den auch **international geforderten Anforderungen an eine effektive Terrorismus-, Geldwäsche- und Korruptionsbekämpfung** sowie an eine wirksame Compliance weiterhin nachkommen kann. Insbesondere wären diese Ergänzungen ein wichtiger Baustein, um künftigen Beanstandungen des deutschen Rechts durch die Financial Action Task Force on Money Laundering vorzubeugen. Deren im Jahre 2009 durchgeführte Deutschland-Prüfung ist ein wesentlicher Anlass für den oben genannten Entwurf eines „Gesetzes zur Optimierung der Geldwäscheprävention“.

c. Konkretisierung der „Verhaltenskontrolle“ in § 32c Abs. 1 Satz 2 Nr. 3 BDSG-E unter Berücksichtigung bankaufsichtsrechtlicher Vorgaben

Zur Klarstellung bietet es sich an, in den Gesetzesmaterialien zu § 32c Abs. 1 Satz 2 Nr. 3 BDSG-E darzulegen, dass das Tatbestandsmerkmal der „Leistungs- und Verhaltenskontrolle“ auch der Erfüllung von (bank-)aufsichtsrechtlichen Anforderungen dienen kann. Diese Aussage klingt bereits auf Seite 4 des „Hintergrundpapiers zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes“ der Bundesregierung an, welches als Grundlage für die Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen das Recht des Arbeitgebers zur Verwendung von Beschäftigtendaten zur Leistungs- und Verhaltenskontrolle nennt.

d. Erweiterung des Anwendungsbereichs von § 32d Abs. 3 BDSG-E

Der § 32d Abs. 3 BDSG-E betrifft nur die „Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen". Bei enger Auslegung wäre damit von der Vorschrift – im Gegensatz zu § 32e BDSG-E – die „Verhinderung weiterer Straftaten oder schwerwiegender Pflichtverletzungen" nicht abgedeckt, was gerade in Bezug auf eine effektive Betrugs- und Korruptionsbekämpfung im Unternehmen zu kurz greifen würde, denn die aufsichtsrechtlichen Anforderungen legen gerade auf die Prävention besonderen Wert. Die Vorschrift sollte daher nicht nur die Aufklärung von begangenen Straftaten/anderen schwerwiegenden Pflichtverletzungen, sondern auch die „Verhinderung weiterer Straftaten oder schwerwiegender Pflichtverletzungen" ermöglichen.

e. Erweiterung des Straftatenkatalogs in § 32d Abs. 3 BDSG-E

Der Katalog der strafrechtlichen Regelbeispiele in **§ 32d Abs. 3 BDSG-E** ist zu eng gefasst, da er nicht alle Straftaten erfasst, die durch die (bank-)aufsichtsrechtlich vorgeschriebenen Maßnahmen verhindert werden sollen. Zudem würde aus der Fokussierung auf § 266 und § 299 StGB folgen, dass eigentlich nur die Führungsebene eines Unternehmens betroffen sein könnte, weil die Beschäftigten der darunter liegenden Ebenen oftmals keine Vermögensbetreuungspflicht haben. Im Sinne der unternehmensinternen Betrugsbekämpfung müssten eigentlich alle Vermögensdelikte erfasst werden.

Zudem ist § 25c Abs. 1 KWG zum 9. März 2011 dahingehend geändert worden, dass Kreditinstitute *„strafbare Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen können"* zu verhindern haben. Dies kann zu einer widersprüchlichen Gesetzeslage führen, da eine Einschränkung der in Betracht kommenden Straftatbestände in diesem Gesetz vom Gesetzgeber bewusst nicht vorgenommen wurde (s. BT-Drs. 17/3023, S. 60).

Wir schlagen zur Harmonisierung der genannten Regelungen vor, den Einschub „*insbesondere zur Aufdeckung von Straftaten nach den §§ 266, 299, 331 bis 334 des Strafgesetzbuchs*" ersatzlos zu streichen, um sowohl alle Vermögensdelikte als auch alle geldwäscherechtlich relevanten Straftaten zu erfassen.

C. Weitere aus Sicht der Kreditwirtschaft wichtige Punkte

1. § 32c Abs. 1 Satz 2 Nr. 1 BDSG-E – Weiter kollektive Rechtsinstrumente als Rechtsgrundlage zulassen

In **§ 32c Abs. 1 Satz 2 Nr. 1 BDSG-E** werden gesetzliche oder auf Grund eines Gesetzes bestehende Vorschriften genannt, aus denen sich Erhebungs-, Melde-, Auskunfts-, Offenlegungs- oder Zahlungspflichten ergeben können, für die eine Erhebung personenbezogener Daten erforderlich ist. Um heute bereits gemäß § 4 BDSG zulässigerweise erfolgende Datenerhebungen zu berücksichtigen, sollten als weitere Rechtsgrundlage für die zulässige Datenerhebung auch Instrumente des kollektiven Arbeitsrechts in der Vorschrift erwähnt werden, wie Tarifverträge und Betriebs-/Dienstvereinbarungen. Diese Vereinbarungen spielen bislang auch bei Kreditinstituten eine bedeutende Rolle, um einen unternehmensspezifischen Interessenausgleich zu erreichen. In Bezug auf konkrete Datenverarbeitungen und –nutzungen besteht damit noch kein „Freifahrtschein“, da nach § 32d Abs. 1 Nr. 3 BDSG immer das Korrektiv der Verhältnismäßigkeit greift. Auch haben es Arbeitgeber und Arbeitnehmervertretung in der Hand, bestehende Betriebsvereinbarungen nach den betrieblichen Belangen und Bedürfnissen anzupassen.

In **§ 32c Abs. 1 Satz 2 Nr. 1 BDSG-E** sollte daher ergänzend folgendes Regelbeispiel aufgenommen werden:

„1a. Pflichten aus Tarifverträgen und Betriebs-/Dienstvereinbarungen zu erfüllen“.

Sollte diesem Vorschlag nicht gefolgt werden, besteht die Gefahr, dass mit dem Inkrafttreten des neuen Beschäftigtendatenschutzrechts bewährte Betriebsvereinbarungen datenschutzrechtlich nicht mehr die Relevanz haben wie nach bisheriger Rechtslage. Das dürfte auch nicht im Interesse der Beschäftigten sein.

2. § 32e Abs. 6 BDSG-E - Löschpflicht aufgrund gesetzlicher Speicherungspflichten relativieren

Die vorgesehene unverzügliche Löschungspflicht kann mit Dokumentationspflichten im Rahmen der Betrugsprävention gemäß KWG und GwG kollidieren und sollte dahin gehend eingeschränkt werden, dass Datenspeicherung aufgrund gesetzlicher Anordnung (z. B. bankaufsichtsrechtlicher Vorgaben) von dem Löschgebot unberührt bleiben.

3. § 32e Abs. 7 BDSG-E – Verarbeitungsverbot zu weitgehend

Die Regelung berücksichtigt nicht hinreichend, dass z. B. Kreditinstitute Erkenntnisse aus der privaten Kontoführung ihrer Mitarbeiter, die sie aufgrund von gesetzlichen Prüfungspflichten erlangen, ggf. auch im arbeitsvertraglichen Verhältnis zu ihren Mitarbeitern verwenden müssen. Die Vorschrift ist folglich in Bezug auf bankaufsichtsrechtliche Vorgaben zu relativieren, um Widersprüche zwischen Beschäftigtendatenschutzrecht und Bankaufsichtsrecht zu vermeiden.

4. § 32i Abs. 1 bis 3 BDSG-E - Aufzeichnung von Inhalten von Telefondiensten an Bedürfnisse des Interbankenhandels anpassen

Die Aufzeichnung von Telefongesprächen steht bereits heute unter dem Regime des § 201 StGB und erfordert grundsätzlich die Einwilligung aller Betroffenen, wenn nicht auf andere Weise von ihrem Einverständnis auszugehen ist. Hierbei können auch Handelsbräuche maßgeblich sein, wie bei der **Aufzeichnung von Telefonaten im Interbankenhandel**.

In der gesamten Finanzbranche (Kreditinstitute, Versicherer) werden die Gespräche der Handelsabteilungen (Wertpapiere, Devisen etc.) telefonisch aufgezeichnet. Es geht dabei um Handelsgeschäfte zwischen Finanzdienstleistern und institutionellen Investoren/anderen Finanzdienstleistern. Dies ist eine etablierte Marktpraxis, die sich auch in der datenschutzrechtlichen und strafrechtlichen Diskussion durchgesetzt hat. Diese Marktpraxis ist erforderlich, da während eines Telefonats Rechtsgeschäfte abgeschlossen werden, die häufig siebenstellige Summen und mehr überschreiten und ein beiderseitiges Beweisinteresse am Inhalt der Telefonate besteht. Dieses Vorgehen wird auch von der Bankenaufsicht nahegelegt (vgl. BTO 2.2.1.4 des von der Bundesanstalt für Finanzdienstleistungsaufsicht veröffentlichten Rundschreibens 6/2007 Mindestanforderungen für das Risikomanagement (MaRisk)). Daher sollte eine Ergänzung aufgenommen werden, nach der eine Aufzeichnung von Telekommunikationsdaten und –inhalten auch dann zulässig ist, wenn dies zum Beispiel aufgrund von **Handelsbräuchen** etabliert ist.

Eine nach Absatz 2 erforderliche Einwilligung sowie konkrete Belehrung der Gesprächsteilnehmer erfolgt dabei nicht flächendeckend. Auf Grund des etablierten Marktbrauchs wird dies auch nicht für erforderlich erachtet. Wenn überhaupt, dann werden zwischen den beteiligten Finanzdienstleistern Erklärungen ausgetauscht, die eine entsprechende Praxis rechtfertigen.

Deshalb sollte Absatz 2 weiter gefasst werden und eine Erhebung und Nutzung von Inhalten auch dann erlaubt sein/werden, wenn zwar keine Einwilligung vorliegt bzw. keine Information des Gesprächspartners stattfand, die Aufzeichnung aber der Marktpraxis entspricht.

5. § 32i Abs. 4 BDSG-E - Gemischte Nutzung von Telekommunikationseinrichtungen des Arbeitgebers nicht in Frage stellen

Wir regen an, zur Klarstellung die Erläuterungen auf Seite 6 des „Hintergrundpapiers zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes“ der Bundesregierung in die Gesetzesmaterialien zu übernehmen. Ansonsten könnte bei reiner Lektüre des Gesetzestextes der ungewollte Eindruck entstehen, dass eine sowohl dienstliche als auch private Nutzung faktisch verboten wird, weil ansonsten der Arbeitgeber Gefahr liefe, im Bereich der betrieblichen Telekommunikationseinrichtungen keine Kontrollmöglichkeiten zu haben. Es muss weiterhin die Möglichkeit bestehen, dass der Arbeitgeber die Privatnutzungserlaubnis z.B. des dienstlichen E-Mail-Accounts von der Einwilligung des Mitarbeiters abhängig macht, dass dieser ihm umgekehrt die gleichen Einsichts- und Kontrollmöglichkeiten gestattet, die der Arbeitgeber bei einem rein dienstlichen Account hätte.

6. § 32l Abs. 1 BDSG-E – Einwilligung nicht einschränken

a. Einwilligungsverbot ist unpraktikabel und inkompatibel mit EU-Recht

Das grundsätzliche **Einwilligungsverbot** mit Ausnahmevorbehalt ist **nicht praktikabel** und **widerspricht der EU-Datenschutzrichtlinie**.

Der abschließende Einwilligungskatalog wird der vielgestaltigen und sich ändernden Arbeitswirklichkeit nicht gerecht. Der Schutz der Beschäftigten wird durch eine Streichung nicht ausgehebelt, sondern bleibt den Parteien, z. B. über Betriebsvereinbarungen oder notfalls den Gerichten vorbehalten, die die vielfältigen praktischen Bedürfnisse der Arbeitgeber und der Beschäftigten viel besser in Einklang zu bringen vermögen, als eine starre gesetzliche Regelung.

Gerade bei zentralisierten Personalverwaltungen in Konzernen und Verbünden können bestimmte Datenübermittlungsvorgänge im Konzern zur Ermöglichung der Mitarbeitersteuerung und -förderung sowie des übergreifenden Mitarbeitereinsatzes nur durch

Betriebsvereinbarungen oder Einwilligungserklärungen der Beschäftigten datenschutzrechtlich abgesichert werden. Folglich wären Unternehmensverbünde und Konzernunternehmen von dem Einwilligungsverbot mit Ausnahmevorbehalt besonders betroffen. Deshalb sollte dieser Ansatz überdacht werden und – wie auch vom Bundesrat gefordert – praktikable Lösungen in Konzernen/Verbünden zur Mitarbeiterdatenverwaltung gefunden werden.

Ferner bestehen deutliche Zweifel, ob das Einwilligungsverbot im Einklang mit der EU-Datenschutzrichtlinie steht, die die Einwilligung als gleichwertigen Erlaubnistatbestand gegenüber gesetzlichen Erlaubnisvorschriften einordnet.

Überdies könnte § 32l BDSG-E zu einer Unzulässigkeit der bisherigen Datenverarbeitung aufgrund von Einwilligungen der Beschäftigten führen mit der Folge, dass bereits erhobene Daten aufwändig gesichtet und gelöscht werden müssten.

b. Erschwerung der Telearbeit bei Auslagerung der Datenverarbeitung

Das grundsätzliche Einwilligungsverbot hat auch nachteilige Effekte auf die Telearbeit, der vor dem Hintergrund der politisch gewollten Flexibilität von Arbeitnehmern sowie Vereinbarkeit von Beruf und Familie immer größere Bedeutung zukommt.

Dazu ist zunächst festzustellen, dass auch bei Kreditinstituten vielfach die tatsächliche Datenverarbeitung im Rahmen von Auftragsdatenverarbeitungsverhältnissen im Sinne des § 11 BDSG ausgelagert ist und die Auftragnehmer zur Erbringung der Dienstleistung hierbei auch die Telearbeit nutzen. Dabei sind gemäß § 11 BDSG Kontrollrechte des Auftraggebers beim Auftragnehmer und dessen Mitwirkungs- und Duldungspflichten zu regeln. Auch wenn sich die Banken nicht im Rahmen der Auftragsdatenverarbeitung bewegen, sondern eine Funktionsübertragung vorliegt oder überhaupt keine personenbezogene Datenverarbeitung (z. B. reine Firmenkundendaten) stattfindet, muss sich die auslagernde Bank nach § 25a KWG und MaRisk die Kontrollrechte beim IT-Dienstleister vorbehalten.

Beim Dienstleister werden diese Kontrollrechte der Bank wiederum in Gestalt von Betriebsvereinbarungen oder Einwilligungslösungen gegenüber den Arbeitnehmern des Auftragnehmers umgesetzt. Konkret geht es hierbei beispielsweise um die Ermöglichung der Rufbereitschaft für Spezialisten oder Systemadministratoren. Diese müssen sich notfalls auch nachts, wenn die wichtige Batch-Verarbeitung für die Zahlungsbuchungen stattfindet, die am nächsten Morgen erfolgt sein müssen, vom Telearbeitsplatz aus in die DV-Systeme einloggen können. Hierbei müssen vom Auftraggeber mit dem Auftragnehmer die Absicherungs-

maßnahmen und die Kontrollrechte gesondert geregelt und die Arbeitnehmer durch eine Betriebsvereinbarung oder Einwilligung eingebunden werden können. Dieser Lösungsweg würde aber durch die vorgesehene Regelung des § 32l Abs. 1 BDSG-E verbaut werden mit der Folge, dass die Kreditinstitute von Telearbeit auf Präsenzarbeit umstellen müssten und es möglicherweise bei der Fehlerbehebung zu Verzögerungen käme.

Da Fernwartungszugriffe, die auch eine übliche Praxis im IT-Umfeld sind, nach § 11 Abs. 5 BDSG nach den gleichen Bestimmungen, wie die Auftragsdatenverarbeitung geregelt werden sollen, stellt sich auch dort das gleiche Problem.