

## ***Europäischen Datenschutz angemessen aktualisieren***

### **Stellungnahme zum Entwurf einer europäischen Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)**

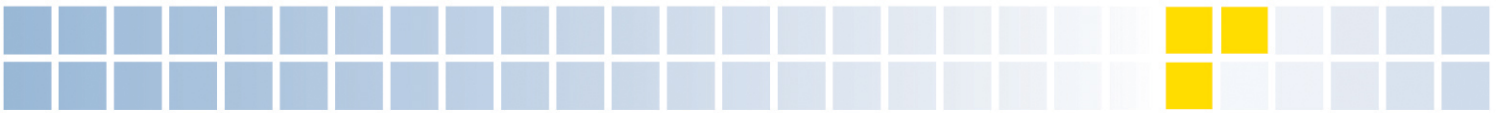
15. Mai 2012

#### ***Zusammenfassung***

- **Kollektivvereinbarungen** wie Tarifverträge und Betriebsvereinbarungen müssen Grundlage für eine Datenverarbeitung sein können.
- Der pauschale Ausschluss der **Einwilligung** in die Datenverarbeitung in bestimmten Sachverhalten ist nicht akzeptabel. Die Einwilligung muss z.B. auch weiterhin im Beschäftigungsverhältnis erteilt werden können.
- **Gesundheitsdaten** eines Arbeitnehmers müssen weiterhin rechtssicher verarbeitet werden können.
- Der Verordnungsvorschlag legt umfangreiche **Informations- und Auskunftspflichten** fest, die zu erheblichen Belastungen führen können. An verschiedenen Stellen sind deshalb Veränderungen erforderlich.
- Bislang bleibt die Chance ungenutzt, eine Regelung zum **konzerninternen Datentransfer** zu schaffen. Diese Lücke muss geschlossen werden.
- Unverhältnismäßiger Aufwand bei der **Auftragsdatenverarbeitung** lässt sich dadurch vermeiden, dass der Auftragnehmer eine Bestätigung der Einhaltung der Datenschutzverordnung erteilt.
- Die umfangreichen **Dokumentationspflichten** würden im Unternehmen dazu führen, dass ein wesentlicher Teil der Arbeitszeit auf die Dokumentation entfallen würde. Das ist weder vor dem Hintergrund wirtschaftlicher noch praktischer Erwägungen haltbar.
- Damit die Aufsichtsbehörde sich beim Thema **Datensicherheit** auf wesentliche Fälle konzentrieren kann, wäre es sinnvoll, dass nur solche Verletzungen angezeigt werden müssen, die eine schwerwiegende Beeinträchtigung für die betroffene Person nach sich ziehen.
- Eine **Datenschutz-Folgenabschätzung** ohne jegliche Ausnahmen ist überflüssig und schafft nur neue, unnötige bürokratische Verfahren.
- Die Einführung eines unechten **Verbandsklagerechts** wird den unter

---

Die BDA ist die sozialpolitische Spitzenorganisation der gesamten deutschen gewerblichen Wirtschaft. Sie vertritt die Interessen kleiner, mittelständischer und großer Unternehmen aus allen Branchen in allen Fragen der Sozial- und Tarifpolitik, des Arbeitsrechts, der Arbeitsmarktpolitik sowie der Bildung. Die BDA setzt sich auf nationaler, europäischer und internationaler Ebene für die Interessen von einer Mio. Betrieben ein, die 20 Mio. Arbeitnehmer beschäftigen und die der BDA durch freiwillige Mitgliedschaft in Arbeitgeberverbänden verbunden sind. Die Arbeitgeberverbände sind in den der BDA unmittelbar angeschlossenen 52 bundesweiten Branchenorganisationen und 14 Landesvereinigungen organisiert.



schiedlichen Rechtstraditionen in Europa nicht ausreichend gerecht. Eine Sammelklage führt zu Friktionen mit dem System des in Kontinentaleuropa verordneten individuellen Rechtsschutzprinzips.

- Die EU-Kommission verliert bei der Festsetzung der Höhe eines **Bußgeldes** den Verhältnismäßigkeitsgrundsatz völlig aus den Augen. Zudem fehlt eine Differenzierung im Hinblick auf die hinter einem Datenschutzverstoß stehende Motivation und Absicht.
- Wenn sich die Union dazu entscheidet, den Datenschutz in einer Verordnung zu regeln, sollte auch der Arbeitnehmerdatenschutz Teil dieser Verordnung werden. Nur wenn es nicht gelingt, Kollektivvereinbarungen des Arbeitsrechts, die Einwilligung und andere Elemente einheitlich durch die Verordnung festzulegen, bedarf es einer **Öffnungsklausel** für das Arbeitsrecht. Diese muss die Gegebenheiten des Arbeitsrechts so berücksichtigen, dass sie weiter Handlungsmöglichkeiten für den nationalen Gesetzgeber und die Parteien des Arbeitsverhältnisses vorsieht.

## Einleitung

Am 25. Januar 2012 hat die EU-Kommission einen Verordnungsvorschlag zum Datenschutz vorgelegt. Mit dem Vorschlag zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr will die EU-Kommission einen neuen Rechtsrahmen zum Schutz personenbezogener Daten in der EU schaffen.

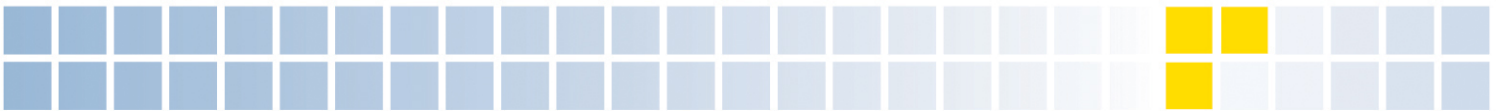
Zu Recht wird von vielen Stimmen in der Literatur die mangelnde Rechtssetzungskompetenz der Union hervorgehoben. Artikel 16 Absatz 2 und Artikel 114 Absatz 1 AEUV bieten keine hinreichende Grundlage für einen so weit gehenden Regelungsansatz. Auch

wenn ein einheitlicher Rahmen für den Datenverkehr innerhalb der Union zu wünschen ist, darf eine entsprechende gesetzliche Regelung nicht ohne Ermächtigungsgrundlage getroffen werden. Diese Rechtsgrundlage besteht nicht.

Die BDA setzt sich dafür ein, dass bei der Schaffung eines neuen Konzepts zum Schutz personenbezogener Daten insbesondere folgende Punkte verwirklicht werden:

- Die Einwilligung muss im Beschäftigungsverhältnis erteilt werden können.
- Kollektivvereinbarungen wie Tarifverträge und Betriebsvereinbarungen müssen Grundlage für eine Datenverarbeitung sein können.
- Regelungen müssen geschaffen werden, die den konzerninternen Datentransfer erleichtern.
- Bürokratische Belastungen müssen so gering wie möglich sein.
- Die Sanktionsregelungen müssen für die Datenverarbeitung in Beschäftigungsverhältnissen auf ein angemessenes Maß zurückgeführt werden.

Eine abschließende Bewertung des Verordnungsvorschlages ist angesichts der Vielzahl der sogenannten „delegierten Rechtsakte“ zum jetzigen Zeitpunkt nicht möglich. Der Verordnungsvorschlag sieht an 26 Stellen „delegierte Rechtsakte“ vor. Hiermit wird der EU-Kommission die Befugnis eingeräumt, Rechtsakte zur Konkretisierung bestimmter Vorschriften der Verordnung verabschieden zu können. Die umfangreiche Anwendung dieses Instruments ist bedenklich. Es muss bezweifelt werden, dass sich die delegierten Rechtsakte tatsächlich nur auf nicht wesentliche Vorschriften beziehen, wie der Vertrag von Lissabon dies vorgesehen hat.



## **Im Einzelnen**

### **Artikel 3 – räumlicher Anwendungsbe- reich**

Regelungsgehalt: Neben der Datenverarbeitung innerhalb der EU sollen die neuen Regelungen auch für Datenverarbeiter außerhalb der EU gelten, wenn sie personenbezogene Daten von Betroffenen verarbeiten, die in der EU ansässig sind. Zudem muss sich die Datenverarbeitung auf das Anbieten von Waren oder Dienstleistungen in der EU beziehen oder der Verhaltensbeobachtung dienen.

Bewertung: Die Ausdehnung des Geltungsbereichs des europäischen Datenschutzrechts auf Unternehmen aus Drittstaaten, die ihre Dienste EU-Bürgern anbieten, ist zu begrüßen. Gerade netzbasierte Geschäftsmodelle erfordern keinen Sitz in der EU, um hier tätig zu werden. Die Ausdehnung des Geltungsbereichs sorgt so für ein level playing field. Dabei ist jedoch klarzustellen, wie der in Artikel 3 Absatz 2 verwendete Begriff „ansässig“ zu verstehen ist.

### **Artikel 5 Buchstabe a - Verarbeitungs- grundsätze**

Regelungsgehalt: Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Bewertung: Es wird nicht weiter ausgeführt, wann eine Verarbeitung in „nachvollziehbarer Weise“ erfolgt. Um hier Rechtssicherheit zu schaffen, ist eine Ergänzung dahingehend erforderlich, dass sich die Möglichkeit des Nachvollziehens nach objektiven Kriterien richten muss. Andernfalls bestünde die Gefahr, dass bei der Datenverarbeitung auf den Empfängerhorizont jeder einzelnen Person abgestellt werden müsste, was in der Praxis nicht zu leisten wäre.

### **Artikel 6 Absatz 1 Buchstabe b, c - Tarif- verträge, Betriebsvereinbarungen**

Regelungsgehalt: Der Verordnungsvorschlag sieht in Artikel 6 Absatz 1 Buchstabe b, c vor, dass die Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrages oder einer gesetzlichen Verpflichtung erforderlich sein muss.

Bewertung: Dies berücksichtigt die nationalen Besonderheiten nicht ausreichend. So gilt z.B. in Deutschland, dass Kollektivvereinbarungen wie Tarifverträge und Betriebsvereinbarungen staatlich gesetztem Recht gleichstehen und somit Grundlage für eine rechtmäßige Datenverarbeitung sein können. Kollektivvereinbarungen sind ein Garant für ein ausgewogenes Datenschutzniveau. Die Betriebsvereinbarung dient dabei vorrangig dazu, unbestimmte Rechtsbegriffe im Datenschutzrecht für die Unternehmen und ihre Mitarbeiter zu konkretisieren und Verfahrensabläufe rechtssicher zu handhaben. Dem Ziel eines praxisnahen Datenschutzes genügen solche Regelungen deshalb vielfach besser und nachhaltiger als gesetzliche Vorgaben. Deshalb muss sichergestellt werden, dass auch Kollektivvereinbarungen wie Tarifverträge und Betriebsvereinbarungen rechtmäßige Grundlage für eine Datenverarbeitung sein können.

### **Artikel 7 Absatz 4 - Einwilligung**

Regelungsgehalt: Gemäß Artikel 7 Absatz 4 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. Nach den Erwägungsgründen soll dies gerade im Beschäftigungsverhältnis der Fall sein, so dass hier eine Einwilligung nicht mehr als Rechtsgrundlage für eine Datenverarbeitung herangezogen werden könnte.



**Bewertung:** Der pauschale Ausschluss der Einwilligung in die Datenvereinbarung im Beschäftigungsverhältnis ist nicht akzeptabel. Sie muss auch weiterhin im Beschäftigungsverhältnis erteilt werden können. Andernfalls würde dem Arbeitnehmer vollständig die Möglichkeit genommen, selbst über die Verwendung seiner Daten zu entscheiden. Die Einwilligung wird im Beschäftigungsbereich zumeist dann erteilt, wenn es um Bereiche geht, in denen es gerade im Interesse des jeweiligen Mitarbeiters liegt, die Verarbeitung und Nutzung seiner persönlichen Daten freizugeben. Um diese Möglichkeit auch zukünftig nicht auszuschließen, ist zumindest zu klären, in welchen einzelnen Bereichen eines Beschäftigungsverhältnisses die Einwilligung weiterhin möglich ist. Die Einwilligung ist auf jeden Fall für Datenverarbeitungen unersetzlich, die auf freiwilligen Leistungen des Arbeitgebers wie Kindergärten oder Restaurantbetriebe beruhen.

#### **Artikel 9 - besondere Kategorien von Daten**

**Regelungsgehalt:** Gemäß Artikel 9 Absatz 2 h i.V.m. Artikel 81 ist die Verarbeitung von Gesundheitsdaten möglich, wenn sie für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin erfolgt. Artikel 9 Absatz 2 j sieht vor, dass Daten über Strafurteile nur unter bestimmten Voraussetzungen verarbeitet werden dürfen.

**Bewertung:** Es muss sichergestellt werden, dass Gesundheitsdaten eines Arbeitnehmers weiterhin verarbeitet werden können. Die aktuellen Formulierungen führen in der Praxis jedoch zu Rechtsunsicherheit. Es ist eine Klarstellung dahingehend notwendig, dass die in Artikel 9 Absatz 2 aufgeführten Fälle der möglichen Datenverarbeitung besonderer Kategorien personenbezogener Daten alternativ gelten. Andernfalls liefe man Gefahr, sich rechtswidrig zu verhalten, wenn man zum Beispiel in Personaldatensystemen aus Entgeltgründen Fehltag wegen krank-

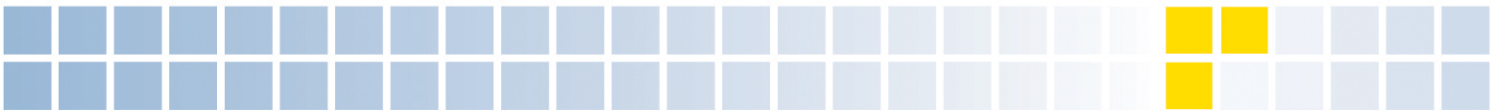
heitsbedingten Abwesenheiten speichert, da Gesundheitsdaten im Sinne von Artikel 4 Absatz 12 gemäß Artikel 9 Absatz 2 h i.V.m. Artikel 81 u.a. nur für Zwecke der Gesundheitsvorsorge verarbeitet werden dürfen. Gesundheitsdaten unterliegen als besondere Arten personenbezogener Daten bereits einem ausreichenden Schutz, der nicht ausgeweitet werden muss.

Für viele Unternehmen ist es erforderlich, zum Beispiel aufgrund von Compliance-Anforderungen oder im Rahmen von Bewerbungsverfahren Daten über Strafurteile zu erheben. Es ist eine Regelung wünschenswert, die die Verarbeitung von Daten für diese Zwecke erlaubt.

#### **Artikel 12, 14, 15, 18 - Informations- und Auskunftspflichten**

**Regelungsgehalt:** Der Verordnungsvorschlag legt umfangreiche Informations- und Auskunftspflichten des für die Verarbeitung Verantwortlichen fest. Gemäß Artikel 12 Absatz 1 sollen Maßnahmen zur Information des Betroffenen elektronisch beantragt werden können, wenn personenbezogene Daten automatisch verarbeitet werden. Die Unterrichtung muss gemäß Absatz 2 dann ebenfalls elektronisch erfolgen. Gemäß Artikel 18 Absatz 1 soll die betroffene Person das Recht haben, eine Kopie der verarbeiteten Daten in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format zu verlangen. Das elektronische Format kann von der EU-Kommission festgelegt werden.

**Bewertung:** Bei den Vorgaben zu den Informations- und Auskunftspflichten wird deutlich, dass die EU-Kommission im Sinne eines „lex facebook“ vorrangig Unternehmen im Blick hatte, deren unternehmerischer Hauptzweck das Sammeln von personenbezogenen Daten ist. Die bürokratischen Pflichten sind jedoch für die Datenverarbeitung im Beschäftigungsverhältnis besonders durch



kleine und mittelständische Unternehmen völlig unangemessen.

Die Regelungen in Artikel 12 des Verordnungsvorschlags können insbesondere für Klein- und Mittelbetriebe zu einer erheblichen Belastung führen, wenn erst entsprechende elektronische Vorkehrungen getroffen werden müssen, damit das Verfahren elektronisch abgewickelt werden kann. Gerade in kleineren Unternehmen mit täglichem unmittelbarem Kontakt zwischen dem für die Verarbeitung Verantwortlichen und dem Betroffenen ist die Einführung einer elektronischen Form überflüssig. Auch der Hinweis auf Standardvorlagen und -verfahren bringt hier kaum Erleichterung. Ob, und wenn ja, wie die EU-Kommission von der Möglichkeit Gebrauch macht, Vereinfachungen für Kleinst- und Kleinunternehmen und mittlere Unternehmen einzuführen, ist zum jetzigen Zeitpunkt unklar.

Die Ausweitung der Informations- und Auskunftsrechte der Artikel 14 und 15 im Vergleich zu den Regelungen der Datenschutzrichtlinie sind bedenklich. Dem für die Verarbeitung Verantwortlichen werden zusätzliche Verpflichtungen auferlegt, die ihn erheblich belasten. So wird zum Beispiel in Artikel 14 Absatz 1 c und Artikel 15 Absatz 1 d geregelt, dass der für die Verarbeitung Verantwortliche der betroffenen Person die Dauer mitteilen muss, für die die personenbezogenen Daten gespeichert werden. Die Speicherdauer für solche Daten variiert im Beschäftigungsbereich stark. Die Mitteilung ist nur mit einem erheblichen bürokratischen Aufwand möglich. In Zeiten, in denen Bürokratie abgebaut und nicht neue aufgebaut werden sollte, ist eine solche Vorgabe kontraproduktiv. Das gilt umso mehr, als das Auskunftsrecht des Betroffenen gemäß Artikel 15 nicht zeitlich beschränkt wird. Um im Sinne eines kooperativen Betriebsklimas arbeiten zu können, sollte dieser Anspruch auf eine Auskunft pro Kalenderjahr begrenzt werden.

Bürokratielastig ist auch die in Artikel 14 Absatz 3 geregelte Pflicht, die Herkunft personenbezogener Daten mitzuteilen, wenn diese Daten nicht bei der betroffenen Person erhoben wurden. Diese Verpflichtung sieht die Richtlinie 95/46/EG für die Informationspflichten nicht vor. Sie ist mit einem erheblichen Mehraufwand verbunden, zumal diese Information nicht auf die verfügbaren Informationen, wie in Artikel 15 Absatz 1 g, beschränkt ist.

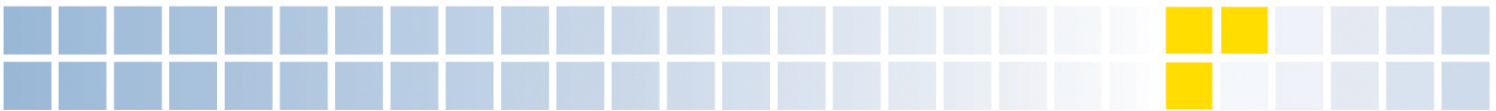
Der in Artikel 14 Absatz 5 a vorgesehene Wegfall der Informationspflicht, falls die betroffene Person bereits über die Informationen des Artikel 14 Absätze 1 bis 3 verfügt, ist zu eng. In der Praxis wird danach ohne erkennbare sachliche Rechtfertigung wesentlich häufiger informiert werden müssen, als dies nach § 33 Absatz 2 BDSG, der sich bewährt hat, der Fall ist. Deshalb sollte die Informationspflicht des Artikel 14 bereits dann nicht eingreifen, wenn die betroffene Person Kenntnis von der Speicherung oder der Übermittlung personenbezogener Daten erlangt hat.

Das in Artikel 18 enthaltene Recht auf Datenportabilität ist zum Schutz der Persönlichkeitsrechte des Betroffenen nicht erforderlich. Es ist sinnvoll, dass die betroffene Person die über sie gespeicherten Daten lesen und ggf. ausdrucken kann. Der Betroffene hat hier durch ein einheitliches Format keinen Mehrwert.

### **Artikel 20 – Profiling**

Regelungsgehalt: Eine natürliche Person darf nicht einer Maßnahme unterworfen werden, die auf einer rein automatisierten Datenverarbeitung beruht. Das gilt dann, wenn die Maßnahme ihr gegenüber Rechtswirkung entfaltet oder sie in maßgeblicher Weise beeinträchtigt und bestimmte Zwecke verfolgt werden. Hiervon sind Ausnahmen vorgesehen.





**Bewertung:** Diese Regelung kann Bedeutung für automatisierte Auswahlverfahren haben, in denen z.B. Mindestnoten festgesetzt werden. Gemäß Artikel 20 Absatz 2 a darf eine Person u.a. dann einer Maßnahme unterworfen werden, wenn gleichzeitig Vorkehrungen, wie ein Recht auf direkten persönlichen Kontakt getroffen wurden, um die berechtigten Interessen der betroffenen Person zu wahren. Ein solches Recht ist sehr weitgehend und würde gerade bei einer Vielzahl von Bewerbungen die Unternehmen vor erhebliche Herausforderungen stellen. In der Praxis hat sich als völlig ausreichend erwiesen, dass die Person die Möglichkeit hat, ihren Standpunkt geltend zu machen – so wie Artikel 15 Absatz 2 a der Datenschutzrichtlinie 95/46/EG dies vorsieht.

### **Artikel 23 – Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen**

**Regelungsgehalt:** Der für die Verarbeitung Verantwortliche setzt unter Berücksichtigung des Standes der Technik Verfahren und technische und organisatorische Maßnahmen ein, die sowohl den Zwecken der Verarbeitung als auch den Zielsetzungen der Verordnung genügen.

**Bewertung:** Der Einsatz technischer und organisatorischer Verfahren und Maßnahmen sollte stärker an einem Risiko orientierten Ansatz ausgerichtet werden. Die Verarbeitung besonderer Kategorien personenbezogener Daten rechtfertigt höhere Anforderungen als die Verarbeitung einfacher Adressdaten.

### **Artikel 26 – Auftragsverarbeiter**

**Regelungsgehalt:** In Artikel 26 des Verordnungsvorschlags wird festgelegt, welche Regelungen getroffen werden müssen, damit ein für die Verarbeitung Verantwortlicher eine weitere Person beauftragen kann. Der Verantwortliche muss dafür sorgen, dass die

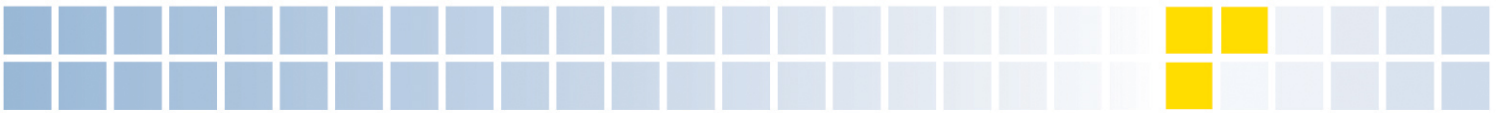
getroffenen Schutzmaßnahmen eingehalten werden.

**Bewertung:** Der Vorschlag sieht vor, dass der Verantwortliche dafür zu sorgen hat, dass der Auftragsverarbeiter Schutzmaßnahmen einhält. Er lässt ihn aber im Unklaren darüber, wann diese Verpflichtung als erfüllt anzusehen ist. Dies ist gerade für kleinere Unternehmen nur mit unverhältnismäßigem Aufwand zu leisten. Diese nutzen die Auftragsdatenverarbeitung häufig, um z.B. die Lohnbuchhaltung auf Dritte zu übertragen. Dafür brauchen sie Rechtssicherheit. Deshalb sollte es ausreichend sein, dass das Unternehmen, das den Auftrag zur Datenverarbeitung vergibt, auch dann seinen Pflichten nach dem Gesetz genügt, wenn der Auftragnehmer eine entsprechende Bestätigung der Einhaltung der Datenschutzverordnung erteilt. Durch eine solche Bestätigung lässt sich unbürokratisch der Aufwand, der aus ständigen Überprüfungen folgt, vermeiden. Artikel 26 darf nicht zu ähnlichen Rechtsanwendungsproblemen führen, wie dies bei § 11 BDSG, der zurzeit entsprechenden deutschen Vorschrift, der Fall ist. Artikel 26 Absatz 1 2. Halbsatz sollte deshalb gestrichen werden.

### **Artikel 28 – Dokumentationspflichten**

**Regelungsgehalt:** Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter und Vertreter müssen umfangreichen Dokumentationspflichten nachkommen.

**Bewertung:** Während bislang solche umfangreichen Pflichten sich nur im Rahmen der Meldepflicht des Artikels 19 der Datenschutzrichtlinie 95/46/EG bzw. Artikel 4e BDSG finden, die unter bestimmten Voraussetzungen entfallen kann, soll die nun vorgesehene Dokumentationspflicht grundsätzlich gelten. Ausnahmen sind für Unternehmen nur dann vorgesehen, wenn ein Unternehmen weniger als 250 Beschäftigte hat und die Datenverarbeitung eine Nebentätigkeit



ist. Dies führt dazu, dass vielfach eine weitreichende Dokumentation eingeführt werden müsste. Diese Dokumentationspflichten würden im Unternehmen, in denen der Umgang mit personenbezogenen Daten Alltag ist, dazu führen, dass ein wesentlicher Teil der Arbeitszeit auf die Dokumentation entfallen würde. Das ist weder vor dem Hintergrund wirtschaftlicher noch praktischer Erwägungen haltbar. Der auch an dieser Stelle vorgesehene Auf- und nicht Abbau von Bürokratie ist höchst bedenklich.

### **Artikel 31, 32 – Datensicherheit**

Regelungsgehalt: Im Hinblick auf die Verletzung des Schutzes personenbezogener Daten sieht der Entwurf strenge Regeln vor. So muss z.B. möglichst binnen 24 Stunden nach Feststellung der Verletzung des Schutzes personenbezogener Daten die Aufsichtsbehörde benachrichtigt werden. Darüber hinaus soll die Wahrscheinlichkeit einer Beeinträchtigung der Privatsphäre oder des Datenschutzes durch die Verletzungshandlung dazu führen, dass der Betroffene benachrichtigt werden muss.

Bewertung: Die EU-Kommission hat hier außer Acht gelassen, dass nicht jede Verletzung gravierende Auswirkungen auf den Betroffenen hat. Damit die Aufsichtsbehörde sich auf wesentliche Fälle konzentrieren kann, wäre es sinnvoll, dass nur solche Verletzungen angezeigt werden müssen, die eine schwerwiegende Beeinträchtigung für die betroffene Person nach sich ziehen. Darüber hinaus rechtfertigt nicht jede Verletzung des Schutzes personenbezogener Daten die strikten Rechtsfolgen. Das deutsche Recht konzentriert sich auf solche Fälle, in denen es um besondere Arten personenbezogener Daten geht, um Daten, die einem Berufsgeheimnis unterliegen, um Daten im Zusammenhang mit strafbaren Handlungen oder Ordnungswidrigkeiten sowie um Daten zu Bank- oder Kreditkartenkonten.

Die 24-Stunden-Frist gibt zudem ein zu starres Korsett vor. Vielmehr sollte der Begriff „unverzüglich“ genutzt werden. Er gibt Spielraum, um dem jeweiligen Einzelfall Rechnung zu tragen.

Weiterhin ist zu beachten, dass die Pflicht zur Benachrichtigung des Betroffenen Unsicherheiten birgt. So soll im Anschluss an die Meldung an die Aufsichtsbehörde auch der Betroffene selbst benachrichtigt werden, „wenn die Wahrscheinlichkeit besteht, dass der Schutz personenbezogener Daten oder der Privatsphäre [...] durch eine festgestellte Verletzung des Schutzes personenbezogener Daten beeinträchtigt wird“. Die Einführung des unbestimmten Rechtsbegriffs „wahrscheinlich“ führt zu Rechtsunsicherheit. Darüber hinaus ist die Formulierung des zitierten Tatbestands insgesamt nicht eindeutig.

Darüber hinaus muss sichergestellt werden, dass als Folge des Verbots des Selbstbelastungszwangs eine Meldung des für die Verarbeitung Verantwortlichen an die Aufsichtsbehörde in einem eventuell folgenden Sanktionsverfahren nur mit seiner Zustimmung verwertet werden darf.

### **Artikel 33, 34 – Datenschutz-Folgenabschätzung**

Regelungsgehalt: Bei Datenverarbeitungen, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten der betroffenen Person bergen, muss der Verantwortliche gemäß Artikel 33 vorab eine Folgenabschätzung vornehmen. Sie wird der Aufsichtsbehörde gem. Artikel 34 Absatz 6 vorgelegt. Könnten die Verarbeitungsvorgänge hohe konkrete Risiken bergen, ist die Aufsichtsbehörde gemäß Artikel 34 Absatz 2 a vorab zu Rate zu ziehen.

Bewertung: Eine Datenschutz-Folgenabschätzung ohne jegliche Ausnah-



men, wie das Vorliegen einer gesetzlichen Verpflichtung oder Einwilligung, 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), 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 t eine empfindliche Geldbuße verhängt werden kann.

#### **Artikel 35 ff – Datenschutzbeauftragter**

Regelungsgehalt: Der Verordnungsentwurf sieht vor, dass ein Datenschutzbeauftragter von Unternehmen mit mehr als 250 Mitarbeitern benannt werden muss. Nach Artikel 35 Absatz 2 ist die Bestellung eines Konzerndatenschutzbeauftragten zulässig. Es werden die Vorschriften zum Datenschutzbeauftragten ausgeweitet, z.B. sollen der Öffentlichkeit der Name und die Kontaktdaten des Datenschutzbeauftragten mitgeteilt werden.

Bewertung: Auch in Bezug auf den Datenschutzbeauftragten sollten die Grundsätze der Vermeidung von Bürokratie Anwendung finden. Das Interesse der Öffentlichkeit, über einen Datenschutzbeauftragten informiert zu werden, steht in keinem Verhältnis zum möglichen Aufwand des für die Verarbeitung Verantwortlichen, zumal völlig unklar ist, wie eine solche Information erfolgen muss.

Um einen zusätzlichen Anreiz zur Benennung eines Datenschutzbeauftragten zu schaffen, sollten bestimmte Auflagen z.B. im Rahmen der Informations- und Auskunftspflicht gem. Artikel 14 und 15, der Vorabge-

nehmigung gemäß Artikel 34 oder der umfangreichen Dokumentationspflichten gemäß Artikel 28 entfallen, wenn ein Datenschutzbeauftragter bestellt wird.

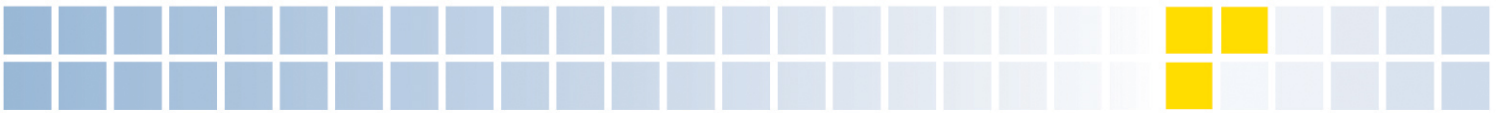
#### **Artikel 26 Absatz 5, Artikel 43, 44 - Konzerninterner Datentransfer**

Regelungsgehalt: Artikel 26 Absatz 5 sieht vor, dass die EU-Kommission in Zukunft vereinfachende Regelungen zur Verarbeitung personenbezogener Daten zu Kontroll- und Berichterstattungszwecken im Konzern treffen kann. Darüber hinaus wird in Artikel 43 geregelt, dass verbindliche Unternehmensvorschriften von der Aufsichtsbehörde in Zusammenarbeit mit EU-Kommission und Europäischem Datenschutzausschuss genehmigt werden können, die dann als geeignete Garantien bei der Datenübermittlung in Drittstaaten angesehen werden.

Bewertung: Für Konzernunternehmen ist der Austausch von Daten unverzichtbar. Hierzu ist eine rechtssichere Grundlage erforderlich. Deshalb geht der Ansatz des Verordnungsentwurfs, den konzerninternen Datentransfer zu erleichtern, in die richtige Richtung. Gleichwohl lässt die EU-Kommission bislang die Chance ungenutzt, eine Regelung zum konzerninternen Datentransfer zu schaffen, die diese Rechtssicherheit sowohl beim Datentransfer innerhalb als auch außerhalb der EU gewährleistet. Die mit der Verordnung vorgesehenen neuen Datenschutzregelungen müssen genutzt werden, um diese Lücke zu schließen.

Das in Artikel 43, 58 beschriebene Verfahren zur Genehmigung verbindlicher unternehmensinterner Vorschriften zum Datentransfer in Drittstaaten ist unnötig komplex und zeitintensiv. Die Einbindung von EU-Kommission und Europäischem Datenschutzausschuss durch die Aufsichtsbehörde erscheint angesichts der bestehenden Erfahrungen der Aufsichtsbehörden mit der Genehmigung verbindlicher Unternehmensrichtlinien nicht





erforderlich. Die in Artikel 51 festgelegte Zuständigkeit der Aufsichtsbehörde für das Hoheitsgebiet ihres Mitgliedstaates sollte bei der Genehmigung von verbindlichen unternehmensinternen Vorschriften nicht untergraben werden. Zudem führt die Ermächtigung der EU-Kommission zum Erlass delegierter Rechtsakte in Bezug auf Kriterien und Anforderungen für verbindliche unternehmensinterne Vorschriften und die Kriterien für ihre Genehmigung dazu, dass heute noch unbekannte Aspekte in das Verfahren einfließen können. Nachdem die Genehmigung unternehmensinterner Vorschriften ein Kernaspekt beim konzerninternen Datentransfer ist, sollte dieser Bereich von der Möglichkeit delegierter Rechtsakte ausgenommen werden.

Die in Artikel 44 Absatz 1h vorgesehene Übermittlung von Daten zur Verwirklichung des berechtigten Interesses greift zu kurz, um diese Regelung als Grundlage für den Datenaustausch zwischen Konzernunternehmen in einem Drittland heranziehen zu können. Eine solche Übermittlung ist nur dann möglich, wenn sie nicht als häufig oder massiv bezeichnet werden kann. Bei der konzerninternen Bündelung von Aufgaben ist es jedoch zwangsläufig, dass es zu einem häufigen Datenaustausch kommt. Deshalb sollte diese unnötige Beschränkung aufgehoben werden.

#### **Artikel 51 – Zuständigkeit der Aufsichtsbehörde**

Regelungsgehalt: Die Aufsichtsbehörde am Ort der Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters ist für seine Verarbeitungstätigkeit in allen EU-Mitgliedstaaten zuständig.

Bewertung: Der Grundgedanke, dass für ein Unternehmen nur noch eine Aufsichtsbehörde zuständig sein soll, ist zu begrüßen. Dieses Prinzip sollte für alle überregional tätigen

Unternehmen gelten, und zwar unabhängig davon, ob sie innerhalb eines Mitgliedstaates, innerhalb der EU oder mit Drittstaatenbezug agieren.

#### **Artikel 73 ff. - Rechtsbehelfe**

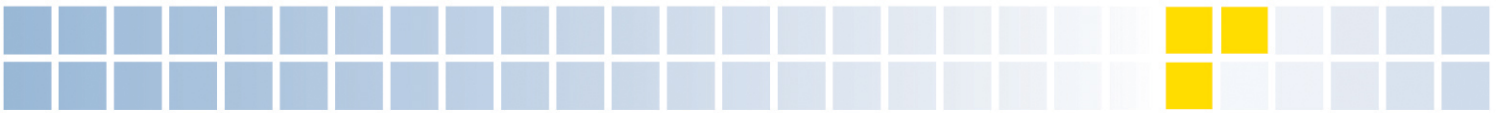
Regelungsgehalt: Nicht nur betroffene Personen, sondern auch Einrichtungen, Organisationen und Verbände, die sich den Schutz personenbezogener Daten zum Ziel gesetzt haben, sollen durch die Verordnung umfangreiche Beschwerderechte erlangen sowie die Möglichkeit, Entscheidungen der Aufsichtsbehörde im Namen der betroffenen Person oder mehrerer betroffener Personen gerichtlich überprüfen zu lassen.

Bewertung: Die Einführung eines unechten Verbandsklagerechts wird den unterschiedlichen Rechtstraditionen in Europa nicht ausreichend gerecht. Es besteht auch keine Notwendigkeit für ein solches Instrument, da sich jeder Betroffene und auch jede Interessensorganisation bereits an die Aufsichtsbehörde wenden kann und deshalb ein ausreichender Schutz vorhanden ist.

Die Regelung, dass z.B. Organisationen auch Entscheidungen der Aufsichtsbehörde im Namen mehrerer betroffener Personen gerichtlich geltend machen können, läuft auf die Einführung einer Sammelklage hinaus. Ein solches Instrument führt zu Friktionen mit dem System des in Kontinentaleuropa, u.a. in Deutschland verorteten Prinzips des individuellen Rechtsschutzes, das Ausfluss des Persönlichkeitsrechts ist. Betroffene sind durch die Möglichkeit einer Streitgenossenschaft (§§ 59 ff. ZPO) sowie einer Prozessverbindung nach § 147 ZPO ausreichend geschützt.

#### **Artikel 78, 79 - Sanktionen**

Regelungsgehalt: Die Aufsichtsbehörde kann gemäß Artikel 79 Sanktionen festlegen, die wirksam, verhältnismäßig und abschreckend



sein sollen. Die Höhe der Geldbuße wird an den weltweiten Jahresumsatz des Unternehmens gekoppelt und soll bis zu 2 % desselben betragen. Die EU-Kommission kann diese Beträge aktualisieren.

**Bewertung:** Die von der EU-Kommission vorgeschlagenen Sanktionen von bis zu 2% des weltweiten Jahresumsatzes stellen eine deutliche Verschärfung gegenüber dem derzeit gültigen Sanktionsregime dar. Die EU-Kommission verliert bei der Festsetzung der Höhe eines Bußgeldes den von ihr selbst aufgestellten Verhältnismäßigkeitsgrundsatz völlig aus den Augen, indem die Sanktion im Verhältnis zum Verstoß nicht mehr zu rechtfertigende Dimensionen erreichen kann. Sie übersieht, dass der Geschäftszweck der meisten Unternehmen nicht die Verarbeitung von Daten ist. Er ist im Beschäftigungsverhältnis vielmehr ein reiner Nebenzweck.

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%) 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 in 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.

Auch über die Höhe der Sanktionen als solche und die Anknüpfung an die bloße weltweite Jahresumsatzzahl muss diskutiert werden. Denn auch im EU-Wettbewerbsrecht, dessen Sanktionsregime offensichtlich zum Vorbild genommen wurde, wird dieses Kriterium zunehmend kritisiert.

### **Artikel 82 – Datenverarbeitung im Beschäftigungskontext**

**Regelungsgehalt:** Die Mitgliedstaaten können in den Grenzen der Verordnung den Beschäftigtendatenschutz u.a. für Zwecke der Einstellung, Erfüllung und Beendigung des Beschäftigungsverhältnisses regeln.

**Bewertung:** Wenn sich die Union dazu entscheidet, den Datenschutz in einer Verordnung zu regeln, sollte auch der Arbeitnehmerschutz Teil dieser Verordnung werden. Nur wenn es nicht gelingt, Kollektivvereinbarungen des Arbeitsrechts, die Einwilligung und andere Elemente einheitlich durch die Verordnung festzulegen, bedarf es einer Öffnungsklausel für das Arbeitsrecht. Diese muss die Gegebenheiten des Arbeitsrechts so berücksichtigen, dass sie weitere Handlungsmöglichkeiten für die Parteien des Arbeitsverhältnisses vorsieht.

### **Ansprechpartner:**

#### **BDA | DIE ARBEITGEBER**

Bundesvereinigung der Deutschen Arbeitgeberverbände

#### **Arbeitsrecht**

T +49 30 2033-1200

arbeitsrecht@arbeitgeber.de