

Stellungnahme

**zum Entwurf eines Gesetzes zur Regelung
des Beschäftigtendatenschutz der
Bundesregierung vom 24.08.2010**

I. Allgemeine Vorbemerkungen

Der Gesetzentwurf soll Rechtssicherheit und klare Regelungen für Arbeitgeber und Beschäftigte schaffen.

Praxiskonkretisierungen

Der Gesetzgeber hat nicht die Form einer Generalklausel gewählt, sondern viele konkrete Sachverhalte normiert.

Die Konkretisierung hat zur Folge, dass der Gesetzgeber nur klare Regelungen schaffen kann, die im Zeitpunkt der Gesetzgebung gängige Praxis sind. Gerade in der Arbeitswelt ändert sich die Personalpolitik ständig ([http://web.fh-ludwigshafen.de/rump/home.nsf/Files/C258826C25A574A7C12571B700245A48/\\$FILE/Wandel%20in%20der%20Personalpolitik.pdf](http://web.fh-ludwigshafen.de/rump/home.nsf/Files/C258826C25A574A7C12571B700245A48/$FILE/Wandel%20in%20der%20Personalpolitik.pdf).)

- Ökonomische Trends
- gesellschaftliche Trends
- demografische Entwicklung und
- aktuelle Trends auf dem Arbeitsmarkt

beeinflussen die Personalpolitik.

Darüber hinaus entwickelt sich nicht nur die Technik, sondern auch die Nutzung der neuen Medien ständig und in hohem Tempo weiter. Eine zu starke Konkretisierung birgt die Gefahr, dass Dinge geregelt werden, die schon in wenigen Monaten durch neue Techniken und Prozesse ersetzt werden, zu denen dann jedoch keine Regelung getroffen wurde. Es ist unmöglich, alle künftig denkbaren Sachverhalte zu antizipieren, die unter die Normen fallen sollen.

Sinnvoller Weise wäre die Normierung von Generalklauseln mit konkretisierenden Spezialtatbeständen. So kann wandelnden Wertmaßstäben, Anschauungen und technischen Veränderungen Rechnung getragen werden.

Einwilligung

Im Entwurf wird häufig die Einwilligung des Beschäftigten verlangt.

Es ist zu beachten, dass die Einwilligungserklärung keine rechtliche Bindung entfaltet, wenn sie der Betroffene nicht „freiwillig“ getroffen hat, insbesondere wenn er sie nur aufgrund einer wirtschaftlichen Machtposition des Gegenübers abgegeben hat. Ein solches Machtgefüge liegt im Arbeitsleben in der Regel vor.

Die Einwilligung darf daher im Arbeitsleben nur sehr zurückhaltend verwandt werden (vgl. auch Aufsichtsbehörde Baden-Württemberg, Hinweis zum BDSG Nr. 34, Staatsanzeiger Nr. 1 vom 02.01.1996, vgl. auch Gola/Schomerus, Komm. zum BDSG, 10. Aufl. § 4a Rn 7). Vielmehr muss der Schwerpunkt zum Schutz der Betroffenen von der Einwilligung auf Vorschriften, die eine Interessenabwägung und insbesondere den

Erforderlichkeitsgrundsatz enthalten, verlagert werden. Denn fast jeder Beschäftigte (gerade auch Bewerber) unterschreiben in der Regel alles, um den Arbeitsplatz zu bekommen oder nicht zu verlieren.

Konzerndatenschutz

Weiter fehlen praktikable und eindeutige Regelungen zum Umgang mit Beschäftigtendaten innerhalb von nationalen und internationalen Konzernen, bzw. beim Zusammenschluss von Unternehmen. Hierzu hat bereits der *Bundesrat* Stellung genommen, in dem die Bundesregierung aufgefordert wird, zeitnah einen weiteren Gesetzentwurf einzubringen; unseres Erachtens ist dies zu spät.

Insbesondere die Anforderungen an ein konzernweites Human Resources Programm sind zu normieren, da es heute bereits in Unternehmen mit Mutter- oder Schwestergesellschaften im Ausland (und insbesondere auch in Staaten außerhalb des Europäischen Wirtschaftsraumes) gängige Praxis ist, die Fähigkeiten und Entwicklungsmöglichkeiten von Mitarbeitern unternehmensübergreifend zu betrachten.

Vollkontrolle

Der Gesetzentwurf enthält keine ausdrückliche Regelung zum Ausschluss einer Vollkontrolle von Beschäftigten (ununterbrochene Verhaltens- oder Leistungskontrolle). Eine Vollkontrolle kann dabei eine optische Kontrolle durch eine Videoüberwachung darstellen, in dem der Betroffene die gesamte Zeit seiner Tätigkeit gefilmt wird, z.B. im Kassenbereich. Eine Vollkontrolle kann aber auch dann entstehen, wenn Auswertungen ein Gesamtbild vom Beschäftigten ermöglichen (z.B. Auswertung aller Außendienstprotokolle, aller Eingabeprotokolle in Computersysteme).

Eine Vollkontrolle stellt im Arbeitsleben einen unverhältnismäßigen Eingriff dar, da der Beschäftigte keine Möglichkeit erhält, selbstbestimmt zu agieren.

Datensicherheit

Es fehlt (trotz aller Konkretisierung) eine Normierung der Datensicherheit von Beschäftigtendaten. Die Datensicherheit muss der Sensibilität und der Fülle der Daten genügen.

Insbesondere bei der Übermittlung von personenbezogenen Daten von Beschäftigten an Dritte oder Auftragnehmer im Sinne des § 11 BDSG ist besonderes Augenmerk auf die Sicherheit zu legen, z.B. Pflicht zur Verschlüsselung von Emails.

Compliance

Datenschutz wird im Beschäftigtengesetz, bzw. in der Begründung als „Gegenüber“ zu Compliance-Aktivitäten von Unternehmen dargestellt, dies stimmt nicht mit der Praxis von Unternehmen überein; in vielen Unternehmen ist Datenschutz Teil der Compliance-Aktivitäten (<http://www.law-blog.de/445/compliance-und-datenschutz/>).

II. Stellungnahme zu den einzelnen Paragraphen

1. § 32 BDSG

§ 32 Abs. 6 BDSG normiert ein Verbot, Informationen über Bewerber aus privaten sozialen Netzwerken wie facebook, zu sammeln und für eine Bewerbung zu nutzen. Daten aus sozialen Netzwerken wie xing sollen dagegen genutzt werden dürfen. Hier stellt sich in der Praxis leider ein großes Abgrenzungsproblem, da auch „rein“ soziale Netzwerke für berufliche Zwecke genutzt werden.

Zudem funktionieren soziale (auch gerade geschäftliche) Netzwerke über Kontakte. Wie diese „Kontakte“ genutzt und ausgewertet werden dürfen, und ob, darüber schweigt sich der Entwurf aus. Denn mit wem und mit wie vielen Personen man in Kontakt steht, lässt Aussagen über die berufliche Qualität und den Nutzen für einen Arbeitgeber zu.

Es bleibt die Frage, ob ein Verbot sinnvoll ist oder ob nicht alleine auf die Erforderlichkeit für die Begründung des Beschäftigungsverhältnisses abgestellt werden sollte.

Im Falle eines Verstoßes gegen den Erforderlichkeitsgrundsatz böte sich eine analoge Anwendung des § 21 AGG an.

2. § 32a BDSG

a. Bewerberbeurteilungen

Hier fehlt leider eine klare Regelung zu den in der Praxis immer häufiger vorkommenden „psychologischen“ Bewerber-Beurteilungen, die teilweise online durch Anbieter außerhalb des Europäischen Wirtschaftsraumes angeboten werden. Ziel der Unternehmen ist es, schon vor der Einladung zu einem Vorstellungsgespräch ein möglichst umfassendes so genanntes Persönlichkeitsprofil zu erstellen, bzw. erstellen zu lassen. Das Persönlichkeitsprofil teilt sich in die drei Kategorien Typ, Beruf und Liebe. Besonders erwähnenswert sind die persönlichen Eigenschaften, die im Bewerbungsgespräch nahezu immer erfragt werden – sowohl positive als auch negative.

In den Fragebögen zu den Persönlichkeitsprofilen sind Fragen enthalten, die Aussagen zu Vorlieben, Verhalten etc. beinhalten; u.a. Fragen wie

- „Ich habe noch niemals gelogen.“;
- „Ich lasse mich oft durch andere beeinflussen.“
- „Es fällt mir leicht, neue Kontakte zu schließen.“
- „Ich bin sehr souverän und selbstbewusst.“
- „Ich schlage meine Frau/meinen Mann.“
- „Vieles hängt davon ab, ob man Glück hat.“

§ 32a Abs. 2 BDSG regelt nur die Anforderungen an so genannte Eignungstest, die die Geeignetheit für die berufliche Tätigkeit abprüfen; die Bewerberbeurteilungen gehen aber darüber hinaus, da sie die persönliche Geeignetheit abprüfen und eben den Bewerber bis in seine Intimsphäre bewerten.

b. ärztliche Untersuchungen

Es fehlt eine ausdrückliche Normierung, dass allgemein bei Bewerbungen nur solche Fragen hinsichtlich der Gesundheit erlaubt sind, die die berufliche Tätigkeit dauerhaft unmöglich machen. Der Arbeitgeber muss es hinnehmen, wenn, gegebenenfalls auch mit vorhersehbaren, gelegentlichen aber zumutbaren Fehlzeiten zu rechnen sein wird. In der Vergangenheit hat das BAG eine Frage nach einer möglichen Schwangerschaft als unzulässig angesehen, es sei denn, wenn sie objektiv dem gesundheitlichen Schutz der Bewerberin und des ungeborenen Kindes diene, bspw. bei der Einstellung einer Röntgenassistentin. Von dieser Rechtsprechung ist das BAG abgewichen, denn die Frage nach der Schwangerschaft sei im Vorstellungsgespräch bei einem anvisierten unbefristeten Anstellungsverhältnis prinzipiell tabu, unabhängig von einem möglichen Beschäftigungshindernis (*Entscheidung vom 06.02.2003 (2 AZR 621/01)*).

Einige Arbeitgeber gehen dazu über, DNA- oder Genom-Analysen von den Bewerbern zu fordern, um eine langfristige Geeignetheit des Bewerbers für dessen zukünftigen Arbeitsplatz zu prüfen. Hier ist ein Verweis auf § 19 GenDG notwendig.

Auch sei ein zukünftiger Arbeitnehmer nach einer Entscheidung des BAG (*Entscheidung vom 12.8.1999 = RDV 2000, 66f.*) regelmäßig nicht verpflichtet, Blutuntersuchungen zur Klärung, ob er alkohol- oder drogenabhängig ist, zuzustimmen, sofern es sich nicht um Tätigkeiten handelt, bei denen der Alkohol- oder Drogenkonsum eine Gefährdung darstelle, z.B. bei Kranfahrern oder Piloten. Es gehen aber immer mehr Unternehmen dazu über, Bewerber ganz allgemein auf Drogenkonsum zu testen (<http://www.derwesten.de/nachrichten/wirtschaft-und-finanzen/2009/6/16/news-122828332/detail.html>).

Hier steht die Einwilligungsmöglichkeit des Gesetzentwurfes im Widerspruch zur BAG-Rechtsprechung.

c. Eignungstest durch Dritte

Im Übrigen fehlt eine klare Regelung, ob Dritte, die Eignungstest außerhalb von Personen, die der ärztlichen Schweigepflicht unterfallen, durchführen, diese Eignungstests im Auftrag gemäß § 11 BDSG durchführen oder ob dies als Funktionsübertragung zu werten ist.

Unseres Erachtens ist diese externe Datenverarbeitung als Auftragsdatenverarbeitung zu werten, da der Arbeitgeber den „Zweck“, nämlich die Feststellung, ob der Bewerber geeignet ist oder nicht, vorgibt (*Abgrenzung gemäß Stellungnahme der Datenschutzgruppe der Europäischen Union 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter, angenommen am 16. Februar 2010*).

3. § 32b BDSG

Da § 32b Abs. 3 BDSG regelt die Löschungspflicht von Bewerberdaten nach dem Prinzip des Zweckwegfalls. Hier sollte alternativ dazu eine starre Frist gesetzt werden, und zwar in Anlehnung an die Praxis der so genannten Bewerberpools von maximal 24 Monaten nach Ablehnung. Unternehmen gehen immer mehr dazu über, Bewerber in Bewerberpools zu speichern, um für mögliche spätere Tätigkeiten auf diesen Pool zurückgreifen zu können.

Die Verwendung der Beschäftigtendaten in den Bewerberpools von der Einwilligung abhängig zu machen, ist -ungeachtet unserer Vorbemerkungen- keine praktikable Lösung. Insbesondere bei Initiativbewerbungen, kann der Arbeitgeber nur im Nachgang eine Einwilligung einholen, was beide Seiten als administrativen Aufwand verstehen. Sinnvoller wäre hier eine transparente opt-out-Lösung. Der Bewerber wird darüber informiert, dass seine Daten für maximal 24 Monate gespeichert werden, sofern er nicht ausdrücklich Widerspruch erhebt. Dies benachteiligt den Betroffenen auch nicht unangemessen, da er bspw. bei Initiativbewerbungen gerade selber aktiv seine Bewerbung kundgetan hat.

4. § 32c / § 32d BDSG

a. Leistungsprofile

Der Gesetzentwurf schweigt sich zu den allgemeinen Anforderungen an Leistungs-, bzw. Verhaltensprofilen von Beschäftigten aus. § 32c Abs. 1 S. 2 Ziffer 3 BDSG normiert nur die Möglichkeit der Datenerhebung, vorbehaltlich der §§ 32e bis 32i. Leistungskontrollen werden aber nicht nur aus Daten erstellt, die unter §§ 32e bis 32i fallen. Zu den Auswertungen, die eine Leistungskontrolle ermöglichen, gehören Handy- und Tankabrechnungen sowie Firmen-Kreditkartenabrechnungen, Außendienstprotokolle, Spesenabrechnungen, Eingabeprotokolle in Computersysteme, etc.

§ 32d macht die Verarbeitung und Nutzung vom Erforderlichkeitsgrundsatz und vom Verhältnismäßigkeitsprinzip abhängig. Es fehlen Anforderungen an Transparenz, Ausschluss einer Vollkontrolle, Methodik der Leistungskontrollen und Anforderungen an ein Zugriffs- und Berechtigungskonzept.

b. Krankenrückkehrergespräche

Ebenfalls nicht erwähnt werden im Entwurf die so genannten Krankenrückkehrergespräche, die gängige Praxis in Unternehmen sind. Diese Gespräche finden regelmäßig nicht nur im Rahmen der betrieblichen Wiedereingliederung statt, sondern häufig schon bei sich häufenden Fehltagen, um vom Arbeitnehmer die Gründe für sein Fehlen zu erfahren und gegebenenfalls auch die Belastbarkeit dieser Gründe zu überprüfen. Diese Gespräche sind nur unter Beachtung des Persönlichkeitsrechts unter Abwägung der betroffenen Interessen im Einzelfall zulässig. Führt der Arbeitgeber solche Gespräche, begründet dies keine erweiterte Auskunft- oder Mitteilungspflicht des Arbeitnehmers. Allerdings ist er zur Teilnahme an Krankengesprächen grundsätzlich kraft seiner Verpflichtung zur Aufrechterhaltung der betrieblichen Ordnung verpflichtet.

An die Durchführung und Dokumentation solcher Gespräche sind gesteigerte Sorgfaltsanforderungen zu stellen. Alleine zulässig in diesem Kontext kann es sein, wenn der Vorgesetzte des Arbeitnehmers als Vertreter des Arbeitgebers das Gespräch führt und nicht, wie häufig der Fall, zwei bis drei Vertreter unterschiedlicher hierarchischer Ebenen. Ein Abfragen im Sinne einer Fragebogensituation verbietet sich von selbst. Ziel dieses Gesprächs muss die Ergründung der für zu hoch erachteten Fehlzeiten sein. So kann zum Beispiel die Frage im Vordergrund stehen, ob es betriebsbedingte Gründe für die Fehlzeiten wie etwa Mobbing oder sexuelle Belästigung gibt. In keinem Fall zulässig ist die Aufforderung des Arbeitgebers, der Arbeitnehmer solle seinen Arzt (oder den Betriebsarzt) von dessen Schweigepflicht entbinden, um sich so ein detaillierteres Bild von den Ursachen der Krankschreibungen machen zu können.

Zu bedenken hat der Arbeitgeber stets auch die negative Ausstrahlung, die dem befragten Arbeitnehmer durch ein solches Gespräch möglicherweise gegenüber seinen Kollegen anhaften kann. Daher muss nicht nur über den Inhalt des Gesprächs Stillschweigen bewahrt werden, sondern auch schon über das Stattfinden an sich. Als Alternative sind transparente und vereinbarte Prozesse denkbar, die nach einer bestimmten Anzahl von Krankmeldungen grundsätzlich ein Krankengespräch vorsehen.

5. § 32e BDSG

Bei § 32e BDSG fehlt völlig die vom BAG geforderte Transparenz.

Zu der Frage der Überwachung, bzw. Kontrolle von Mitarbeitern hat das BAG am 26.08.2008 Aktenzeichen 1 ABR 16/07 eine heimliche Kontrolle ohne entsprechenden Anlass für unzulässig erklärt:

"Für die Schwere des Eingriffs ist insbesondere von Bedeutung, wie viele Personen wie intensiv den Beeinträchtigungen ausgesetzt sind. Das Gewicht der Beeinträchtigung hängt u.a. davon ab, ob die Betroffenen als Personen anonym bleiben, welche Umstände und Inhalte der Kommunikation erfasst werden und welche Nachteile den Grundrechtsträgern aus der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden..."

Die Intensität der Beeinträchtigung hängt ferner maßgeblich von der Dauer und Art der Überwachungsmaßnahme ab... Von erheblicher Bedeutung ist, ob der Betroffene einen ihm zurechenbaren Anlass für die Datenerhebung geschaffen hat - etwa durch eine Rechtsverletzung - oder ob diese anlasslos erfolgt. Auch die "Persönlichkeitsrelevanz" der erfassten Informationen ist zu berücksichtigen. Die Heimlichkeit einer in Grundrechte eingreifenden Ermittlungsmaßnahme erhöht das Gewicht der Freiheitsbeeinträchtigung. Den Betroffenen kann hierdurch vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erschwert werden...."

Das BAG schließt letztlich keine heimliche Überwachung aus, es schließt aber aus, dass der Beschäftigte über diese Möglichkeit des Arbeitgebers nicht vorher entsprechend informiert wird.

6. § 32f BDSG

a. Abs. 1

In § 32f BDSG Abs. 1 S. 1 Ziffer 1 bis 7 stehen sich die Zwecke unauflösbar gegenüber; die Ziffern 1 – 3 und 5 – 7 stellen Arbeitgeberzwecke dar; Ziffer 4 steht allein im Interesse der Beschäftigten. Dieser Widerspruch ist aufzulösen; über Ziffer 4 könnte der Arbeitgeber eine Vollkontrolle rechtfertigen.

Es fehlt auch wieder ein Hinweis auf den Ausschluss einer Vollkontrolle. Gerade in Kassenbereichen stehen die Beschäftigten unter einer ununterbrochenen Überwachung; eine Vollkontrolle könnte bspw. technisch durch so genannte Schwenk-Kameras verhindert werden, deren Schwenks optisch für die Betroffenen nicht nachvollziehbar sind, aber eben keine ununterbrochene Überwachung darstellen.

b. Abs. 2

In Abs. 2 sollte der Gesetzgeber normieren, ob der Aufenthaltsraum überwacht werden darf oder nicht. Für Sanitär-, Umkleide- oder Schlafräume ist dies ohnehin aufgrund der tragenden Prinzipien des Datenschutzes ausgeschlossen.

7. § 32g BDSG

§ 32g Abs. 2 BDSG geht an einem effektiven Fuhrparkmanagement völlig vorbei. Systeme zur Fahrzeugortung sind gerade darauf ausgerichtet, das Fahrverhalten zu analysieren. In der Regel kann man

- genauen Fahrzeugstandort
- exakte Fahrzeitenübersicht einschließlich der Standzeiten mit Datums- und Zeitangaben
- Ermittlung der Fahrzeugnutzung sowie aller Umwege
- Statistiken über die Fahrweise in Bezug auf den Verbrauch
- Tages-, Wochen- und Monatsübersichten aller gefahrenen Strecken in Kilometer

ermitteln, um den Fuhrpark und die Kosten zu optimieren. Der Zweck der Optimierung des Fuhrparks müsste entsprechend im Gesetz Berücksichtigung finden, natürlich unter Abwägung der Interessen der Beschäftigten.

8. § 32i BDSG

a. § 31 BDSG

Es fehlt eine Klarstellung, wie sich § 31 BDSG zu § 32i Abs. 1 S. 1 Ziffer 2 und 3 BDSG verhält.

b. Private Nutzung von Telekommunikationseinrichtungen

In § 32i BDSG fehlt eine eindeutige Regelung zur privaten Nutzung von Telekommunikationseinrichtungen. Ein Verbot der privaten Nutzung (dies ist der Umkehrschluss zu § 32i) ist in Unternehmen in der Regel nicht durchsetzbar, insbesondere dann nicht, wenn es sich um mobile Geräte handelt, die die Beschäftigten auch mit auf Dienstreisen nehmen wie Handys. Auf der anderen Seite können die Vorschriften zum Telekommunikationsgeheimnis, u. ä. in der Regel nicht effektiv umgesetzt werden (da ein Arbeitgeber kein Telekommunikations-Provider ist), so dass den Beschäftigten eine Vertraulichkeit vorgespielt wird, die es nicht gibt.

Das *BVerfG* hat bereits 2006 (*vom 02.03.2006 – 2 BvR 2099/04*) und 2007 entschieden, dass der Geheimnisschutz nur für die laufende Telekommunikation gelte, archivierte Emails also nicht vor dem Einblick durch den Arbeitgeber durch das Telekommunikationsrecht geschützt werden, denn zu diesem Zeitpunkt sei der Telekommunikationsvorgang bereits abgeschlossen, sondern alleine durch das informationelle Selbstbestimmungsrecht.

Pragmatisch wäre also eine Regelung im Beschäftigtendatenschutz, die eindeutig benennt, dass eine nicht dienstliche Nutzung der Telekommunikationseinrichtung im sozialüblichen Rahmen und außerhalb der Arbeitszeit zulässig ist, der Arbeitgeber aber Anweisungen hinsichtlich Internet- und Emailnutzung, etc. erlassen darf, insbesondere auch zum Sachverhalt, was er bei nicht nur vorübergehender Abwesenheit eines Mitarbeiters tun darf (Zugriff z.B. auf offensichtlich betriebliche Emails).

Hinzu kommt in § 32i BDSG wiederum die schwierige Abgrenzung zwischen privater und geschäftlicher Nutzung. Sofern die private Nutzung untersagt ist, ist der Arbeitgeber auch verpflichtet, die Einhaltung des Verbotes zu kontrollieren. Dabei stehen Unternehmen dann regelmäßig vor den Schwierigkeiten, ob beispielsweise das Prüfen, wann der Nahverkehrszug zu Zeiten der Tarifaueinandersetzungen fährt, bereits eine private oder noch geschäftliche Nutzung ist.

9. § 32I BDSG

In § 32I Abs. 1 BDSG ist die Beschränkung der Einwilligungsmöglichkeit auf den Unterabschnitt der Paragraphen des Gesetzentwurfes und in Abs. 3 die Unberührtheit der Rechte der Interessenvertretungen normiert.

Hier fehlt eine Klarstellung, welche Auswirkungen eine Betriebsvereinbarung auf die Anforderung der Einwilligung eines Beschäftigten hat, ggf. ob die Einwilligung durch eine Betriebsvereinbarung ersetzt werden kann.

Zu den Verfassern:

Stephanie Iraschko-Luscher ist Rechtsanwältin mit dem Tätigkeitsschwerpunkt Datenschutzrecht. Auch außerhalb des Datenschutzes verfügt sie über mehrjährige Erfahrungen in der Beratung von Unternehmen zu verschiedenen juristischen Themen. Zudem ist sie stellvertretende Arbeitskreisvorsitzende des Arbeitskreises Datenschutz des Bundesverbandes Credit Management (BvCM).

Pia Kiekenbeck ist Unternehmensberaterin im Bereich Projekt- und Prozessmanagement. Als Beraterin und Trainerin verfügt sie über umfassende Erfahrungen in den Bereichen Unternehmensanalyse und Kommunikation.

Beide sind Geschäftsführerinnen der **MGDS Managementgesellschaft für Datenschutz** in Hamburg, eine Unternehmensberatung für Datenschutz.

MGDS hat die Datenschutzberatung im Gegensatz zu vielen Mitbewerbern zu ihrer Hauptaufgabe gemacht. Die MGDS Managementgesellschaft für Datenschutz wurde im Januar 2006 gegründet und berät seitdem eine Vielzahl von Unternehmen unterschiedlichster Branchen, vom mittelständischen Unternehmen bis hin zu weltweit operierenden Konzernen.

Zudem betreibt die **MGDS** eine Internetseite www.datenschutzskandale.de.

Pia Kiekenbeck ist Vorsitzende des liberalen Datenschutzforums in Hamburg.

Hamburg, 20. Mai 2011

MGDS Managementgesellschaft für Datenschutz

Baumeisterstr. 2

20099 Hamburg



Stephanie Iraschko-Luscher

**(Geschäftsführerin /
Rechtsanwältin)**



Pia Kiekenbeck

**(Geschäftsführerin /
Unternehmensberaterin)**