

# IT Ticker

## Themenübersicht:

- Vorwort
- Datenschutzbeauftragter
- Arbeitnehmerdatenschutz
- Datensicherheit
- Auftragsdatenverarbeitung
- Scoring und Auskunfteien
- Erhöhte Anforderungen an die Einwilligung
- Werbung mit eigenen Daten
- Werbung mit fremden Daten
- Informations- und Veröffentlichungspflichten bei Datenschutzverstößen
- Verschärfte Bußgeld- und Strafvorschriften
- Inkrafttreten und Übergangsvorschriften
- Handlungsbedarf

### Vorwort

Mit dieser Sonderausgabe des IT-Tickers wollen wir Sie über einige Schwerpunkte der beiden Reformen des übergreifend geltenden Bundesdatenschutzgesetzes (BDSG) in diesem Jahr informieren.

Die erste Reform behandelt das sogenannte „Scoring“ und die Tätigkeit von Auskunfteien. Sie wurde im Bundestag am 12.05.2009 beschlossen. Der zweiten Reform gingen Datenskandale und intensive Diskussionen über ihre Konsequenzen voraus, etwa die Abschaffung des „Listenprivilegs“. Dieses Gesetz hat der Bundestag am 03.07.2009 beschlossen. Es wurde vom Bundesrat am 10.07.2009 gebilligt. Nicht beschlossen wurde das geplante Datenschutzauditgesetz. Die Neuerungen gelten in weiten Teilen bereits ab dem **01.09.2009**.

Wir stellen Ihnen einige Schwerpunkte beider Reformen, die vielfältige Änderungen im BDSG bewirken, gemeinsam thematisch gegliedert dar.

### Datenschutzbeauftragter

Die Stellung des betrieblichen Datenschutzbeauftragten wird weiter gestärkt: Unternehmen, die sich mit der anonymisierten Übermittlung von Daten oder der Markt- oder Meinungsforschung befassen, benötigen nun unabhängig von der Zahl ihrer Mitarbeiter stets einen

Datenschutzbeauftragten (§ 4f Abs. 1 BDSG). Ein Datenschutzbeauftragter kann nur aus wichtigem Grund abberufen werden. Zusätzlich erhält er nun einen besonderen Kündigungsschutz für sein Arbeitsverhältnis (§ 4f Abs. 3 BDSG), das während seiner Amtszeit und für ein Jahr danach ebenfalls nur aus wichtigem Grund gekündigt werden kann – vergleichbar etwa einem Betriebsrat. Die für die Datenverarbeitung verantwortliche Stelle wird nun ausdrücklich verpflichtet, dem Datenschutzbeauftragten die Fort- und Weiterbildung zu ermöglichen sowie die Kosten dafür zu tragen. Die bisherigen Anforderungen (etwa an die Fachkunde des Datenschutzbeauftragten) gelten unverändert weiter.

Martin Schweinoch, München

### Arbeitnehmerdatenschutz

Neu ist eine spezielle Vorschrift (§ 32 BDSG) für sämtliche datenschutzrechtlich relevanten Maßnahmen im Arbeits- und Beschäftigungsverhältnis.

Für Zwecke eines Beschäftigungsverhältnisses dürfen personenbezogene Daten nur erhoben, verarbeitet oder genutzt werden, soweit dies für seine Anbahnung, Durchführung oder Beendigung erforderlich ist. Eine Erhebung, Nutzung oder Verarbeitung solcher Daten zur Aufdeckung von Straftaten ist (nur) zulässig, wenn ein dokumentierter Anhaltspunkt dafür vorliegt, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat.

Die Neuregelung ist in mehrfacher Hinsicht problematisch. So führt etwa das Erfordernis eines dokumentierten tatsächlichen Anhaltspunkts für eine Straftat des Betroffenen dazu, dass der Arbeitgeber nur dann rechtmäßig handelt, wenn er sich bereits auf einen dokumentierten Anfangsverdacht stützen kann. Davon sind auch Elemente der in vielen Unternehmen aufwendig eingeführten „Compliance“-Programme betroffen, die nicht nur Straftaten, sondern auch Ordnungswidrigkeiten verhindern sollen und ohne eine vorbeugende Kontrolle und die damit verbundene Nutzung personenbezogener Daten nicht funktionieren können.

Problematisch erscheint auch die Dokumentationspflicht der tatsächlichen Anhaltspunkte für einen konkreten Verdacht. Danach ist ein Arbeitgeber schon zum Beweis der eigenen Pflichterfüllung gehalten, die Dokumentation auch dann aufbewahren, wenn sich der Verdacht zerstreut

hat - also noch mehr Daten zu speichern als bisher. Nicht recht klar ist auch das Verhältnis der Dokumentationspflicht zu den unveränderten Löschungs- und Sperrpflichten (§ 35 BDSG).

Diese Neuregelungen für Beschäftigungsverhältnisse gelten auch für nicht-elektronische Daten. Zukünftig ist deshalb jede Erhebung, Verarbeitung oder Nutzung von Daten ohne Rücksicht auf die Form der Speicherung oder Übermittlung erfasst. Erfasst werden somit auch rein physische Vermerke. Trotz allgegenwärtiger IT wird damit der Anwendungsbereich des BDSG enorm ausgeweitet. So werden z.B. auch Datenerhebungen am Telefon (z.B. Anruf bei früherem Arbeitgeber eines Bewerbers), bei der Leistungs- und Verhaltenskontrolle (z.B. Beobachtung durch Kamera) und handgeschriebene Notizen über ein Bewerbungsgespräch erfasst.

Die Neuregelung soll einen ersten Schritt hin zu einem eigenen Arbeitnehmer-Datenschutzgesetz darstellen. Leider führt sie zu Unsicherheiten bei der Auslegung und lässt wichtige praktische Fragen unbeantwortet. Eines ist aber sicher: Im Arbeitsverhältnis gibt es keinen datenschutzfreien Raum - und darauf müssen sich die Unternehmen kurzfristig einstellen.

Udo Steger, München

### Datensicherheit

Die gesetzliche Zielvorgabe der Datenvermeidung und Datensparsamkeit wurde neu formuliert (§ 3a BDSG). Sie erfasst nun generell die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Nach wie vor gilt, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden sollen. Nunmehr sind allerdings personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck technisch möglich ist und keinen unverhältnismäßigen Aufwand erfordert. Unternehmen sollten deshalb genau prüfen, ob sie ihre Prozesse entsprechend anpassen müssen, etwa weil zu viele Daten gespeichert oder gespeicherte Daten nicht rechtzeitig pseudonymisiert oder anonymisiert werden.

Auch der neue § 30a BDSG enthält Regelungen zur Anonymisierung und Pseudonymisierung. Danach dürfen zu Markt- oder Meinungsforschungszwecken erhobene oder gespeicherte Daten nur für diesen Zweck verarbeitet oder genutzt werden. Daten aus nicht allgemein zugänglichen Quellen dürfen ausschließlich für das konkrete

Forschungsvorhaben verarbeitet oder genutzt werden, für das sie erhoben worden sind. Eine Verwendung für andere Zwecke ist nur anonymisiert zulässig, also wenn kein Personenbezug mehr hergestellt werden kann (§ 3 Abs. 6 Alt. 1 BDSG).

Es bestehen nun gestufte Pflichten: Personenbezogene Daten sind zu anonymisieren (§ 3 Abs. 6 BDSG), sobald dies der Zweck der Markt- oder Meinungsforschung ermöglicht. Bis dahin sind die Daten zu pseudonymisieren (§ 3 Abs. 6a BDSG), was bis auf wenige Ausnahmen nicht mehr aufgehoben werden darf. Verstöße gegen § 30a BDSG sind bußgeldbewehrt. Die betroffenen Unternehmen sollten ihre Prozesse kurzfristig anpassen und dies zu dokumentieren. In Verbindung mit der Pflicht zur Speicherung der Datenherkunft hat die Regelung besondere Brisanz: Verstöße können so besonders einfach nachgewiesen werden.

Eine Neuerung mit eher technischen Auswirkungen findet sich in der Anlage zu § 9 BDSG. Danach gehört eine Verschlüsselung der Daten nun „insbesondere“ zu den Maßnahmen, die zur Gewährleistung der Zugangs-, Zugriffs- und Weitergabekontrolle ergriffen werden müssen. Nach der verwendeten Formulierung „dem Stand der Technik entsprechend“ sollen fortschrittliche Verfahren einzusetzen seien, die sich in der Praxis bewährt haben und einen hohen Sicherheitsstandard gewährleisten. Praktisch dürften deshalb die meisten als sicher und leistungsfähig geltenden Verfahren anwendbar sein, die teilweise auch bereits in Betriebssystemen und Applikationen enthalten sind. Im Ergebnis sind Unternehmen stärker als bisher gehalten, jeden Datenspeicher zu verschlüsseln und Auftragsdatenverarbeiter entsprechend anzuweisen. Die Realität sieht bekanntlich oft anders aus. Auch hier besteht also Handlungsbedarf.

Udo Steger, München

### Auftragsdatenverarbeitung

Auch die Vorschriften für die Auftragsdatenverarbeitung (§ 11 BDSG) werden strenger: Für den schon bisher schriftlich zu erteilenden Auftrag werden nun Pflichtinhalte vorgeschrieben, die wesentliche Details für den Umgang mit personenbezogenen Daten abbilden müssen. Dazu gehören auch Umfang, Art und Zweck des Umgangs mit den Daten, die zu treffenden technischen und organisatorischen Maßnahmen, die Kontrollpflichten des Auftragnehmers und die Kontrollrechte des Auftraggebers sowie dessen Weisungsbefugnisse etc. Der Auftraggeber

wird nun auch verpflichtet, sich vor Beginn der Datenverarbeitung und anschließend regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen und die Ergebnisse dieser Prüfungen zu dokumentieren.

Damit will der Gesetzgeber zu detaillierten Festlegungen und ernsthaften Prüfungen verpflichten, da bisher in der Praxis nach seiner Auffassung erhebliche Defizite aufgetreten sind. Dieser Ansatz wird unterstrichen, indem eine nicht ordnungsgemäße Auftragserteilung und eine unterbliebene Vorab-Kontrolle des Auftragnehmers durch den Auftraggeber zukünftig Ordnungswidrigkeiten sind, die mit Bußgeld bis zu EUR 50.000,00 geahndet werden können (§ 43 Abs. 1 Nr. 2b BDSG).

Diese Regelungen gelten entsprechend für (Fern-)Wartungsarbeiten durch Dritte an IT-Systemen, bei denen – wie so häufig – ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (§ 11 Abs. 5 BDSG).

Die Vertragspartner einer Auftragsdatenverarbeitung müssen bis zum Inkrafttreten der Änderungen am 01.09.2009 dokumentiert für ordnungsgemäße Zustände nach den neuen Anforderungen sorgen.

Martin Schweinoch, München

### Scoring und Auskunftfeien

Datenschutzfragen bei Scoring und für die Übermittlung von Daten an und durch Auskunftfeien sind Gegenstand der ersten Reform des BDSG in diesem Jahr.

Zunächst wird definiert, wann von einer automatisierten Einzelentscheidung auszugehen ist (§ 6a BDSG). Dafür geltende Auflagen wurden erhöht: Auf Verlangen sind die wesentlichen Gründe für eine den Betroffenen belastende Entscheidung mitzuteilen und zu erläutern hat.

Besonders geregelt sind nun die nun Zulässigkeitsvoraussetzungen für Scoringverfahren (§ 28b BDSG). Für Entscheidungen über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen dürfen Wahrscheinlichkeitswerte für sein zukünftiges Verhalten nur erhoben oder verwendet werden, wenn die zu ihrer Berechnung genutzten Datenarten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Wahrscheinlichkeit dieses Verhaltens erheblich sind. Aus dem Wortlaut kann gefolgert werden, dass Scoringverfahren für Werbezwecke davon nicht erfasst sind. Es bleibt gleichwohl die Frage, ob diese völlig „unwissen-

schaftlich“ ausgestaltet werden können. Für die heftig umstrittenen Anschriftendaten gilt nun den Kompromiss, dass Scoringverfahren nicht ausschließlich auf Anschriftendaten beruhen dürfen. Bei der Nutzung von Anschriftendaten ist der Betroffene jedenfalls darüber (etwa in AGB) zu unterrichten. Gleichzeitig wurden die Auskunftsrechte des Betroffenen deutlich ausgeweitet. Die für die Entscheidung verantwortliche Stelle (z.B. Onlineshop) hat dem Betroffenen auf Verlangen über die in den sechs Monaten vor seinem Auskunftsverlangen erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte Auskunft zu erteilen (§ 34 Abs. 2 BDSG). Daneben sind die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar allgemeinverständlich mitzuteilen. Dies hat erhebliche Auswirkungen auf die Speicherprozesse und die Korrespondenz mit Betroffenen.

Neu definiert werden die Voraussetzungen für zulässige Meldungen an Auskunftfeien (§ 28a BDSG). Sie folgen für sog. Negativdaten im Wesentlichen den von der Rechtsprechung bereits entwickelten Regelbeispielen. Ebenfalls geregelt werden Voraussetzungen für die Übermittlung von Positivdaten. Unklar bleibt jedoch, für welche Positivdaten nach wie vor eine Einwilligung notwendig ist. Unabhängig davon hat das meldende Unternehmen seine Meldungen zu korrigieren, wobei auch hier Einzelheiten (Wesentlichkeit der Änderungen) unklar bleiben.

Auch das reformierte BDSG enthält keine Definition der „Auskunftfei“. Durch das Gesetz zur Umsetzung der Verbraucherkreditrichtlinie ist allerdings in § 29 Abs. 6 BDSG eine Beschreibung erfolgt. Zu beachten ist, dass auch konzerninterne Zahlungserfahrungsdatenbanken vom Begriff der Auskunftfei und damit vom geänderten BDSG erfasst sein können.

Dr. Wulf Kamlah, Frankfurt/M.

### Erhöhte Anforderungen an die Einwilligung

Die Verschärfung der formalen Anforderung an die Einwilligung durch den Betroffenen hat besondere Bedeutung für die Praxis. Dies betrifft sowohl Einwilligungen, die in Allgemeinen Geschäftsbedingungen erklärt werden, als auch die mündliche Datenerhebung.

Eine wirksame Einwilligung kann auch künftig nicht „versteckt“ in den Allgemeinen Geschäftsbedingungen erfolgen. Vielmehr ist eine ausdrückliche, drucktechnisch

hervorgehobene Gestaltung der Einwilligungserklärung erforderlich. Die Regelungen für die Einwilligung müssen sich deutlich von den anderen Regelungen abheben. Der Gesetzgeber setzt damit die Regelungen der Rechtsprechung des Bundesgerichtshofs aus dem letzten Jahr in das Datenschutzgesetz um (z.B. „Payback“-Urteil). Die anfänglich geforderte, weitere Verschärfung wurde jedoch nicht vorgenommen. Ein umständliches Verfahren ist für die mündliche Datenerhebung vorgesehen. Nachdem eine mündliche Einwilligung erfolgt ist, etwa im Gespräch mit einem Call-Center, muss das Unternehmen dem Betroffenen darüber anschließend eine schriftliche Bestätigung übermitteln. Dieser Medienbruch stellt Unternehmer vor eine besondere Herausforderung.

Für die Praxis bedeutet die Neuregelung, dass Unternehmen dringend die Gestaltung ihrer Allgemeinen Geschäftsbedingungen anpassen müssen, um Kundendaten auch künftig weitreichend verwenden zu können und Rechtsverstöße zu vermeiden.

Stefan C. Schicker, LL.M., München

#### Werbung mit eigenen Daten

Auch nach dem geänderten BDSG ist für die Eigenwerbung für Waren und Dienstleistungen, die vom Unternehmen selbst erbracht werden, gegenüber eigenen Kunden keine Einwilligung des Adressaten nötig, wenn die Daten durch das Unternehmen selbst erhoben wurden.

Interessanterweise gilt dies nach den geänderten Regelungen auch für fremde Werbung, die im Zusammenhang mit eigener Werbung steht, die zusammen mit dieser verteilt wird (Beipackwerbung). Vorgeschrieben ist nur, dass der Betroffene weiß, wer die verantwortliche Stelle ist, die ihm die Hauptwerbung zugeschickt hat. Weiterhin bleibt auch die Werbung im Hinblick auf die berufliche Tätigkeit des Empfängers an seine berufliche Adresse zulässig.

Stefan C. Schicker, LL.M., München

#### Werbung mit fremden Daten

Eines der umstrittensten Themen ist das „Listenprivileg“. Bislang dürfen bestimmte listenmäßig zusammengefasste Daten (Name, Titel, akademischer Grad, Anschrift, Geburtsjahr, Berufs-/Branchenbezeichnung, Zugehörigkeit zu einer bestimmten Personengruppe) ohne Einwilligung des Betroffenen für Werbezwecke verwendet und übermittelt werden. Dies wurde als Auslöser für viele Datenschutz-

skandale angesehen. So war es anfangs erklärtes Ziel des Gesetzgebungsverfahrens, das Listenprivileg ganz abzuschaffen. Das Listenprivileg blieb nun erhalten, wenn auch mit erheblichen Einschränkungen.

Zukünftig dürfen zusammengefasste personenbezogene Daten nur noch dann für Werbezwecke übermittelt und von dem Datenempfänger verwendet werden, wenn für den mit der Werbung Angesprochenen die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Es muss für den Betroffenen klar sein, woher seine Daten stammen bzw. wer diese Daten erhoben hat.

Damit verbunden ist die Pflicht der die Daten übermittelnden Stelle, die Herkunft der Daten und die Identität des Empfängers der Daten für zwei Jahre nach der Übermittlung zu speichern. Darüber hinaus muss sie dem Betroffenen auch Auskunft über die Herkunft der Daten und den Empfänger erteilen. Diese Speicher- und Auskunftspflichten treffen auch den Empfänger der Daten.

Sinn der Speicher- und Auskunftspflichten ist es vor allem, dem Betroffenen die Ausübung seines schon bisher bestehenden Widerspruchsrechts gegen die Datenverwendung zu erleichtern. Auch über das Widerspruchsrecht muss der Betroffene informiert werden. Damit kann er künftig um so leichter gegenüber der Stelle, die seine Daten erhoben hat, wie auch gegenüber dem Empfänger der Daten, seinen Widerspruch erklären und seine Daten damit für die Verwendung und Übermittlung für Werbezwecke sperren.

Diese Einschränkungen des Listenprivilegs haben gravierende Auswirkungen für Unternehmen, die mit Adressen handeln, aber auch deren Abnehmer, Unternehmen aus dem Internet- und Versandhandel sowie der Verlagsbranche. Sie alle müssen bei der Gewinnung von Neukundendaten schon ab dem 01.09.2009 genau darauf achten, die neuen Vorgaben einzuhalten, um nicht Bußgeld- oder sogar Straftatbestände zu verwirklichen.

Dr. Daniel Kaboth, München

#### Informations- und Veröffentlichungspflichten bei Datenschutzverstößen

Völlig neu sind bußgeldbewehrte Informationspflichten gegenüber der Aufsichtsbehörde und den Betroffenen bei Datenmissbrauch. Die Informationspflichten gelten, wenn besonders schutzwürdige Daten außerhalb des Unternehmens unrechtmäßig zur Kenntnis gelangen und Betroffenen dadurch schwerwiegende Beeinträchtigungen

von Rechten oder schutzwürdigen Interessen drohen (§ 42a BDSG).

Besonders schutzwürdige Daten sind dabei (a) Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualeben, (b) Berufsgeheimnissen unterliegende Daten, (c) Daten über (mögliche) strafbare Handlungen und Ordnungswidrigkeiten des Betroffenen sowie (d) Bank- und Kreditkartendaten. Wird einem Unternehmen etwa bekannt, dass Bank- und Kontodaten seiner Kunden unrechtmäßig in dritte Hände gelangt sind (z.B. durch Adresshandel), muss das Unternehmen die Datenschutzaufsicht und die Betroffenen informieren.

Es ist unverzüglich nach Kenntnis eines solchen Datenmissbrauchs zu informieren. Mit der Information der Betroffenen kann aber gewartet werden, bis angemessene Maßnahmen zur Datensicherung erfolgt sind und die Strafverfolgung nicht mehr gefährdet ist. Es sollen nicht breitere Kreise von Sicherheitslücken informiert oder Täter unnötig gewarnt werden. Erfordert die direkte Benachrichtigung der Betroffenen - etwa wegen ihrer Anzahl - unverhältnismäßigen Aufwand, muss das Unternehmen halbseitig in zwei bundesweiten Tageszeitungen oder durch gleichwertige Maßnahmen informieren.

Der Betroffene muss über die Art des Datenmissbrauchs und Empfehlungen zur Schadensabwendung informiert werden. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss mögliche nachteilige Folgen und ergriffene Schutzmaßnahmen des Unternehmens enthalten.

Zwar können solche Mitteilung in Straf- und Ordnungswidrigkeitsverfahren gegen Informationspflichtige nur eingeschränkt verwendet werden (§ 42a BDSG). Wesentlich bedeutender wird jedoch die negative Öffentlichkeitswirkung von Pflichtinformationen über Datenmissbrauch sein, wie jüngste Datenskandale zeigen.

Sabine Kröger, München

### **Verschärfte Bußgeld- und Strafvorschriften**

Die Bußgelder für Datenschutzverstöße werden deutlich erhöht. Zusätzlich sanktioniert das Gesetz jetzt weitere Pflichtverstöße. Bei leichteren Ordnungswidrigkeiten verdoppelt sich der Bußgeldrahmen von € 25.000,00 auf € 50.000,00.

Bei schweren Ordnungswidrigkeiten können nun bis zu € 300.000,00 verhängt werden. Diese Bußgeldrahmen

können auch überschritten werden: war der wirtschaftliche Vorteil des Täters aus der Ordnungswidrigkeit größer, kann ein höheres Bußgeld verhängt werden.

Es werden auch neue Bußgeldvorschriften geschaffen. Dies betrifft automatisierte Abrufverfahren (§ 10 BDSG), bei denen die speichernde Stelle zu gewährleisten hat, dass die Datenübermittlung zumindest durch geeignete Stichprobenverfahren überprüft werden kann.

Auch für die Auftragsdatenverarbeitung gelten neue Sanktionen. Werden die im Einzelnen festgelegten Anforderungen (§ 11 Abs. 2 Satz 2 BDSG) an die Auftragserteilung nicht erfüllt oder überzeugt sich der Auftraggeber nicht vorab von den technischen und organisatorischen Maßnahmen beim Auftragnehmer, liegt eine Ordnungswidrigkeit vor. Die Auftragserteilung sollten deshalb sehr sorgfältig abgefasst und die Vorbereitung des Auftrags dokumentiert werden. Ordnungswidrig ist es auch, für den Widerspruch des Betroffenen gegen die Datenverwendung für Werbung oder Markt- und Meinungsforschung strengere Formerfordernisse aufzustellen als für das Schuldverhältnis, durch das die Daten erlangt werden.

Verantwortliche Stellen, die Daten an Auskunftsteilnehmer übermitteln, müssen spätere Änderungen innerhalb eines Monats an die Auskunftsteilnehmer übermitteln. Auch der Verstoß dagegen ist eine Ordnungswidrigkeit. Das dürfte alle betreffen, die Meldungen über ihre Schuldner an Kreditauskunftsteilnehmer übermitteln.

Die Auskunftsrechte des Betroffenen werden gestärkt, denn ordnungswidrig ist es nun auch, wenn bestimmte Auskünfte nicht ordnungsgemäß erteilt werden oder gegen einige andere Pflichten im Zusammenhang damit verstoßen wird. Spätestens jetzt ist es Zeit, im Unternehmen klare Abläufe für Auskunftsverlangen von Betroffenen zu definieren.

Zu solchen neuen „leichteren“ Ordnungswidrigkeiten kommen auch neue Sanktionen mit bis zu € 300.000,00 Bußgeld. Dies gilt, wenn der Vertragsabschluss mit dem Betroffenen davon abhängig gemacht wird, dass er in die Nutzung seiner Daten zu Adresshandel oder Werbung einwilligt, obwohl er keinen anderen zumutbaren Zugang zu gleichwertigen Leistungen ohne diese Einwilligung hat. Die gleichen Sanktionen drohen, wenn personenbezogene Daten trotz Widerspruchs des Betroffenen für Werbung, Markt- oder Meinungsforschung verwendet werden.

Auch Pflichten zur Anonymisierung personenbezogener Daten sind von besonderer Bedeutung: Wird die Anonymisierung in bestimmten Fällen rückgängig

gemacht, indem ein bestimmtes Merkmal mit einer Einzelangabe zusammengeführt wird, stellt auch das eine schwere Ordnungswidrigkeit dar.

Dr. Oliver Bühr, Frankfurt/M.

### Inkrafttreten und Übergangsvorschriften

Viele Änderungen des BDSG treten schon am 01.09.2009 in Kraft, also in weniger als zwei Monaten.

Dafür gelten drei Ausnahmen: Die Regelungen zum Scoring und für Auskunftfeien (siehe oben zum „Scoring“) gelten ab dem 01.04.2010. Auch die Änderungen für Auskünfte an Betroffene mit den neuen Speicherpflichten treten am 01.04.2010 in Kraft. Der geänderte § 28 BDSG („Listenprivileg“) gilt zeitlich abgestuft: Ab dem 01.09.2009 gelten für neu erhobene oder gespeicherte Daten die Neuregelungen. Nur für „Altdaten“ gilt die bisherige Regelung noch für Markt- und Meinungsforschung bis zum 31.08.2010 sowie für Werbung bis zum 31.08.2012.

Es erscheint zwingend, bis zu diesen Zeitpunkten die notwendigen Mechanismen umzusetzen. Das gilt insbesondere für die erhöhten Anforderungen an die Einwilligung und deren Notwendigkeit, aber etwa auch für Dokumentationspflichten über die Herkunft von Daten, um zum Inkrafttreten der Neuregelungen den gesetzlichen Anforderungen zu entsprechen.

Ein vorausschauendes Datenmanagement ist notwendig. Die Umsetzung der Anforderungen sollten in keinem Fall auf die lange Bank geschoben werden.

Florian Hensel, München

### Handlungsbedarf

Wir können hier nur einen ersten Überblick für Kernpunkte der Neuregelungen geben.

Die kontroversen Diskussionen in der Gesetzgebung haben zu teilweise komplexen Vorschriften geführt, deren Auswirkungen an der konkreten Gestaltung im Einzelfall zu prüfen sind. Für viele der Neuerungen hat der Gesetzgeber keine lange Übergangsfrist eingeräumt, sie gelten in weiten Teilen bereits ab dem 01.09.2009.

Bis dahin müssen Unternehmen nicht nur bestehende Verfahren und Verträge auf ihre weitere Verwendbarkeit prüfen, sondern die notwendigen Änderungen auch praktisch umsetzen.

Für Fragen stehen wir gerne zur Verfügung.

Martin Schweinoch

### Practice Group IT, Internet und E-Business

Nikolaus Bertermann

Dr. Oliver Bühr

Thomas Eigen, LL.M.

Markus von Fuchs, LL.M.

Florian Hensel

Johann Heyde

Dr. Oliver Hornung

Dr. Daniel Kaboth

Dr. Wulf Kamlah

Sabine Kröger

Dr. Eberhard Kromer MBA

Dr. Karolin Nelles

Dr. Matthias Nordmann, M.A.

Dr. Andreas Peschel-Mehner

Dr. Ulrich Reber

Stefan C. Schicker, LL.M.

Prof. Dr. Mathias Schwarz

Martin Schweinoch

Udo Steger

Martin Stück

Dr. Johannes Thoma

Julian Westpfahl

Dr. Anne Zoll

### Impressum

#### SKW Schwarz

#### Rechtsanwälte Steuerberater Wirtschaftsprüfer Partnerschaft

Sitz der Partnerschaft ist München, eingetragen beim Amtsgericht München PR 884.

Vertretungsberechtigter: Prof. Dr. Mathias Schwarz, Redaktionell Verantwortlicher: Martin Schweinoch.

E-Mail: [IT@skwschwarz.de](mailto:IT@skwschwarz.de)

#### Standorte:

##### 10719 Berlin

Kurfürstendamm 38/39

T +49 (0) 30.889 26 50-0

F +49 (0) 30.889 26 50-10

##### 40212 Düsseldorf

Steinstraße 1/Kö

T +49 (0) 221.82 89 59-0

F +49 (0) 221.82 89 59-60

##### 20095 Hamburg

Spitalerstraße 4

T +49 (0) 40-33 40 10

F +49 (0) 40-33 40 15 21

##### 60598 Frankfurt/Main

Mörfelder Landstraße 117

T +49 (0) 69.63 00 01-0

F +49 (0) 69.63 55 22

##### 80333 München

Wittelsbacherplatz 1

T +49 (0) 89.286 40-0

F +49 (0) 89.280 94-32

Um den IT-Ticker abzubestellen, senden Sie uns bitte eine E-Mail oder informieren Sie Ihren Ansprechpartner in der Kanzlei. Gerne informieren wir Sie über unsere anderen Ticker und Newsletter.

Gesetzliche Berufsbezeichnung: Rechtsanwalt/-anwältin der BRD.

Zuständige Rechtsanwaltskammer: Rechtsanwaltskammern Berlin, Düsseldorf, Frankfurt a.M., Hamburg und München.

Die berufsrechtlichen Regelungen sind unter <http://www.brak.de> in der Rubrik „Berufsrecht“, Informationspflichten gem. § 5 TMG abrufbar.

© SKW Schwarz 2009