

# BDSG-Übergangsfrist endet am 23. Mai 2004

**Nun läuft sie also aus, die ›Gnadenfrist‹, die der deutsche Gesetzgeber den Unternehmen und anderen datenverarbeitenden Stellen eingeräumt hatte, ehe sie nun endlich das novellierte Datenschutzgesetz in die Praxis umsetzen müssen.**

**W**ERDEN BÜRGER-, Kunden-, Patienten-, Klienten-, Mandanten- oder auch Beschäftigtendaten verarbeitet, sind das Bundesdatenschutzgesetz (BDSG) oder auch die jeweiligen Landesdatenschutzgesetze einzuhalten. Im BDSG heißen die Unternehmen, Verwaltungen und Organisationen, die diese personenbezogenen Daten verarbeiten, ›verantwortliche Stelle‹. Diese verantwortlichen Stellen können Behörden des Bundes sein, Unternehmen in ihren unterschiedlichen Rechtsformen (z.B. GmbH, AG, OHG), eingetragene Vereine, aber auch Freiberufler, wie Rechtsanwälte oder Wirtschaftsprüfer. Für öffentliche Stellen (Behörden) der Länder gilt das jeweilige Landesdatenschutzgesetz.

## Übergangsfrist abgelaufen

DAS NOVELLIERTE BDSG ist in Kraft getreten am 23. Mai 2001 (siehe Schierbaum: ›Die erste Stufe der Modernisierung‹ in CF 7/01 ab Seite 24) – allerdings mit einer Übergangsfrist für alle ›laufenden Anwendungen‹. Das hieß: Alle Erhebungen, Verarbeitungen und Nutzungen personenbezogener Daten, die bereits

vor dem Inkrafttreten des novellierten BDSG in ›Anwendung‹ waren, hatten für die Umsetzung der neu hinzugekommenen Vorschriften noch eine ›Gnadenfrist‹ (§ 45 BDSG). Diese läuft jetzt, drei Jahre später, mit dem 23. Mai 2004 aus. Konkret heißt das: Bis zum 23. Mai 2004 müssen nun auch alle ›Alteinrichtungen‹ (= laufenden Anwendungen) mit den Vorgaben des BDSG endgültig in Übereinstimmung gebracht worden sein. Für alle nach dem 23. Mai 2001 erhobenen, verarbeiteten oder genutzten personenbezogenen Daten mussten die Vorschriften des novellierten BDSG ohnehin sofort angewandt werden.

Zur Erinnerung: Die Novellierung des BDSG erfolgte seinerzeit auf der Basis der im Oktober 1995 beschlossenen EG-Datenschutzrichtlinie, die bis spätestens zum 24. Oktober 1998 in deutsches Recht hätte umgesetzt sein müssen. Tatsächlich erfolgte dies aber erst durch die BDSG-Novellierung am 23. Mai 2001, also mit fast dreijähriger Verspätung. Dabei wurde die praktische Umsetzung des erweiterten Datenschutzrechts noch einmal verzögert durch die dreijährige Übergangsfrist, die den ›verantwortlichen Stellen‹ eingeräumt wurde. Eine solche Übergangsfrist war den Mitgliedsstaaten durch die EG-Datenschutzrichtlinie zwar grundsätzlich gestattet, führte nun aber dazu, dass die Verwirklichung

eines europa-einheitlichen Datenschutzstandards erst neun (!) Jahre nach Inkrafttreten der EG-Richtlinie und sechs Jahre nach deren eigentlich vorgesehener Umsetzung erreicht wird. Ob eine so verzögerte Umsetzung der Richtlinie mit den Vorgaben der EG-Richtlinie überhaupt vereinbar ist, muss in Frage gestellt werden...<sup>1</sup>.

## Neue Pflichten ab dem 23. Mai 2004

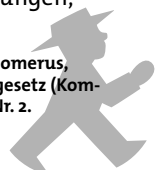
JEDENFALLS GILT: Bis Ende Mai muss eine ganze Reihe neuer Datenschutzverpflichtungen (siehe info-Kasten Seite 22) in die Praxis umgesetzt sein. Einige davon sollen hier kurz beleuchtet werden:

(1) Mit der Regelung über automatisierte Einzelentscheidungen (§ 6 a BDSG) soll sichergestellt werden, dass Entscheidungen, die einzelne Beschäftigte oder auch Bürger betreffen, nicht ausschließlich auf der Basis automatisiert erstellter Auswertungen erfolgen dürfen, sondern durch Menschen entschieden werden müssen. Dem Betroffenen steht hier flankierend ein Recht auf Auskunft zu, das sich auch auf den logischen Aufbau der automatisierten Verarbeitung erstreckt.

(2) Es gilt die Vorgabe ›Datenvermeidung und Datensparsamkeit‹ (§ 3 a BDSG). Danach sind Datenverarbeitungssysteme so auszuwählen und auszugestalten, dass keine oder so wenig personenbezogene Daten wie möglich verarbeitet werden. Durch die gezielte Auswahl und den gezielten Einsatz datenschutzfreundlicher Technik sollen die Gefahren für das ›informationelle Selbstbestimmungsrecht‹ [→] von vornherein minimiert werden. So wird man zum Beispiel vor dem Einsatz von Videoüberwachungsanlagen überprüfen müssen, ob es nicht ›schonendere‹ Überwachungs- und Sicherungsmethoden gibt.

(3) Für ›besondere Arten personenbezogener Daten‹ – auch kurz als ›sensitive Daten‹ bezeichnet – gelten besondere Regelungen. Hierunter fallen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen,

<sup>1</sup>... So auch: Gola/Schomerus, Bundesdatenschutzgesetz (Komentar), § 45 Rand-Nr. 2.



## Die wichtigsten Neuregelungen

Änderungen/Neuregelungen	BDSG
Strafvorschriften; Ordnungswidrigkeiten mit teilweiser Erhöhung des Strafrahmens	§ 43, § 44
Übermittlung personenbezogener in EU-Mitgliedstaaten und Übermittlung in Drittstaaten	§ 4 b + c
Mobile Speichermedien (Chip-Karten)	§ 6 c
Videoüberwachung	§ 6 b
Direkterhebung	§ 4 Abs. 2
Widerspruchsrecht des Betroffenen	§ 20
Vorabkontrolle	§ 4 d Abs. 5
Besondere Arten personenbezogener Daten (z.B. Gesundheitsdaten, Gewerkschaftszugehörigkeit)	§ 28 Abs. 6–9
Automatisierte Einzelentscheidungen	§ 6 a
Datenschutzaudit	§ 9 a
Stärkung der Stellung der Aufsichtsbehörden	§ 38
Interne Datenschutzbeauftragte auch im öffentlichen Bereich	§ 4 f
Führen von Übersicht	§ 4 e
Einwilligung	§ 4 a
Datenvermeidung und Datensparsamkeit	§ 3

### ■ § 28 Abs. 6 BDSG

#### Erheben, Verarbeiten und Nutzen besondere Arten personenbezogener Daten

Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist nur zulässig, soweit nicht der Betroffene nach Maßgabe des § 4 a Abs. 3 eingewilligt hat, wenn

- dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
- es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
- dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
- dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen am Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

### ■ Übersichten (nach § 4 e in Verbindung mit § 4 g Abs. 2 BDSG)

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- Zweckbestimmung der Datenerhebung, -verarbeitung und -nutzung,
- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten und Datenkategorien,
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
- eine geplante Übermittlung in Drittstaaten,
- eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind,
- zugriffsberechtigte Personen.

Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Alle Unternehmen und Einrichtungen, die solche sensiblen Daten verarbeiten, müssen die strengen Vorgaben in § 28 Abs. 6 – 9 BDSG zwingend einhalten (siehe info-Kasten links).

(4) Das neu ins BDSG aufgenommene Prinzip der ›Direkterhebung‹ (§ 4 Abs. 2 BDSG) muss unter anderem zur Folge haben, dass der Arbeitgeber bei Bewerbungen keine Informationen bei dem früheren Arbeitgeber des Bewerbers einholen darf.

(5) Die Unternehmen müssen die zu führenden Übersichten auf den aktuellen Stand bringen (siehe info-Kasten links). Diese Übersichten sind dem betrieblichen Datenschutzbeauftragten nach § 4 g BDSG zur Verfügung zu stellen. Zudem sind diese Übersichten auf Antrag jedermann (also jedem Bürger) in geeigneter Weise verfügbar zu machen.

(6) Die Aufsichtsbehörden können die verantwortlichen Stellen (z.B. Unternehmen) jederzeit in Bezug auf die Umsetzung des BDSG kontrollieren, denn mit der Novellierung in 2001 ist die so genannte ›Anlassaufsicht‹ (Kontrolle nur dann, wenn es einen bestimmten Anlass, also beispielsweise eine konkrete Beschwerde gab) weggefallen.

(7) Zudem wurde der Bußgeldrahmen auf bis zu 250 000 Euro erweitert – dieses Bußgeld kann aufgrund des Straftatbestands nicht ordnungsgemäß durchgeführter und erhobener Daten angeordnet werden.

## Datenschutzregeln müssen umgesetzt sein

UM ES NOCH EINMAL ganz deutlich zu sagen: Diese Datenschutzregeln sind nicht neu. Sie galten so schon für alle Datenerhebungen und -verarbeitungen, die nach dem 23. Mai 2001 in Betrieb genommen wurden. Jetzt aber gelten sie auch für die ›Altsysteme‹, also flächendeckend. Da das BDSG bekanntermaßen ein Schutzgesetz (auch) für die Beschäftigten ist, gehört es zu den Aufgaben von Betriebs- und Personalräten, seine Einhaltung zu überwachen. Zudem müssen Betriebsräte und auch Arbeitgeber im Rahmen der Umsetzung der Mitbe-

stimmungsrechte nach § 87 Abs. 1 Nr. 6 BetrVG (technische Überwachungseinrichtungen) und § 94 BetrVG (Personalfragebogen) die geltenden Vorschriften des BDSG beim Abschluss von Betriebsvereinbarungen berücksichtigen. So kann auch eine Überprüfung bereits bestehender Betriebsvereinbarungen erforderlich sein.

Auch auf den betrieblichen Datenschutzbeauftragten (bzw. für das Unternehmen) kommen im Rahmen der Anpassung der Altsysteme (laufende Verarbeitungen) eine Fülle an Aufgaben zu. Festzustellen bleibt jedoch, dass für ein Unternehmen, dass sich auch bisher schon angemessen um den Datenschutz gekümmert hat, der 23. Mai 2004 nicht überraschend kommen kann ...

Bruno Schierbaum, BTQ Niedersachsen, Donnerschwerer Straße 84, 26123 Oldenburg, schierbaum@btq.de



[-> informationelle Selbstbestimmung = das Recht jedes Bürgers (Arbeitnehmers) im Grundsatz selbst über Speicherung und Verwendung ›seiner‹ Daten zu bestimmen; das heißt praktisch, dass jede Speicherung personenbezogener Daten verboten ist, es sei denn, der Betroffene hat zugestimmt oder es gibt irgendeine gesetzliche Regelung, die die Datenerfassung, -speicherung und -verarbeitung ausdrücklich gestattet oder sogar verlangt

# aus der praxis datenschutztipps für die praxis

In dieser Serie werden regelmäßig Informationen und Praxisfälle zum Datenschutz veröffentlicht, wie sie in den Berichten der Datenschutzbeauftragten und Aufsichtsbehörden der Länder und des Bundes zu finden sind ...

HAJO KÖPPEN

## Arzt-Warnlisten, Video-Bauüberwachung

»ERST DENKEN, DANN Handeln«, sollte auch bei der Umsetzung von Datenschutz-Maßnahmen ein zu beherzigender Grundsatz sein. Wer danach handelt, spart sich möglicherweise viel Arbeit und so manche Peinlichkeit. Dies kann man an zwei gegensätzlichen Vorgehensweisen sehen, wie sie im 19. Tätigkeitsbericht des Hamburger Datenschutzbeauftragten beschrieben sind:

### 1.

›Blaumacher‹ sind weder bei Arbeitgebern noch bei Krankenkassen sonderlich beliebt. So wurden von Arbeitgebern auch schon Detektive eingesetzt, um ›Simulanten‹ zu ›entlarven‹. Etwas zu weit ging allerdings die Betriebskrankenkasse (BKK) Hamburg. Sie verschickte an zahlreiche Arbeitgeber eine Liste mit einer Reihe von Ärzten, die bei der Krankenkasse in dem Verdacht standen, übermäßig viele Arbeitsunfähigkeits-Bescheinigungen auszustellen. Damit hatte die BKK, so die Hamburger Datenschutzaufsicht, die Vorschriften des Sozialgesetzbuches zur Überprüfung der Arbeitsunfähigkeit von Versicherten missachtet (Seite 35):

»Das Sozialgesetzbuch enthält spezielle Regelungen, wie bei Zweifeln an der Arbeitsunfähigkeit von Versicherten zu verfahren ist. Danach ist die Krankenkasse in solchen Fällen gesetzlich verpflichtet, den Medizinischen Dienst der Krankenversicherung

(MDK) einzuschalten. Allein der MDK hat zu prüfen, ob die Zweifel der Krankenkasse an der Arbeitsunfähigkeit zu Recht bestehen. Das Ergebnis dieser Überprüfung erfährt die Krankenkasse dann vom MDK, damit sie mögliche Maßnahmen treffen kann, die ihr nach den Bestimmungen des Sozialgesetzbuches zustehen, z.B. Kürzung des Krankengeldes.«

Mit seiner Aufsichtstätigkeit konnte der Datenschützer erreichen, dass die BKK zukünftig auf die Versendung solcher Ärztelisten verzichtet. Allerdings weigerte sich die BKK, die mit der Liste belieferten Arbeitgeber erneut anzuschreiben und um Löschung der Arztlisten zu bitten. Erst nach ›sanftem Druck‹ mit einer Beanstandung gegenüber dem Senator für Umwelt und Gesundheit lenkte die BKK ein und verfuhr im Sinne des Datenschutzauftragten.

### 2.

Besser ging es dagegen die Behörde für Bau und Verkehr an. Sie bat vor Einführung einer Bauüberwachung durch Videokameras den Hamburger Datenschutzbeauftragten um eine Stellungnahme zu ihrem Plan (Seite 58). Danach war die Installation einer Videokamera an einer Brückenbaustelle vorgesehen, deren Bilder über ein Passwort via Internet vom zuständigen Bauüberwachungspersonal abgerufen