BRUNO SCHIERBAUM

Rechte der Beschäftigten im novellierten BDSG

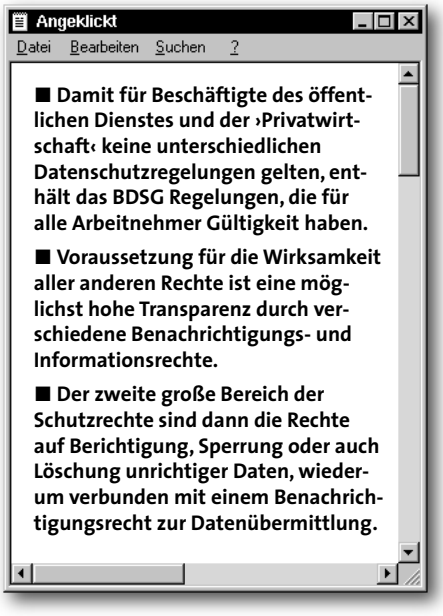
Das Erscheinen des lange angekündigten Arbeitnehmedatenschutzgesetzes lässt weiter auf sich warten. Das heißt allerdings nicht, dass es keinen Datenschutz für Arbeitnehmer gäbe – entsprechende Bestimmungen sind nur ›mit lockerer Hand‹ über das notorisch unübersichtliche Bundesdatenschutzgesetz verteilt. Hier deshalb eine Zusammenstellung der wichtigsten Regelungen.

Angesichts der zunehmenden Verarbeitung von Arbeitnehmerdaten in Unternehmen und Behörden sollten die im Bundesdatenschutzgesetz verankerten Rechte der Beschäftigten eigentlich an Bedeutung gewinnen. Praktisch jeder Mensch sollte – ob als Beschäftigter, Kunde, Klient oder Patient - die Möglichkeit haben, wissen zu können, welche Daten über ihn verarbeitet werden; ein Grundsatz, der schon seit dem ›Volkszählungsurteil‹ im Jahre 1983 eine wichtige Vorgabe zum Datenschutz ist. Da in der Praxis von den Rechten der Beschäftigten auf Information, Benachrichtigung, Auskunft oder Korrektur ihrer Daten wenig Gebrauch gemacht wird und es zudem einschlägige Neuerungen im BDSG gibt, sollen nachfolgend die Rechte der Beschäftigten näher betrachtet werden.

Dies geschieht aus zwei Gründen. Erstens ist die Kenntnis dieser Rechte für Betriebs- und Personalräte von Bedeutung, da diese die Einhaltung bestehender Gesetze (in diesem Fall des BDSG) zu überwachen zu haben. Zweitens sollte jede Interessenvertretung prüfen, inwieweit die im BDSG festgelegten Rechte in Betriebs-/Dienstvereinbarungen verankert werden sollten. Und falls Betriebs-/Dienstvereinbarungen bereits bestehen, sollte geprüft werden, ob vor dem Hintergrund der Novellierung des BDSG Anpassungen vorzunehmen sind.

Anwendung des Datenschutzrechts

Sollen personenbezogene Daten der Beschäftigten erhoben, verarbeitet oder genutzt werden, wird in der Regel die Zulässigkeit der Datenverarbeitung *aus den Datenschutzgesetzen* selbst herzuleiten sein – aber auch Betriebs- und Dienstvereinbarungen kommen als Grundlage für eine rechtmäßige Datenverarbeitung in Betracht. Auf Grund der verschiedenen gesetzlichen Regelungen zum Datenschutz (etwa dem BDSG und den daneben bestehenden Datenschutzgesetzen der Länder) herrscht eine gewisse Unübersichtlichkeit und somit in der Praxis auch Unklarheit, welche gesetzlichen Vorgaben in der Praxis anzuwenden sind. Diese Unübersichtlichkeit ist leider auch mit der Novellierung des BDSG nicht geändert worden.



Nimmt man zum Beispiel das Bundesdatenschutzgesetz zur Hand, so nennt das Gesetz unter ›Zweck und Anwendungsbereich‹ folgende Adressaten:

- öffentliche Stellen des Bundes,
- öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und
- nicht-öffentliche Stellen.

Für die öffentlichen Stellen *des Bundes* findet neben den allgemein geltenden Regelungen vor allem der zweite Abschnitt des BDSG Anwendung, der mit ›Datenverarbeitung der öffentlichen

Stellen‹ überschrieben ist. Wenn öffentliche Stellen des Bundes allerdings als *öffentlich-rechtliche Unternehmen* ›am Wettbewerb teilnehmen‹, gilt an Stelle des zweiten Abschnitts der dritte Abschnitt. Das heißt: Diese Stellen werden datenschutzrechtlich den Privatbetrieben gleichgestellt.

Da alle Bundesländer eigene Datenschutzgesetze erlassen haben, ist für öffentliche Stellen *der Länder* das jeweilige Landesdatenschutzgesetz anzuwenden.

Für die so genannten nicht-öffentliche Stellen, zu denen Privatbetriebe in jeder Rechtsform, ebenso wie Vereine und Stiftungen gehören, gilt neben den allgemein geltenden Regelungen vor allem der dritte Abschnitt des BDSG, der mit ›Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen‹ überschrieben ist. So weit, so kompliziert.

Für den Beschäftigten-Datenschutz gilt allerdings noch eine besondere Regelung:

Damit Beschäftigte im öffentlichen Dienst (des Bundes) und die Beschäftigten in der Privatwirtschaft (nicht-öffentlicher Bereich) unter datenschutzrechtlichen Gesichtspunkten *gleich* behandelt werden, verweist das BDSG *für den Beschäftigten-Datenschutz* bei öffentlichen Stellen auf den für Privatbetriebe geltenden dritten Abschnitt des BDSG (siehe info-Kasten auf Seite 22).

Das heißt, dass die im Folgenden aufgearbeiteten Rechte der Beschäftigten *sowohl für den öffentlichen Bereich des Bundes als auch für den nicht-öffentlichen Bereich gelten*. Für den öffentlichen Bereich der Länder gelten im Grunde die gleichen Rechte der Betroffenen, da auch die Landesdatenschutzgesetze mit der Novellierung den Vorgaben der EG-Richtlinie entsprechen müssen.

Transparenz der Datenverarbeitung

Mit der Novellierung des BDSG und gerade auch mit der Zunahme der Datenverarbeitung in den Betrieben und im öffentlichen Leben sind die Aussagen des Bundesverfassungsgerichts (BVerfG) zum Datenschutz (= Schutz der Persönlichkeitsrechte) von zentraler Bedeutung. Das BVerfG hat in seinem Urteil…[1] vom 15. 12. 1983 aus Artikel 1 Abs. 1 und

Artikel 2 Abs. 1 Grundgesetz ein Recht jedes Einzelnen auf ›informationelle Selbstbestimmung‹ abgeleitet – das heißt: Jeder Mensch soll im Grundsatz die Möglichkeit haben, über Verbleib und Verarbeitung ›seiner‹ Daten selbst zu bestimmen (was allerdings entsprechendes Wissen voraussetzt).

In der Erkenntnis der mit der modernen Datenverarbeitung verbundenen Gefahren für die Betroffenen führt das Gericht aus: »Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.«

Zudem stellt das Gericht auch das Recht Einzelnen heraus, »grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.«

Dieses *Recht auf informationelle Selbstbestimmung* ist allerdings nicht ›schrankenlos‹, jede Einschränkung bedarf aber einer gesetzlichen Grundlage. Anders ausgedrückt bedeutet dies, dass jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten immer nur auf der Basis eines Gesetzes erfolgen darf.

Für die Existenz und Ausübung des Rechts auf informationelle Selbstbestimmung bildet *Transparenz* der Datenverarbeitung eine wesentliche Voraussetzung. Das BVerfG führt dazu aus: »Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt sein, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen, wer was bei welcher Gelegenheit über sie weiß.«…[2] Transparenz der Datenverarbeitung gehört somit zu den verfassungsrechtlich gewährleisteten Grundpositionen.

1… Vergl.: BVerfG, Urteil vom 15. 12. 1983, in: Neue Juristische Wochenschrift 8/84,ab Seite 419

2… Siehe gleiche Quelle wie Fußnote 1.

info

Grundlage des

Arbeitnehmerdatenschutzes im neuen BDSG

§ 12 Abs. 4 BDSG

Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- und arbeitsrechtliche Rechtsverhältnisse erhoben, verarbeitet oder genutzt, gelten anstelle der §§ 13 bis 16, 19 bis 20 der § 28 Abs. 1 und 3 Nr. 1 sowie die §§ 33 bis 35 , auch soweit personenbezogene Daten weder automatisiert verarbeitet noch in nicht automatisierten Dateien verarbeitet oder genutzt oder dafür erhoben werden.

Vorrang für andere gesetzliche Regelungen

§ 1 Abs. 3 BDSG

Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes (gemeint ist das BDSG, B.S.) vor.

Rechte und Pflichten der Betroffenen im Einzelnen

Das BDSG enthält eine Reihe von Rechtsansprüchen der Betroffenen, die sich durch das ganze Gesetz hindurchziehen. Für denjenigen, der das BDSG anzuwenden hat, oder denjenigen, der seine Rechte nutzen will, wäre eine Zusammenfassung dieser Rechte an einer Stelle im Gesetz mehr als sinnvoll gewesen.

Aber jedenfalls hat ein Betroffener (Beschäftigter) die Rechte auf:

Information	§ 4 Abs. 3 BDSG
Unterrichtung	§ 6 c BDSG
Benachrichtigung	§ 33 BDSG
Auskunft	§ 34 Abs. 1 und 6 a Abs. 3 BDSG
Berichtigung	§ 35 Abs. 1 BDSG
Löschung	§ 35 Abs. 2 BDSG
Sperrung	§ 35 Abs. 4 BDSG
Recht auf Widerspruch	§ 35 Abs. 5 BDSG
Verpflichtung auf das Datengeheimnis	§ 5 BDSG
Schadensersatz	§ 7 und 8 BDSG

Hinzu kommt dann noch die in § 6 Bundesdatenschutzgesetz festgelegte:

Unabdingbarkeit der Rechte

Die eben genannten Rechte auf Auskunft, Berichtigung, Löschung, Sperrung oder Widerspruch sind also ›unabdingbar‹ und können durch ein ›Rechtsgeschäft‹ (wie z. B. einen Arbeitsvertrag oder auch eine Betriebs-/Dienstvereinbarung) weder ausgeschlossen noch beschränkt werden. Verträge und Vereinbarungen, die diese Rechte ganz oder teilweise einschränken, sind also unwirksam. Und weil das Recht auf informationelle Selbstbestimmung (einschließlich Datentransparenz) ein bedeutendes Rechtsgut ist, ist es nur konsequent, dass in diesem Punkt die Vertragsfreiheit eingeschränkt wird. Denn insbesondere in Abhängigkeitsverhältnissen – wie etwa Arbeitsverhältnissen – ist der schwächere Vertragspartner (Arbeitnehmer) eher bereit, auf seine Rechte zu verzichten.

Recht auf Information

Das BDSG enthält eine neue Neuregelung bei der Erhebung von Daten (§ 4 Abs. 3 BDSG). Zum einen ist dort jetzt das Prinzip der *Direkterhebung* (Daten dürfen also nur direkt beim Betroffenen und nicht über Dritte erhoben werden) und zum anderen ein *Informationsrecht* verankert. Außerdem muss die verarbeitende Stelle bereits zum Zeitpunkt der Datenerhebung konkret den Verarbeitungszweck festlegen. Zusammengenommen ist deshalb der Beschäftigte (der Betroffene) bei der Direkterhebung von dem Unternehmen (der verantwortlichen Stelle) über folgende Aspekte zu unterrichten:

- die Identität der verantwortlichen Stelle,
- die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
- die Kategorien von Empfängern, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit einer Übermittlung seiner Daten rechnen muss.

Nur wenn der Betroffene diese Informationen auf andere Weise erhält, entfällt diese Informationspflicht.

Recht auf Unterrichtung bei mobilen Speichermedien

Das BDSG enthält eine Regelung zu mobilen Speicher- und Verarbeitungsmedien. Dieses sind Datenträger, ...

... die an den Betroffenen (Beschäftigten) ausgegeben werden,
... auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle *automatisiert verarbeitet* werden können und
... bei denen der Betroffene (Beschäftigte) diese Verarbeitung durch den Gebrauch des Datenträgers beeinflussen kann (§ 3 Abs. 10 BDSG).

Gemeint sind damit laut Gesetzesbegründung mobile Speicher- und Verarbeitungsmedien, die mit einem Prozessorchip ausgestattet sind. Dieses sind zum Beispiel personalisierte Chip-Karten oder zukünftig auch Armbänder oder Halsketten, die mit einem Chip ausgestattet sind. Dem Gesetzgeber kam es darauf an, die Speicher- und Verarbeitungsmedien mit zu erfassen, die sich dadurch auszeichnen, dass personenbezogene Daten auf ihnen nicht nur gespeichert, sondern *auch verarbeitet* werden können, ohne dass diese Verarbeitungsgänge für den Betroffenen unmittelbar nachvollziehbar sind. Zu diesen Medien zählen auch die Chip-Karten der Krankenkassen, die an die Versicherten ausgegeben werden.

Die Stelle also, die ein solches mobiles personenbezogenes Speicher- *und Ver-*

*arbeitungs*medium ausgibt oder die Verfahren zur automatisierten Verarbeitung auf dieses Medium aufbringt, muss den Betroffenen (Beschäftigten) unterrichten ...

... über Identität und Anschrift der verantwortlichen Stelle,
... in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden Daten,
... darüber, wie der Betroffene seine Rechte auf Auskunft, Berichtigung, Löschung und Sperrung ausüben kann,
... über die bei Verlust und Zerstörung zu treffenden Maßnahmen (siehe § 6c Abs. 1 BDSG).

Zusätzlich hat die verantwortliche Stelle dafür Sorge zu tragen, dass die zur Wahrnehmung dieses Auskunftsrechts erforderlichen Geräte in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen. Das kann zum Beispiel heißen, dass entsprechende Lesegeräte aufgestellt werden müssen, an denen der Betroffene die über ihn gespeicherten personenbezogenen Daten einsehen und ausdrucken kann.

Alle technischen Vorgänge, die auf dem Speicher- und Verarbeitungsmedium (z. B. einer Chip-Karte) eine Datenverarbeitung auslösen, müssen laut § 6 c Abs. 3 BDSG für den Betroffenen eindeutig erkennbar sein. Damit soll sichergestellt werden, dass Verarbeitungen nicht vom Betroffenen unbemerkt – etwa durch Vorbeigehen an einem Zugangskontrollgerät – ausgelöst werden.

Benachrichtigung des Arbeitnehmers

Werden *erstmals* personenbezogene Daten eines Betroffenen (Beschäftigten) gespeichert, ohne das dieser davon Kenntnis hat, ist der Betroffene zu benachrichtigen ...

... von der Speicherung selbst,
... der Art der gespeicherten Daten,
... der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
... der Identität der verarbeitenden Stelle.

Eine solche Benachrichtigung hat also zu erfolgen, wenn über eine Person Daten gespeichert werden, zu der bisher nichts gespeichert wurde – etwa bei einer Neueinstellung. Sie hat aber auch immer dann zu erfolgen, wenn später eine neue Art von Daten hinzukommt.

Das Gesetz schreibt für diese Benachrichtigung keine bestimmte Form vor. Sie liegt im Ermessen der verantwortlichen Stelle und kann mündlich, telefonisch oder schriftlich erfolgen. Allerdings sollte schon aus Beweissicherungsgründen immer die Schriftform gewählt werden. Damit kann sich die verantwortliche Stelle (das Unternehmen) gegen mögliche Vorwürfe absichern, sie habe die Benachrichtigung

Arbeitnehmer müssen nicht nur einmal über die von ihnen gespeicherten Personaldaten informiert werden, sondern immer wieder dann, wenn eine neue Art von Daten erfasst wird.

Werden also beispielsweise im Laufe eines Beschäftigungsverhältnisses von einem bestimmten Zeitpunkt an neu Qualifikationsdaten für die Personalplanung gespeichert, muss auch darüber eine Benachrichtigung erfolgen. Dies ergibt sich aus der Verpflichtung im BDSG, dass auch *über die Art der Daten* zu benachrichtigen ist.

Wäre das nicht so, könnte sich das Ziel der Benachrichtigung in sein Gegenteil verkehren. Ein Betroffener (Beschäftigter) würde dann unter Umständen immer noch glauben, dass über ihn nur die vielleicht ›harmlosen‹ Daten vom Beginn seines Beschäftigungsverhältnisses erfasst sind, während tatsächlich längst auch sensible, seine Persönlichkeitsrechte gefährdende Daten gespeichert wurden.

Die Folge wäre, dass der Betroffene trotz der veränderten Situation keinen Grund sehen würde, von seinem ihm zustehenden Auskunftsrecht Gebrauch zu machen ...

Eine Benachrichtigung über ›erstmals erfasste personenbezogene Daten‹ hat unverzüglich – das heißt, ›ohne schuldhaftes Zögern‹ – *nach* der erstmaligen Speicherung zu erfolgen. Sie wird nach allgemeiner Auffassung dem Betroffenen also spätestens zwei bis vier Wochen nach erstmaliger Speicherung zugegangen sein müssen.

unterlassen und damit eine Ordnungswidrigkeit begangen (§ 43 Abs. 1 Nr. 8 BDSG).

Ausnahmen von der Benachrichtigung

Das BDSG sieht eine Reihe von Ausnahmen von der Benachrichtigungspflicht vor (§ 32 Abs. 2 BDSG). Die Ausnahmetatbestände sind allerdings eng und im Zweifel zu Gunsten der Betroffenen und damit auch zu Gunsten der Benachrichtigungspflicht auszulegen.

Erlangung der Kenntnisse ›auf andere Weise‹

Eine Pflicht zur Benachrichtigung besteht *nicht*, so heißt es im Gesetz, wenn »der Betroffene auf andere Weise Kenntnis von der Speicherung und Übermittlung erlangt hat« (§ 33 Abs. 2 Nr. 1 BDSG). Gerade im Arbeitsleben kommt dieser Ausnahmeregelung große Bedeutung zu, da hieraus manchmal abgeleitet wird, dass in Arbeitsverhältnissen eine Benachrichtigung zu erstmals neu gespeicherten Daten generell unterbleiben könne.

Von der Kenntnis einer beabsichtigten Datenspeicherung wird dann aus-

gegangen, wenn ein Betroffener (Beschäftigter) eine Einwilligungserklärung nach § 4 BDSG unterschrieben hat. Außerdem gibt es noch die Auffassung, dass ein Beschäftigter ›Kenntnis auf andere Weise‹ auch in dem Augenblick erlangt, wenn er das erste Mal eine offensichtlich EDV-erstellte Lohn- und Gehaltsabrechnung erhält.

Rechtlich bleibt die Sache aber nicht immer klar abgrenzbar. Betriebs- und Personalräte sollten deshalb eine umfassende Benachrichtigungspflicht in einer Betriebs- oder Dienstvereinbarung verankern.

Gesetzliche Aufbewahrungsfristen / Datenschutz- und Datensicherungskontrolle

Die Benachrichtigungspflicht entfällt auch dann, wenn die Daten auf Grund gesetzlicher, satzungsgemäßer oder vertraglicher Aufbewahrungsfristen *nicht gelöscht werden dürfen* oder ausschließlich der *Datensicherung* oder der *Datenschutzkontrolle* dienen (§ 33 Abs. 2 Nr. 2 BDSG).

Die erste Ausnahme (vertragliche Aufbewahrungsfristen) ist hinsichtlich der Benachrichtigungspflicht weitgehend gegenstandslos, da die aufzubewahrenden Daten zuvor regelmäßig *für einen bestimmten Zweck* gespeichert wurden – und das heißt, dass da bereits eine Benachrichtigungspflicht bestanden hat. Auch dass die ausschließlich der Datensicherung und Datenschutzkontrolle dienenden Daten nicht der Benachrichtigungspflicht unterliegen, lässt sich hinnehmen, da das BDSG ein generelles Verbot der *Zweckentfremdung* dieser Daten enthält (§ 31 BDSG).

Geheimhaltungspflicht

Eine Benachrichtigung muss ebenfalls *nicht* erfolgen, wenn die Daten nach einer Rechtsvorschrift oder ›ihrem Wesen nach‹ – namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten – geheim gehalten werden müssen (§ 33 Abs. 2 Nr. 3 BDSG). In Bezug auf Arbeitnehmerdaten wird dies in der Regel nicht zum Tragen kommen.

Gesetzliche Vorschrift

Eine Benachrichtigung entfällt nach § 33 Abs. 2 Nr. 4 BDSG auch, wenn die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist.

Wissenschaftliche Forschung

Nach § 33 Abs. 2 Nr. 5 BDSG gibt es keine Benachrichtigungspflicht, wenn die Speicherung oder Übermittlung von Daten für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde.

Gefährdung der öffentlichen Sicherheit

Eine Benachrichtigungspflicht besteht ebenfalls nicht, wenn zum Beispiel eine Sicherheitsbehörde gegenüber der speichernden Stelle (dem Unternehmen) festgestellt hat, dass das Bekanntwerden bestimmter Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde (§ 33 Abs. 2 Nr. 6 BDSG).

Diese Regelung kann in Unternehmen von Bedeutung sein, die mit staatlichen Stellen Vertragsbeziehungen zu geheimhaltungspflichtigen Angelegenheiten unterhalten. Einen solchen Fall, dass personenbezogene Daten auch gegenüber dem Betroffenen geheim gehalten werden müssen, kann es zum Beispiel geben, wenn ein Beschäftigter unter dem Verdacht geheimdienstlicher Tätigkeit steht. Nach Lage der Dinge kommt eine solche Maßnahme aber allenfalls im Rahmen der Strafverfolgung in Betracht.

Allgemein zugängliche Quellen

Die Benachrichtigung kann auch entfallen, wenn die Daten *für eigene Zwecke* gespeichert und aus allgemein zugänglichen Quellen entnommen sind und wenn eine Benachrichtigung wegen der Vielzahl der Betroffenen unverhältnismäßig wäre (§ 33 Abs. 2 Nr. 7 a BDSG). Zu den ›allgemein zugänglichen Quellen‹ zählen insbesondere Druckmedien (wie Zeitungen, Adressbücher, Branchenverzeichnisse, Telefonbücher) sowie Hörfunk, Fernsehen, Filme und Videos. Darüber hinaus zählen zu den öffentlich zugänglichen Quellen öffentliche Register, wie das Schuldnerverzeichnis (§ 915 ZPO), das Handelsregister (§ 9 HGB) und ähnliches.

Das klingt einleuchtend, ist in dieser Form aber nicht akzeptabel. Zwar steht nach Artikel 5 Abs. 1 Satz 1 GG jedem das Recht zu, sich aus allgemein zugänglichen Quellen zu informieren, dies schließt aber eine Befugnis, diese Informationen in eigenen EDV-Systemen zu speichern und dort vielleicht mit anderen personenbezogenen Daten zu verknüpfen, keinesfalls ein.

Gefährdung der Geschäftszwecke

Eine Benachrichtigung kann schließlich auch dann entfallen, wenn die Benachrichtigung die *Geschäftszwecke der verantwortlichen Stelle* (des Unternehmens) erheblich gefährden würde. Eine Ausnahme von dieser Ausnahme soll nur dann gelten, wenn das Interesse an der Benachrichtigung (durch den Betroffenen) die Gefährdung überwiegt (§ 33 Abs. 2 Nr. 7b BDSG). In Bezug auf das Arbeitsverhältnis kommen hier wohl nur Betriebs- oder Geschäftsgeheimnisse in Betracht. Dabei wird eine Beeinträchtigung allein nicht genügen, vielmehr muss die Mitteilung (gegenüber dem einzelnen Betroffenen!) dazu füh-

Für die Benachrichtigungspflicht gibt es zahlreiche Ausnahmen. Deshalb sollte eine umfassende Benachrichtigungspflicht in Betriebs- oder Dienstvereinbarungen verankert werden.

ren, dass beispielsweise bestimmte Geschäfte aus Kostengründen unmöglich würden. Aber selbst bei einigem Nachdenken fällt einem eigentlich kein Beispiel ein, in dem die Benachrichtigung eines Arbeitnehmers über von ihm gespeicherte Daten ein Betriebs- oder Geschäftsgeheimnis gefährden würde. Wir können also davon ausgehen, dass dieser Ausnahme im Arbeitsrecht keine große Bedeutung zukommt.

Verstoß gegen die Benachrichtigungspflicht

Ein Verstoß gegen die Benachrichtigungspflicht zieht ein Bußgeld nach sich (§ 43 Abs. 3 BDSG): Wer einen Betroffenen (Beschäftigten) nicht, nicht richtig oder nicht vollständig benachrichtigt, begeht eine Ordnungswidrigkeit (§ 43 Abs. 1 Nr. 8 BDSG). Beruft sich die verantwortliche Stelle (das Unternehmen) auf eine der hier aufgeführten Ausnahmen, so hat sie darzulegen, dass sie die Voraussetzungen und deren tatsächliches Vorhandensein sorgfältig geprüft hat.

Recht auf Auskunft

Neben dem Recht, unaufgefordert über die Speicherung ›eigener‹ Daten informiert zu werden, gibt es gemäß § 34 Abs.1 BDSG auch das Recht, von sich aus Auskunft zu verlangen über:

- die zur eigenen Person gespeicherten Daten,
- deren Herkunft,
- den oder die Empfänger (oder Kategorien von Empfängern) und
- den Zweck der Speicherung.

Dieses Auskunftsrecht ermöglicht einem Betroffenen (Beschäftigten) den Anspruch auf Mitteilung der ›zu seiner Person gespeicherten Daten‹. Dieser Begriff ist weiter zu fassen als der im BDSG sonst verwendete Begriff ›personenbezogene Daten‹ (§ 3 Abs. 1 BDSG), denn er umfasst über jede Einzelangabe, über ›persönliche und sachliche Verhältnisse‹ hinaus, auch Angaben *über die gespeicherten Daten*. So gehört zu den ›zur Person gespeicherten Daten‹ auch die Bezeichnung der jeweiligen Dateien. Auch gesperrte Daten unterliegen der Auskunftspflicht.

Zudem müssen dem Betroffenen ›Herkunft und Empfänger‹ seiner Daten mitgeteilt werden. ›Herkunft‹ meint die Quelle, das heißt die Person oder Institution, von der die Information stammt. Gemeint sind natürlich *externe* Personen und Stellen, wobei auch die Adresse desjenigen, von dem die Daten stammen, anzugeben ist. ›Empfänger‹ sind alle Personen und Institutionen, an die in der Vergangenheit (d.h. bis zur Auskunftserteilung) Daten übermittelt wurden.

Dabei ist es gleichgültig, ob es sich um regelmäßige oder einmalige Datenübermittlungen gehandelt hat. Der Arbeitnehmer hätte dann die Möglichkeit, unzulässigen oder unrichtigen Angaben bis hin zu weiteren (externen) Empfängern nachzugehen. Durch diese Regelungen wird die Durchsetzung des Rechts auf Datenkorrektur über die speichernde Stelle hinaus in die gesamte Übermittlungskette erleichtert.

Ferner ist dem Betroffenen der Zweck der Speicherung der Daten mitzuteilen. Hierzu gehört nicht nur der allgemeine Verwendungszusammenhang (wie z. B. Produktionssteuerung oder Lohn- und Gehaltsabrechnung), sondern auch die Angabe der eingesetzten Software-Anwendungen.

Das Auskunftsverlangen ist an keine bestimmte Form gebunden und kann mündlich, telefonisch oder schriftlich erfolgen. Dabei kann der Betroffene sein Auskunftsverlangen jederzeit an den Arbeitgeber richten und muss dies auch nicht näher begründen. Er ist jedoch verpflichtet, die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher zu bezeichnen (§ 34 Abs. 1 BDSG).

Die Auskunft ist vom Arbeitgeber in schriftlicher Form zu erteilen, wobei die Daten in entschlüsselter Form mitzuteilen sind. Die Auskunft unentgeltlich (§ 34 Abs. 5 BDSG).

Ein besonderes Auskunftsrecht gibt es bei den ›automatisierten Einzentscheidungen‹ – das sind Personalentscheidungen, die allein durch eine Software getroffen werden.

Ein Verstoß gegen die Benachrichtigungspflicht kann als Ordnungswidrigkeit geahndet werden, unverständlicherweise gilt dies jedoch nicht für einen Verstoß gegen die Auskunftspflicht. Der Betroffene kann zwar gemäß § 38 Abs. 1 BDSG die Aufsichtsbehörde einschalten, die aber keinerlei Zwangsmittel gegen die Stelle hat, da sie eben auch nur in Bezug auf die aufgeführten Ordnungswidrigkeiten bei Gericht antragsberechtigt ist ...

Ein besonderes Auskunftsrecht ist bei so genannten ›automatisierten Einzelentscheidungen festgelegt worden (§ 6 a Abs. 3 BDSG). Gemeint sind damit Entscheidungen, die allein auf Grund gespeicherter Daten automatisch durch eine Software getroffen werden. Zu denken ist hier an die sogenannten Profilabgleiche. Mit Hilfe von Personalinformationssystemen werden automatisiert für zu besetzende Stellen die Mitarbeiter mit der erforderlichen Qualifikation gesucht. Werden solche automatisierten Einzelentscheidungen durchgeführt, erstreckt sich das Auskunftsrecht des Betroffenen auch auf den logischen Aufbau der automatisierten Verarbeitung.

Die Probleme für die praktische Umsetzung sind jedoch nicht zu übersehen, denn Software vor allem dieser Art ist äußert umfangreich und komplex. In jedem Fall aber muss der logische Auf-

bau, so wie er sich im Programmablauf vollzieht, der betroffenen Person verständlich gemacht werden. Der Betroffene muss also verstehen können, in welcher Weise aus seinen Daten bestimmte Bewertungen und Klassifizierungen abgeleitet werden und welche Bedeutung diese Werte im Verarbeitungssystem besitzen. Er muss also genau erkennen können, wie diese automatisierte Einzelentscheidung zustande kommt.

Recht auf Einsicht in die Personalakte nach § 83 BetrVG

Auch für das Auskunftsrecht gilt nach § 1 Abs. 3 BDSG (siehe info-Kasten auf Seite 22) grundsätzlich, dass *andere Rechtsvorschriften* des Bundes, soweit sie auf personenbezogene Daten anzuwenden sind, *dem BDSG vorgehen*. Die wichtigste Spezialregelung in Bezug auf das Auskunftsrecht im BDSG ist der § 83 BetrVG. Danach hat der Arbeitnehmer das Recht, in die über ihn geführten Personalakten Einsicht zu nehmen. Er kann hierzu ein Mitglied des Betriebsrats hinzuziehen.

Dieses Einsichtsrecht erstreckt sich auf alle Aufzeichnungen, die sich mit der Person des Arbeitnehmers befassen, ohne Rücksicht auf die Stelle, an der diese Sammlung geführt wird, auf ihre Form oder das verwendete Material – es gilt also auch für elektronisch gespeicherte Daten. Der Anspruch auf Akten- oder Dateieinsicht ist unentgeltlich und kann während der Arbeitszeit wahrgenommen werden. Einsichtnahme bedeutet dabei auch, dass der Arbeitnehmer erhaltene Informationen tatsächlich verstehen können muss – Fachausdrücke sind also zu erläutern und Computer-Ausdrucke gegebenenfalls zu entschlüsseln. Der Arbeitnehmer kann sich anhand der Personalakte Notizen machen und auch Fotokopien aus der Akte anfertigen.

Verhältnis § 34 BDSG zu § 83 BetrVG

Das Akteneinsichtsrecht hat allerdings nur so weit dem Auskunftsrecht (§ 34 BDSG) Vorrang, wie eine Deckungsgleichheit beider Ansprüche besteht.

Eine umfassende Deckungsgleichheit besteht aber nicht, so dass das Auskunftsrecht im BDSG zu einer Ausweitung des Akteneinsichtsrechts (§ 83 BetrVG) führt. Denn: Nach § 33 Abs. 1 BDSG bezieht sich die Auskunft auch *auf Herkunft und Empfänger* der Daten sowie dem *Zweck* der Speicherung.

Außerdem ist eine Auskunft nach § 34 BDSG ist im Gegensatz zum Akteneinsichtsrecht grundsätzlich schriftlich zu erteilen – ein deutlicher Vorteil gegenüber der betriebsverfassungsrechtlichen Regelung. In Bezug auf den Personenkreis schließlich fallen unter das Akteneinsichtsrecht (§ 83 BDSG) nur Arbeitnehmer, wohingegen vom Auskunftsrecht nach § 34 BDSG auch Bewerber, ausgeschiedene Arbeitnehmer ud auch freie Mitarbeiter Gebrauch machen können.

Daten können auch dann ›unrichtig‹ (und damit zu löschen) sein, wenn an sich richtige Daten in einem Umfeld gespeichert sind, das zu Fehlinterpreationen führen kann.

Recht auf Datenkorrektur

Da von den Rechten auf Benachrichtigung und Auskunft – soweit ersichtlich – in der Praxis wenig Gebrauch gemacht wird, dürfte das Recht auf Daten*korrektur* wohl gänzlich ohne praktische Bedeutung sein. Trotzdem sollen sie hier natürlich dargestellt werden, schon um so ihren Bekanntheitsgrad zu erhöhen.

In § 35 BDSG werden die Rechte der Betroffenen auf Datenkorrektur bei unrichtiger oder unzulässiger Datenverarbeitung geregelt. Es sind dies die Rechte auf ...

Berichtigung	(§ 35 Abs. 1 BDSG),
Löschung	(§ 35 Abs. 2 BDSG) und
Sperrung	(§ 35 Abs. 3 und 4 BDSG).
Widerspruch	(§ 35 Abs. 5 BDSG)

Zudem hat der Arbeitnehmer das Recht, zum Inhalt seiner Personalakte Gegenerklärungen abzugeben (§ 83 Abs. 2 BetrVG).

Anspruch auf Berichtigung

Es klingt so selbstverständlich: Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind (§ 35 Abs. 1 BDSG).

Die Berichtigung hat unverzüglich zu erfolgen und ist nicht davon abhängig, ob der Betroffene sein Recht geltend macht. Vielmehr ist die verantwortliche Stelle (das Unternehmen) auch von sich aus verpflichtet, unrichtige Daten zu berichtigen.

Die Berichtigungspflicht besteht für unrichtige Daten, also solche Daten, die mit der Realität nicht übereinstimmen. Unrichtigkeit liegt jedoch nicht nur bei offenkundigen Fehlern vor, bei unrichtigen Adressen oder falschem Geburtsdatum, sondern auch bei einem so genannten Kontextverlust der Daten – wenn dieser so gravierend ist, dass Fehlinterpretationen zumindest wahrscheinlich sind.

Wird beispielsweise bei einem Arbeitnehmer nur die Summe der Fehlzeiten gespeichert, ohne dass nach den Gründen wie Krankheit, Urlaub, Weiterbildung und so weiter differenziert wird, führt dies zu falschen Vorstellungen über die Leistungsfähigkeit eines Arbeitnehmers. Dieses gilt ebenfalls für Werturteile, die auf falschen Tatsachen oder unangemessener Würdigung dieser Tatsachen beruhen. (Wobei grundsätzlich anzustreben ist, dass die Speiche-

rung von Werturteilen generell unterbleibt.)

Eine Berichtigung kann erfolgen, indem ...

... falsche durch ein richtige Datum ersetzt,
... ein Datum vervollständigt oder
... ein Datum ersatzlos gestrichen wird.

Wurden Daten regelmäßig an Dritte weitergegeben, hat die verantwortliche Stelle diese von der Berichtigung zu verständigen (§ 35 Abs. 6 BDSG). So kann die Stelle, an die Daten übermittelt werden, ebenfalls eine Berichtigung vornehmen.

Das Gesetz schreibt keine bestimmte Frist vor, innerhalb derer die Berichtigung zu erfolgen hat. In jedem Fall wird die Berichtigung so rechtzeitig erfolgen müssen, dass eine weitere Verarbeitung oder Nutzung der unrichtigen Daten nicht mehr stattfindet.

Löschung von Daten

Der Betroffene kann über sein Recht auf Berichtigung hinaus die Löschung seiner Daten verlangen (§ 35 Abs. 2 BDSG), wenn ...

... die Speicherung unzulässig war,
... die Richtigkeit besonderer Arten personenbezogener (sensitiver) Daten durch die speichernde Stelle nicht bewiesen werden kann oder
... die Daten nicht mehr erforderlich sind.

Eine unzulässige Speicherung liegt immer dann vor, wenn die Zulässigkeitsvoraussetzungen gemäß § 4 Abs. 1 BDSG nicht gegeben sind (wenn es also weder eine rechtliche Grundlage noch die Einwilligung des Betroffenen gibt). Insbesondere ist zu beachten, dass das novellierte BDSG zusätzlich zur Speicherung, Verarbeitung und Übermittlung jetzt auch die Daten*erhebung* mit einbezieht.

Nicht rechtmäßig sind Daten dann erhoben worden, wenn zum Beispiel der Arbeitgeber rechtlich unzulässige Fragen gestellt hat. Darüber hinaus ist die Speicherung auch dann unzulässig, wenn im Rahmen einer Arbeitnehmerbefragung ein Personalfragebogen eingesetzt, der Interessenvertretung aber das Mitbestimmungsrecht gemäß § 94 BetrVG verweigert wurde.

Dieses gilt in gleicher Weise für das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG in Bezug auf Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, Verhalten oder Leistung der Beschäftigten zu überwachen.

Besonders sensitive Daten, nämlich über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit, das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten, sind zu löschen, wenn ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann.

In vielen Fällen wird die Speicherung entsprechender Daten von vornherein unzulässig sein, da der Arbeitgeber nur in Ausnahmefällen danach fragen darf. Soweit der Arbeitgeber ausnahmsweise diese Daten speichern durfte, reicht es für einen Löschungsanspruch aus, wenn der Betroffene die Richtigkeit der gespeicherten Angaben bestreitet. Der Gesetzgeber hat mit dieser Regelung dem besonders sensiblen Charakter dieser Daten Rechnung getragen.

Eine Löschung kann zudem verlangt werden, wenn die Kenntnis der Daten für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist. Dieses kann sich sowohl auf Daten von erfolglos gebliebenen Bewerbern als auch um Daten von Beschäftigten oder auch ausgeschiedenen Arbeitnehmern beziehen.

Sperrung von Daten

Auch in Bezug auf den Löschungsanspruch sieht das BDSG Ausnahmen vor. In § 35 Abs. 3 BDSG werden dazu drei Alternativen genannt, bei denen die Daten nicht gelöscht, sondern in gesperrter Form weitergeführt werden dürfen oder müssen.

So tritt an die Stelle einer Löschung eine Sperrung, wenn ...

... einer Löschung gesetzliche, satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen (§ 35 Abs. 3 Nr. 1 BDSG),
... Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden (§ 35 Abs. 3 Nr. 2 BDSG) oder
... eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit verhältnismäßig hohem Aufwand möglich ist (§ 35 Abs. 3 Nr. 3 BDSG).

Zudem ist eine Sperrung vorgesehen, wenn die Richtigkeit gespeicherter Daten vom Betroffenen und der verantwortlichen Stelle (dem Unternehmen) unterschiedlich beurteilt wird und eine Klärung nicht zu erreichen ist. In § 35 Abs. 7 BDSG sind die Folgen aufgeführt, die für die verantwortliche Stelle mit der Sperrung von Daten verbunden sind. So ist die Übermittlung und Nutzung gesperrter Daten nur zulässig, wenn es zu wissenschaftlichen Zwecken unerlässlich, zur Behebung einer bestehenden Beweisnot oder aus sonstigen, im Interesse der verantwortliche Stelle oder eines Dritten liegenden Gründe unerlässlich ist. Voraussetzung hierfür ist allerdings, dass die Daten, wenn sie *nicht* gesperrt wären, genutzt und übermittelt werden dürften.

Recht auf Widerspruch

Die Benachrichtigungs- und Auskunftsrechte werden noch um ein Widerspruchsrecht ergänzt (§ 35 Abs. 5 BDSG). Dieses Recht erlaubt, dass der Betroffene in den Datenverarbeitungsprozess eingreifen kann, mit dem Ziel, die Verarbeitung – selbst in dem Fall, dass sie prinzipiell rechtmäßig ist – zu untersagen.

Das Widerspruchsrecht greift dann, wenn eine Prüfung des eingelegten Widerspruchs ergibt, dass das schutzwürdige Interesse des Betroffenen we-

gen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle (des Unternehmens) an der Erhebung, Verarbeitung oder Nutzung der Daten überwiegt. Das Widerspruchsrecht gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten verpflichtet. Das Recht auf Widerspruch wird auch dann zum Tragen kommen können, wenn der Betroffene vorher eine Einwilligung erteilt hat.

Da im Arbeitsleben aber Datenverarbeitung immer nur sehr eng an der Zweckbestimmung des Arbeitsvertragsverhältnisses erfolgen darf, ist fraglich, ob dieses Widerspruchsrecht oft zum Tragen kommen kann.

Verpflichtung auf das Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei Aufnahme der Tätigkeit auf das Datengeheimnis zu verpflichten. Dabei besteht das Datengeheimnis auch nach Beendigung der Tätigkeit fort (§ 5 BDSG).

Diese Vorschrift beinhaltet ein umfassendes gesetzliches Verbot unbefugter Datenverarbeitung. Der Begriffs ›unbefugt‹ meint, dass ›befugte Datenverarbeitung‹ nur diejenige ist, die sich nach den Bestimmungen des BDSG vollzieht. Eine Erhebung, Verarbeitung oder Nutzung ist also immer dann unbefugt, wenn sie zugleich auch rechtswidrig ist. Darunter sind alle Möglichkeiten der unzulässigen Verwendung von Daten zu verstehen, wie zum Beispiel:

- Auswertungen für eigene/private Zwecke;
- Bekanntgabe von Daten an Dritte ohne Rechtsgrundlage (etwa zum Zweck der Wirtschaftspionage);
- Herausgabe von Datenträgern an unbefugte Dritte;
- Entwendung von Datenträgern (etwa zum Zweck der Veräußerung sowie Verkauf von Kundendateien);
- einem Dritten Gelegenheit zu geben, damit dieser Daten abrufen oder Datenträger entwenden kann;
- unzulässiger Abruf von Daten.

Von einer Verpflichtung betroffen sind die »bei der Datenverarbeitung beschäftigten Personen«. In erster Linie sind dies die im DV-Bereich eingesetzten Mitarbeiter, aber auch diejenigen, die in den Fachabteilungen personenbezogene Daten verarbeiten. Die Verpflichtung selbst ist an keine besonderen Formvorschriften gebunden. Insbesondere eine zustimmende Erklärung dessen, der verpflichtet wird, ist nicht erforderlich

Es reicht allerdings nicht aus, die Verpflichtungserklärung durch Anhang an das schwarze Brett bekannt zu machen. Erforderlich ist vielmehr die Verpflichtung in jedem Einzelfall. Aus Beweissicherungsgründen sollte die Verpflichtung durch die Unterschrift des Betroffenen bestätigt werden.

Die Verpflichtung erfüllt nur dann ihren vom Gesetz beabsichtigten Zweck, wenn sie mit einer Unterweisung des Beschäftigten über seine besonderen Verpflichtungen nach dem BDSG verbunden sind. Die Mitteilung des Wortlautes des § 5 BDSG reicht nicht aus.

Der Beschäftigte kann sich bei einem Verstoß gegen das Datengeheimnis strafbar machen und sich Schadensersatzansprüchen aussetzen (§ 43 BDSG). Darüber hinaus können arbeitsvertragliche Sanktionen, wie Abmahnung oder Kündigung in Betracht kommen. Eine Kündigung des Arbeitsverhältnisses allerdings scheidet jedenfalls dann aus, wenn die fragliche Verletzung des Datengeheimnisses überwiegend durch den Arbeitgeber (z.B. auf Grund fehlerhafter Organisation) verursacht wurde.

Schadensersatzanspruch

Die §§ 7 und 8 BDSG enthalten eine eigenständige Anspruchsgrundlage für den Betroffenen (Beschäftigten), um gegenüber nicht-öffentlichen und öffentliche Stellen Schadensersatz geltend machen zu können.

Schadensersatzansprüche können geltend gemacht werden, wenn eine verantwortliche Stelle einem Betroffenen durch eine nach dem BDSG oder anderer Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zufügt (§ 7 BDSG). Dabei muss der Betroffene der datenverarbeitenden Stelle ein Verschulden *nicht* nachweisen. Denn in Anbetracht der komplexen, für außenstehende Dritte kaum nachvollziehbaren Vorgängen bei der automatisierten Verarbeitung kann es dem Betroffenen nicht zugemutet werden, dies gegenüber dem Betreiber der Datenverarbeitung zu tun.

Der für die Verarbeitung Verantwortliche kann von der Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann. In § 7 Satz 2 BDSG heißt es:

»Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.« § 8 BDSG enthält dem § 7 BDSG entsprechende Vorgaben, richtet sich aber ausschließlich an öffentliche Stellen, wobei hier zusätzlich die Höhe der Schadensersatzansprüche auf ca. 127 000 Euro begrenzt wird.

Bruno Schierbaum, Kontakt: Beratungsstelle für Technologiefolgen und Qualifizierung (ver.di) Niedersachsen in Oldenburg, Telefon 0 44 11 - 8 20 68, **schierbaum@btq.de**