► Smartphones sein oder in betrieblichen Netzen.

Auch der Ort,von dem aus auf Daten zugegriffen wird, ist nicht eindeutig festgelegt (im Prinzip ist das von jedem Internetcafe aus möglich). Und schließlich ist auch der Nutzungsumfang (die Nutzung der verschiedenen Funktionen) dynamisch, da er ja jederzeit über das Internet neu konfiguriert – also sowohl erweitert wie auch ganz anders zugeschnitten – werden kann. „Klassische" Betriebsvereinbarungen, die Auswertungen, Zugriffsrechte und zu verarbeitende Daten regeln, werden in diesem Umfeld wohl kaum funktionieren.

Da stellt sich natürlich die Frage, wie eine neue „Generation" von SAP-Vereinbarungen auszusehen hätte?

Nun, man muss als Berater nicht immer sofort eine Antwort haben und ich habe sie in diesem Fall auch nicht. Aber man kann und muss sagen, dass wir nach einer Antwort suchen müssen – dringend!

*Autor*

**Jochen Konrad-Klein** ist Berater bei der Technologieberatungsstelle (TBS) Nordrhein-Westfalen, jochen.konrad-klein@tbs-nrw.de, www.tbs-nrw.de

*Lexikon*

**SAP Business One** ► eine eigenständige Unternehmenssoftware von SAP speziell für kleinere Unternehmen

**SAP ERP** ► ERP (englisch: *enterprise resource planning* = Planung/Verwaltung der Unternehmensmittel) ist ein Sammelbegriff für betriebswirtschaftliche Unternehmenssoftware und die Bezeichnung für das aktuelle „große" SAP-Systeme (als Nachfolger für SAP R/3)

**Server** ► (englisch: *server* = Zusteller) Bezeichnung für einen speziellen Rechner, der in Netzwerken für die angeschlossene Arbeitsplatzrechner bestimmte Aufgaben übernimmt (z.B. Netzwerkverwaltung, Datenspeicherung, E-Mail-Abwicklung)

**Shareware** ► (englisch: *share* = teilen) Software, die zum Kennenlernen und Testen zunächst kostenlos zur Verfügung gestellt wird (meist übers Internet); für eine uneingeschränkte Nutzung muss dann aber eine kostenpflichtige Registrierung erfolgen

**Smartphone** ► (englisch: *smart* = gerissen, gewieft; *phone* = Telefon) mobiles Telefon/Handy, das auch über Funktionen eines mobilen Computers verfügt (z.B. Kalender, Adressammlung, Projektplanung, Datenbanken, Internetanschluss)

# Das Bundesdatenschutzauditgesetz

Bruno Schierbaum // BTQ Niedersachsen, Oldenburg

**Das Datenschutzaudit, also die systematische Analyse und Bewertung von Datenschutzkonzepten, -techniken und -maßnahmen, ist schon seit längerer Zeit ein Thema. Nun liegt der Entwurf eines Gesetzes vor, nämlich – Achtung: Wortungetüm! – des Bundesdatenschutzauditgesetzes (BDSAuditG). Ein Blick darauf kann auch für eine Belegschaftsvertretung nicht schaden …**

Mit der Novellierung des Bundesdatenschutzgesetzes im Jahr 2001 hatte der Gesetzgeber mit dem § 9a BDSG die Möglichkeit eines Datenschutzaudits bereits ins Gesetz eingefügt und eine Regelung der „näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter […] durch besonderes Gesetz" angekündigt.

Damit haben Unternehmen und andere datenverarbeitende Einrichtungen schon seit 2001 die Möglichkeit, sich freiwillig einem Datenschutzaudit zu unterziehen. Das allein aber reichte erwartungsgemäß nicht aus. Deshalb liegt nun für das „Bundesdatenschutzauditgesetz" (BDSAuditG) ein Referentenwurf vor, der im Internet unter www.datenschutzzentrum.de/bdsauditg/ abgerufen werden kann. Wobei auch dieses BDSAuditG das Datenschutzaudit immer noch nicht abschließend regelt – § 8 BDSAuditG sieht den Erlass weiterer Rechtsverordnungen vor …

## Datenschutzaudit

Anbieter von Datenverarbeitungssystemen und -programmen sowie alle datenverarbeitenden Stellen (Unternehmen, Behörden, Organisationen usw.) können auf Antrag ihr Datenschutzkonzept oder ihre Datenverarbeitungstechnik auf Vereinbarkeit mit den Datenschutzvorschriften prüfen und bewerten lassen (§ 1 Abs. 1 BDSAuditG). Eine solche Auditierung/Zertifizierung wird auf freiwilliger Basis erfolgen und kann bei zugelassenen Sachverständigen direkt in Auftrag gegeben werden. Die Einzelheiten dazu und auch Form und Verfahren der Auditierung sollen noch – wie schon erwähnt – durch Rechtsverordnungen geregelt werden (§ 8 BDSAuditG).

### DATENSCHUTZTAGUNG

Die BTQ Niedersachsen veranstaltet am **4.6.2008** in Hannover eine Fachtagung zum Thema „Arbeitnehmerdatenschutz – aktuell!" Darin geht es u.a. um Entwicklungen bei den digitalen Personalakten, um die Rolle, die das sogenannte „Verpfeifen" in Unternehmens-Leitlinien spielt und um Regelungen zur Videoüberwachung. Ergänzt werden diese Themen durch zahlreiche Praxisfälle aus den Tätigkeitsberichten der Landesbeauftragten. Informationen und Anmeldung unter:

BTQ Niedersachsen, fon 0441 82068 oder schierbaum@btq.de

## Sachverständige

Nach § 2 BDSAuditG wird die Zertifizierung durch Sachverständige durchgeführt, die von der Datenschutzaufsichtsbehörde eines Bundeslands öffentlich bestellt worden sind. Das Gesetz sieht zwar vor, dass die Sachverständigen nur in „ihrem" Bundesland tätig werden können, sie können sich aber auch von den Aufsichtsbehörden

mehrerer Bundesländer bestellen lassen. Trotzdem hat diese regionale Begrenzung zu Kritik geführt: Zum einen gebe es keinen guten Grund für diese räumliche Einschränkung der Tätigkeit und zum anderen stelle die Begrenzung eine unzulässige Beschränkung der Berufsausübung der Sachverständigen dar.

Nach welchen Kriterien die Bestellung/Abberufung eines Sachverständigen erfolgen kann und welche Sachkunde dafür verlangt wird, ist im Gesetzentwurf noch nicht festgelegt, sondern wird wohl erst in den ergänzenden Rechtsverordnungen geregelt werden.

## Zertifikat/Datenschutzsiegel

Wenn ein geprüftes Datenschutzkonzept oder eine technische Einrichtung mit den Vorschriften über den Datenschutz vereinbar ist, dann wird der Sachverständige dies in einem Zertifikat bestätigen. Ist dies nicht der Fall, wird er einen ablehnenden Bescheid erteilen.

Die zertifizierten Konzepte/Einrichtungen dürfen auch mit einem Datenschutzsiegel gekennzeichnet werden, das eine Gültigkeit von maximal zwei Jahren haben wird. Auch hier wird Näheres noch im Rahmen von Rechtsverordnungen geregelt werden.

Nach § 1 Abs. 3 BDSAuditG soll übrigens die Bewertung der Sicherheit von IKT-Systemen und -Komponenten vom Datenschutzaudit ausgenommen sein. Damit wollte der Gesetzgeber wohl eine Abgrenzung zu den Sicherheitszertifizierungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) vornehmen.

Allerdings stellt sich hier die Frage, inwieweit die nach § 9 BDSG vorgesehenen „technischen und organisatorischen Maßnahmen" zum Datenschutz im Rahmen des Datenschutzaudits geprüft werden können und sollen? Bei den dort vorgeschriebenen Maßnahmen wäre eine Abgrenzung zwischen solchen, die dem Datenschutz, und solchen, die der Datensicherheit dienen, nämlich schlichtweg unmöglich.

## Datenschutzauditregister

Der Bundesdatenschutzbeauftragte (genau: der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) soll zu den Auditierungen ein öffentliches Register führen, das über das Internet einsehbar sein wird. In diesem Register sollen unter anderem die zertifizierten Konzepte, Maßnahmen usw. mit Anschrift des Antragstellers (z.B. eines Unternehmens) sowie die Dauer der Zertifizierung (und auch des eventuell vergebenen Siegels) dokumentiert werden.

## Rücknahme und Widerruf

Für Rücknahme oder Widerruf einer Zertifizierung ist die Datenschutzaufsichtsbehörde (z.B. der Landesdatenschutzbeauftragte) zuständig, die den Sachverständigen bestellt hat. Die Aufsichtsbehörde holt vorher eine Stellungnahme des Sachverständigen ein. Wie es zu einem solchen Rücknahme-/Widerrufsverfahren kommen kann, ist im Entwurf allerdings vorerst nicht geregelt.

## Fazit

Die bisher noch nicht einmal im Entwurf vorliegenden Rechtsverordnungen zum BDSAuditG sind natürlich entscheidende Voraussetzungen für die konkrete Umsetzung der Datenschutzaudits in die Praxis. Und wenn diese ebenso lange auf sich warten lassen, wie der jetzt vorliegende Entwurf für das Gesetz selbst, wird es mit Datenschutzaudits in absehbarer Zeit wohl nichts werden.

Dabei wäre eine zügige Verabschiedung des BDSAuditG und natürlich auch der dazugehörenden Rechtsverordnungen sehr zu wünschen, weil dadurch der Datenschutz in der betrieblichen Praxis weiter an Bedeutung gewinnen würde.

*Autor*

**Bruno Schierbaum** ist Technologie- und Datenschutzberater bei der BTQ Niedersachsen, Donnerschweerstraße 84, 26123 Oldenburg, fon 0441 82068, schierbaum@btq.de, www.btq.de