Dirk Fox

Compliance und Datenschutz

Im Kontext verschärfter interner Kontroll- und Transparenzmaßnahmen börsennotierter Unternehmen kommt es in vielen Firmen zur Diskussion über die Abgrenzung der Zuständigkeiten und Befugnisse von Compliance-Officer und betrieblichem Datenschutzbeauftragten. Der folgende Beitrag unternimmt den Versuch einer Antwort.

Hintergrund

Die betrügerischen und skandalösen Bilanzmanipulationen der amerikanischen Unternehmen Enron (2001 eines der zehn größten Unternehmen der USA) und Worldcom (damals drittgrößte Telekommunikationsgesellschaft der Welt) endeten im Dezember 2001 bzw. Juli 2002 in der Insolvenz. Sie lösten in den USA eine drastische Verschärfung der Kontrollen börsennotierter Unternehmen zum Schutz der Aktionäre aus – die weit über die USA hinaus Auswirkungen zeitigte.

Eine der unmittelbaren Folgen der Skandale war der am 30.07.2002 in Kraft getretene „Sarbanes-Oxley Act" (SOX), benannt nach seinen Verfassern, den US-Senatoren Paul S. Sarbanes und Michael Oxley. SOX enthält zahlreiche Verpflichtungen wie die Einführung eines „Whistleblowing"-Systems, Regelungen zur Unabhängigkeit und Haftung der Wirtschaftsprüfer und erweiterte Offenlegungspflichten, durch die das Vertrauen von Anlegern in die Verlässlichkeit veröffentlichter Finanzdaten börsennotierter Unternehmen wiederhergestellt werden soll. Damit erfuhr der betriebswirtschaftliche Begriff „Compliance" eine erhebliche Aufwertung. Denn die Ordnungsgemäßheit der Jahresabschlüsse muss von CEO und CFO (Vorstandsvorsitzendem und Finanzvorstand) durch eidesstattliche Erklärung bestätigt werden – bei Verstößen drohen persönliche Haftung und verschärfte Strafvorschriften. Betroffen sind auch nicht-amerikanische Unternehmen, die an einer US-Börse gelistet sind; sie mussten die SOX-Bestimmungen bis Juli 2006 umsetzen.

Mit SOX gewann konsequenter Weise auch die Einhaltung zahlreicher anderer rechtlicher Verpflichtungen von Unternehmen an Gewicht, da das Vertrauen der Anleger und Finanzmärkte in ein Unternehmen auch bei der Aufdeckung anderer rechtlicher Verstöße beschädigt werden kann.

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.

E-Mail: dirk.fox@secorvo.de

Was ist „Compliance"?

Tatsächlich ist der Begriff keineswegs neu; nicht zuletzt im Zusammenhang mit den Anforderungen des Geldwäschegesetzes (GWG) spielte Compliance insbesondere in Kreditinstituten schon lange vor SOX eine wichtige Rolle.

Konzentriert man sich auf seriöse Veröffentlichungen, so wird dort – über die rein betriebswirtschaftliche Bedeutung hinaus – unter „Compliance" die Einhaltung aller relevanten Gesetze, Verordnungen, Richtlinien und Selbstverpflichtungen durch ein Unternehmen als Ganzes verstanden. Dazu können auch ethische Kodizes gehören.

Somit ist Compliance einerseits eine Selbstverständlichkeit – denn zur Einhaltung geltender Gesetze und Verordnungen ist natürlich jedes Unternehmen verpflichtet. Andererseits verdeutlicht das Bekenntnis zu den dahinter stehenden Prinzipien und die Initiierung von Compliance-Maßnahmen den Willen des Unternehmens (genauer: der Unternehmensleitung), auch für eine konsequente Umsetzung der gesetzlichen Anforderungen und Selbstverpflichtungen zu sorgen.

Compliance-Treiber

Die Compliance-Anforderungen, die an ein Unternehmen gestellt werden, können sich im Detail von Unternehmen zu Unternehmen erheblich unterscheiden. So müssen Anbieter von Telekommunikationsdiensten – darunter fallen auch Unternehmen, die ihren Mitarbeitern die Privatnutzung von Telefon, Internet oder E-Mail erlauben oder diese dulden – das Telekommunikationsgesetz (TKG) einhalten und unterliegen insbesondere strengen Schutz- und Löschvorschriften hinsichtlich der von ihnen verarbeiteten Kommunikationsinhalten und TK-Verbindungsdaten. Deutsche Kreditinstitute wiederum sind insbesondere an das Kreditwesengesetz (KWG), das Geldwäschegesetz (GWG) sowie an die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erlassenen Verordnungen wie die „Mindestanforderungen an das Risikomanagement" (MaRisk) gebunden. Kapitalgesellschaften haben außerdem die Bestimmungen des Aktiengesetzes bzw. des GmbH-Gesetzes, darunter die Bestimmungen des „Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich" (KonTraG) zu beachten. Gemeinsam ist wenigstens allen deutschen Unternehmen die Pflicht zur Einhaltung der „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme" (GoBS), im Falle digitaler Rechnungslegung und elektronischer Buchhaltungssysteme der „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPdU), sowie des Bundesdatenschutzgesetzes (BDSG).

Ebenso wie sich die konkreten Compliance-Anforderungen unterscheiden, die unter anderem von der Branche, der internationalen Aufstellung des Unternehmens, der Rechtsform und einer eventuellen Börsennotierung abhängen, sind auch

die „Treiber" verschieden, die dem Thema Compliance in einem Unternehmen Gewicht verleihen.

So stehen in den meisten börsennotierten Unternehmen die Anforderungen an das Risikomanagement in Kapitalgesellschaften und die Informationspflichten gegenüber den Aktionären an erster Stelle, gefolgt von Korruptionsprävention, Strafzahlungen bei Wettbewerbsverstößen und dem Schutz der Unternehmensleitung vor Haftungsrisiken.

Auch wenig kalkulierbare Risiken wie die Furcht vor Image-Schäden oder die öffentliche Macht von Verbraucherschutzverbänden können wichtige Treiber sein. Bei jungen, schnell wachsenden Unternehmen oder in Konsolidierungsphasen können in einzelnen Märkten auch „Due Dilligence"-Prüfungen eine Rolle spielen.

Umsetzung von Compliance

Um Compliance zu erreichen, ist ein regelkonformes Verhalten *aller* Mitarbeiter erforderlich. Dabei kommt Führungskräften aufgrund ihres größeren Einflusses und ihrer Vorbildfunktion eine besondere Verantwortung zu. Will man eine solche Übereinstimmung zwischen Anspruch (gesetzliche Anforderungen) und Unternehmenswirklichkeit (tatsächliches Verhalten der Mitarbeiter) erreichen, ist dreierlei erforderlich:

- die Etablierung von Informations- und Sensibilisierungsmaßnahmen,
- die Einführung von Kontroll- und Überwachungsmaßnahmen sowie
- eine unmittelbare Sanktionierung aufgedeckter Verstöße.

Geeignete Compliance-Maßnahmen sollen einen präventiven Schutz vor Fehlverhalten bewirken – sowohl vor bewussten Verstößen als auch vor solchen aus Unwissenheit oder Fahrlässigkeit. Ein zentrales Element der Überwachungsmaßnahmen ist vor allem bei von SOX betroffenen Unternehmen die Einrichtung eines – anonymen – Meldesystems, einer so genannten „Whistleblowing-Hotline"[1].

Compliance-Maßnahmen lassen sich verstehen als ein konsequenter Ausfluss der Sorgfaltspflicht:[2] Die Geschäftsleitung muss die sich aus rechtlichen Anforderungen ergebenden Aufgaben erkennen, deren Umsetzung organisieren – und schließlich das Ergebnis kontrollieren. Dabei kann die Umsetzung delegiert werden (und wird es in der Regel auch) – z. B. an einen Compliance-Beauftragten. Diese Delegation befreit die Geschäftsleitung nicht von der Pflicht, die Delegation an eine geeignete Person mit einer klaren Aufgabenbeschreibung vorzunehmen – und regelmäßig die Aufgabenerfüllung zu kontrollieren.

Compliance vs. Datenschutz

Mit der Ernennung eines Compliance-Beauftragten ergibt sich in deutschen Unternehmen in der Praxis unvermeidlich ein Abgrenzungsproblem zu den Aufgaben des betrieblichen Datenschutzbeauftragten (bDSB). Nicht selten führt dies zu Konflikten – die sich bei genauer Betrachtung der Rollen und Aufgaben beider Funktionen vermeiden ließen.

Denn die Funktion und Aufgabe des bDSB ist klar gesetzlich geregelt: „Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin." (§ 4g (1) BDSG). Die Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften durch das Unternehmen verbleibt dabei bei der Unternehmensleitung. Konkret umfassen die gesetzlichen Aufgaben des bDSB (§ 4g BDSG)

- die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden,
- die Information und Schulung der bei der Verarbeitung personenbezogener Daten tätigen Personen über die Vorschriften des BDSG und anderer datenschutzrechtlicher Vorschriften,
- die Erteilung der Jedermann-Auskunft auf der Basis des Verfahrensregisters,
- den Erhalt seiner Fachkunde und
- die Durchführung von Vorabkontrollen (§ 4d (5) BDSG).

Der bDSB ist der Geschäftsleitung direkt unterstellt und in der Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei (§ 4f (3) BDSG). Dabei verfügt der bDSB über keine Weisungsbefugnis – sein Instrumentarium sind die Aufklärung, Sensibilisierung, Überzeugung und schließlich der Bericht an die Unternehmensleitung. Gegebenenfalls muss er sich in Zweifelsfällen, wie z. B. bei der Vorabkontrolle, an die zuständige Aufsichtsbehörde wenden.

Ganz anders die Aufgabe des Compliance-Beauftragten: Er ist zuständig für die *Sicherstellung der Einhaltung* gesetzlicher Anforderungen. Daher zielt seine Tätigkeit weniger auf Motivation denn auf Kontrolle: Zwar muss auch der Compliance-Beauftragte die Mitarbeiter über die gesetzlichen Anforderungen informieren – hier überschneiden sich die Aufgaben von Compliance- und Datenschutzbeauftragtem tatsächlich –, seine Kernaufgabe ist jedoch die Umsetzungskontrolle.

Während der bDSB zur Verschwiegenheit hinsichtlich der Identität Betroffener verpflichtet ist, ist es Aufgabe des Compliance-Beauftragten, Fehlverhalten festzustellen, zu korrigieren und erforderlichenfalls für die Sanktionierung der Verantwortlichen zu sorgen.

Besonders deutlich wird der Unterschied, wenn man einzelne datenschutzrechtliche Verpflichtungen des Unternehmens betrachtet. Während der bDSB beispielsweise die Etablierung eines Prozesses empfiehlt, durch den neue Mitarbeiter zunächst informiert, eingewiesen und dann auf das Datengeheimnis verpflichtet werden, interessiert den Compliance-Beauftragten im Kern, ob

- die Vollständigkeit der unterzeichneten Verpflichtungserklärungen regelmäßig überprüft,
- fehlende Verpflichtungserklärungen kurzfristig eingeholt und
- Fehler in den zugehörigen Prozessen, die zur Unvollständigkeit geführt haben, umgehend korrigiert werden.

Auch hinsichtlich der korrekten Gestaltung der Auftragsdatenverarbeitung wird der Unterschied deutlich: Während der bDSB auf die Formulierung und Einfüh-

1 Zu den datenschutzrechtlichen Implikationen siehe auch Schmiedl, „Datenschutz für Whistleblowing-Hotlines", DuD 6/2006, S. 353 ff.; „Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität", Art. 29 Gruppe, WP 117, 00195/06/DE, vom 14.02.2006; „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz", Arbeitsbericht der Ad-hoc-Arbeitsgruppe Beschäftigtendatenschutz des Düsseldorfer Kreises vom 27.04.2007; „Whistleblowing – Chancen und Risiken bei der Umsetzung von anonym nutzbaren Hinweisgebersystemen im Rahmen des Compliance-Managements von Unternehmen", Astrid Breinlinger/Gabriela Krader, RDV 2/2006.

2 „Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden", § 43 (1) GmbHG; „Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden", § 93 (1) AktG.

rung einer Vertragsvorlage zur Auftragsdatenverarbeitung hinwirkt, fordert der Compliance-Beauftragte eine systematische Überprüfung anhand einer Checkliste und die revisionssichere Dokumentation des Prüfergebnisses. Während der Datenschutzbeauftragte „sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen" hat, bleibt dem Compliance-Beauftragten keine Alternative zum Audit, mit dessen dokumentiertem Ergebnis er die Überprüfung der Einhaltung der Schutzmaßnahmen auch gegenüber Dritten belegen kann.

Richtig verstanden wird damit der Compliance-Beauftragte zum perfekten Pendant des bDSB: Während der Datenschutzbeauftragte Motivations- und Überzeugungsarbeit zur frühzeitigen Berücksichtigung und Umsetzung datenschutzrechtlicher Erfordernisse leistet und beratend bei der Gestaltung mitwirkt, sorgt der Compliance-Beauftragte mit einem regelmäßigen Umsetzungsaudit für die Umsetzungskontrolle.

Der Datenschutzbericht

In diesem Lichte betrachtet lässt sich auch eine weitere „alte" Frage des betrieblichen Datenschutzes sinnvoll beantworten. So ist in § 4f (3) BDSG der Berichtsweg des betrieblichen Datenschutzbeauftragten (bDSB) eindeutig festgelegt: „Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nichtöffentlichen Stelle unmittelbar zu unterstellen." Damit steht außer Frage, dass der bDSB direkt an die Geschäftsleitung berichtet. Was aber soll er berichten? Schriftlich oder mündlich? Und wie häufig?

Die Beantwortung dieser Fragen überlässt das BDSG dem Datenschutzbeauftragten – denn er „ist in der Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei." (§ 4f (3) BDSG). Tatsächlich gibt es zu einem schriftlichen Bericht keine Alternative – denn das ist (abgesehen von einer Kontaktaufnahme mit der Datenschutz-Aufsichtsbehörde) das einzige Instrument, das dem bDSB bleibt, wenn es ihm nicht gelingt, das datenschutzrechtlich Gebotene mit Überzeugungsarbeit zu bewirken.

Bei der Strukturierung und inhaltlichen Ausrichtung des Datenschutz-Berichts orientieren sich in der Praxis einige betriebliche Datenschutzbeauftragte an den Tätigkeitsberichten der Landes- und des Bundesdatenschutzbeauftragten. Das führte in der Vergangenheit gelegentlich zu eigenwilligen Stilblüten, wenn sich im Bericht eines betrieblichen DSB im nichtöffentlichen Bereich Abschnitte zum „Datenschutz im Internetzeitalter" fanden.

Oft ist auch schon der Name Programm: Gelegentlich ist Struktur, Stil und Inhalt eines „Tätigkeitsberichts" zu entnehmen, dass der Datenschutzbeauftragte ihn – möglicherweise unterschwellig – als „Rechtfertigungsbericht" versteht, der der Unternehmensleitung die Frage beantworten soll, was der Datenschutzbeauftragte denn während seiner Arbeitszeit so getrieben hat. Manchmal haben Berichte auch eher den Charakter eines „Erlebnisberichts".

In vielen Fällen ist die Frage, welchem Zweck der Datenschutzbericht dient (oder dienen soll), vom betrieblichen Datenschutzbeauftragten vorab nicht oder zumindest nicht eindeutig beantwortet – und erschließt sich dem Leser konsequenter Weise daher auch nicht nach der Lektüre. Dabei lässt sich aus Compliance-Perspektive der Zweck eines – schriftlichen! – Berichts an die Geschäftsleitung sehr einfach und klar definieren: Er dokumentiert

- die Sorgfalt des bestellten Datenschutzbeauftragten bei der Umsetzung seiner gesetzlichen Aufgaben und
- die Erfüllung datenschutzrechtlicher Pflichten durch das Unternehmen.

Aus einer solchen Zweckbestimmung lässt sich geradezu zwingend die Gliederung eines Datenschutzberichts ableiten: Er sollte sich orientieren an den konkreten datenschutzrechtlichen Grundpflichten, die ein Unternehmen zu erfüllen hat. Die Gliederung sollte daher die folgenden Punkte umfassen:

- Schulung und Information der Mitarbeiter im Umgang mit personenbezogenen Daten
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- gDokumentations- und Aktualitätsstand des Verfahrensregisters
- Zulässigkeitsprüfungen automatisierter Verarbeitungen
- Ordnungsgemäßheit der Verarbeitung
  - Festlegung und Einhaltung von Löschfristen
  - Organisatorische und technische Schutzmaßnahmen
  - Übermittlung personenbezogener Daten in Drittstaaten
  - Datenverarbeitung im Auftrag
- Auskunftsersuchen
- Sonderfälle
  - Vorabkontrolle
  - Videoüberwachung

Inhaltlich darf die Darstellung weder beschönigen noch weglassen, denn die Ergebnisse müssen auf realistische Weise die Unternehmenswirklichkeit widerspiegeln. Einfließen sollten dabei auch die Ergebnisse etwaiger Audits, die von der internen Revision oder dem Compliance-Beauftragten zu Datenschutzaspekten durchgeführt wurden.

Für die Unternehmensleitung müssen sich daraus sowohl Compliance-Verstöße als auch ein etwaiger unmittelbarer Handlungsbedarf erkennen und ableiten lassen. Ein „Management Summary", das diese Folgerungen zusammenfasst, sollte dem Bericht daher vorangestellt werden.

Fazit

Bei genauerem Hinsehen entpuppt sich der vermeintliche Konflikt zwischen den Kompetenzen und Zuständigkeiten des Compliance- und des Datenschutzbeauftragten als Glücksfall, denn die schon im Ansatz gänzlich unterschiedlichen Rollen der beiden Beauftragten können sich in der Praxis hervorragend ergänzen.

So wirkt der betriebliche Datenschutzbeauftragte durch Information, Aufklärung und Überzeugungsarbeit auf die Umsetzung datenschutzrechtlicher Erfordernisse im Unternehmen hin, währen der Compliance-Beauftragte das Ergebnis einem aussagekräftigen Kontrollverfahren unterzieht und für eine Korrektur etwaiger festgestellter Mängel sorgt. Dafür wird er in der Regel auf die fachliche Unterstützung durch den Datenschutzbeauftragten angewiesen sein, z. B. bei der Erstellung geeigneter Checklisten und sinnvoller Kontrollmethoden.

Ein regelmäßiger, beispielsweise jährlicher schriftlicher Bericht des bDSB ist grundsätzlich zu empfehlen; er kann die Grundlage für ausgewählte Schwerpunktkontrollen bilden.

Allein bei Information und Aufklärung (Schulung und Einweisung) der Mitarbeiter in Datenschutzfragen sind beide Beauftragte gefordert – und können sich dabei gegenseitig unterstützen.