

# Enthftung durch Zertifizierung?

Maria Winkler

**O**ffensichtlich ist die Frage, welche Anforderungen an Unternehmen bzw. deren Führungskräfte bezüglich der Einhaltung von Gesetzen, Normen und Weisungen gestellt werden, nicht so einfach zu beantworten. Das Bewusstsein, für die Gesetzeskonformität des unternehmerischen Handelns verantwortlich zu sein, wurde bei den Führungskräften in den letzten Jahren geschärft durch Wirtschaftsskandale und deren Folgen für die betroffenen Manager. Durch den Erwerb von Zertifikaten für einzelne Geschäftsbereiche, für konkrete Abläufe oder für das gesamte Unternehmen kann im Zusammenhang mit Gesetzeskonformität sehr vieles erreicht werden. Inwieweit eine Zertifizierung die verantwortlichen Personen von ihrer Verantwortung befreien kann, soll im Folgenden erörtert werden.

## Abstrakte Gesetze schaffen Unsicherheit

Nicht zuletzt wegen der wachsenden Technologieabhängigkeit zahlreicher Branchen wird die Regelungsdichte immer grösser. Insbesondere die immer stärkere Durchdringung aller Lebensbereiche mit den Mitteln und Möglichkeiten der Informationstechnologie zwingt den Gesetzgeber neue Normen zu schaffen, um neu entstandene Regelungslücken zu füllen und um Rechtssicherheit zu schaffen. Beispiele für diese Entwicklung finden sich in grosser Zahl. So wurden die Voraussetzungen der elektronischen Rechnungstellung durch die Verordnung des EFD über elektronisch übermittelte Daten und Informationen (ELDI-V) auf den 17. September

**Sucht man in Google nach «Compliance», dann stösst man innerhalb von 0,26 Sekunden auf hunderttausende von Einträgen – und dies nur auf schweizerischen Websites. Viele davon betreffen Beratungen, Seminare und Publikationen, wie denn nun Compliance tatsächlich erreicht und erhalten werden kann.**

2007 neu geregelt. Die auf den 1. Januar 2008 in Kraft getretenen Vorschriften des revidierten Datenschutzgesetzes schaffen unter anderem die Möglichkeit, die meldepflichtigen Datensammlungen neu auch über das Internet dem EDÖB zu melden. Gerade gesetzliche Regelungen, welche auf technische Rahmenbedingungen Bezug nehmen oder von technischen Entwicklungen stark beeinflusst werden, sind allerdings meist nur sehr allgemein formuliert. Schliesslich soll eine einmal erlassene Regelung nicht bei der nächsten technologischen Neuerung wieder angepasst werden müssen. Dies hat aber zur Folge, dass Unternehmen nicht nur immer mehr neue Gesetze beachten müssen, sondern auch, dass sie sich bei der Umsetzung der abstrakten Vorschriften oft nicht auf umfangreiche Literatur und Rechtsprechung stützen können, wie dies bei den älteren Normen der Fall ist.

## Macht bringt auch Verantwortung

Grundsätzlich ist in einem Unternehmen jeder Arbeitnehmer dafür verantwortlich, seine Aufgaben mit der grössten Sorgfalt und im Interesse des Arbeitgebers auszuüben. Verletzt ein Arbeitnehmer diese Pflicht, fahrlässig oder absichtlich, und verursacht er deshalb dem Arbeitgeber einen Schaden, so kann der Arbeitgeber gegen ihn Regress nehmen. Je nach Ausbildung, Erfahrung und Funktion im Unternehmen wird im Rahmen dieser Sorgfaltspflicht mehr oder weniger verlangt – und je nachdem besteht auch ein höheres oder ein geringeres Haftungsrisiko. Die Mitglieder des Verwaltungsrats und der Geschäftsleitung tragen grundsätzlich

auf Grund ihrer Organstellung mehr Verantwortung und das Risiko, bei einer Verletzung ihrer Sorgfaltspflichten auch mit dem privaten Vermögen zu haften.

Die Verantwortung für die Einhaltung der Gesetze, Statuten, Reglemente und Weisungen im Unternehmen liegt gemäss Gesetz letztendlich beim Verwaltungsrat. Dieser hat die Geschäftsführung entsprechend zu kontrollieren und er muss zudem dafür sorgen, dass genügend Informationen an ihn gelangen, um seine Aufgaben erfüllen zu können. Er ist nicht befugt, diese Aufgabe zu delegieren. Verwaltungsrat und Geschäftsführung müssen bei der Erfüllung ihrer Pflichten mit aller gebotenen Sorgfalt vorgehen und die Interessen des Unternehmens optimal vertreten. Dazu gehört nicht nur die Auswahl geeigneter Personen, sondern auch die Zurverfügungstellung der nötigen Ressourcen und Informationen sowie die Kontrolle der Einhaltung der Vorgaben.

Die Frage, welche Massnahmen eine ordnungsgemäss handelnde Person bei der Umsetzung von gesetzlichen Anforderungen konkret ergreifen würde, ist somit gleichermassen schwierig zu beantworten wie sie für die betroffenen Entscheidungsträger wichtig ist.

## Zunehmende Bedeutung der Selbstregulierung

Kein Wunder also, dass bei der Umsetzung solch abstrakter rechtlicher Normen nach allgemein anerkannten Standards gesucht wird. Durch die Umsetzung von Standards sowie durch den Erwerb von Zertifikaten und Labels erhoffen sich die Unterneh-



men, nachweisen zu können, dass sie den gesetzlichen Anforderungen genügen. Die Führungskräfte erhoffen sich eine Befreiung von ihrer Haftung.

Aber auch der Gesetzgeber selbst verweist immer häufiger auf das Instrument der Selbstregulierung. So verweist Art. 2 der Geschäftsbücherverordnung bei der Auslegung der durch die Unternehmen zu beachtenden Grundsätze der «ordnungsgemässen Buchführung» und der «ordnungsgemässen Datenverarbeitung» auf «allgemein anerkannte Regelwerke und Fachempfehlungen». Im Bereich des Datenschutzes soll durch die neu auf den 1. Januar 2008 in Kraft getretenen Vorschriften die Selbstregulierung und damit der Datenschutz und die Datensicherheit gefördert werden, indem Datenschutz-Zertifikate erworben werden können, welche vom EDÖB anerkannt sind. Bei der Regelung technologischer Fragen wird zudem häufig auf den «aktuellen Stand der Wissenschaft und

Technik» verwiesen, was beispielsweise im Bereich der Informationssicherheit bedeutet, dass man allgemein anerkannte Normen wie das BSI-Grundschutzhandbuch oder die ISO-Norm 27001:2005 einzuhalten hat.

### Möglichkeiten und Grenzen der Reduktion der Führungsverantwortung

Selbstregulierung ergänzt somit immer häufiger die Regulierung. Welche Bedeutung hat sie aber für die Frage der Verantwortung der Führungsorgane eines Unternehmens? Ist mit dem Erwerb eines ISO-Zertifikats bereits jegliches Haftungsrisiko eliminiert?

Im Rahmen der Zertifizierung eines Unternehmens oder einzelner Bereiche oder von Abläufen im Unternehmen, müssen zunächst alle für die Zertifizierung relevanten Informationen dokumentiert werden, damit diese überhaupt von einer unabhängigen Zertifi-

zierungsstelle überprüft werden können. Die internationalen Zertifikate und Normen enthalten meist auch Kontrollmechanismen, welche implementiert und regelmässig angewandt werden müssen. So verlangt die ISO-Norm 9001:2000, dass die Wirksamkeit und die Zweckmässigkeit des Qualitätsmanagementsystems durch regelmässige Management-Reviews überprüft wird. Das Datenschutz-Label GoodPrivacy verlangt nicht nur, dass die datenschutzrelevanten Objekte erfasst und bewertet werden, sondern auch, dass Verfahren zur Überwachung und Messung der für den Datenschutz und die Informationssicherheit relevanten Tätigkeiten eingeführt werden. Zudem muss ein Verfahren bestehen, das sicherstellt, dass Verstösse festgehalten und Korrektur- und Vorbeugemassnahmen eingeleitet werden.

Das Erfüllen dieser Normvorgaben kann aber durch die Zertifizierungsstelle immer nur für den Zeitpunkt bestätigt werden, in dem die Überprüfung stattfand. Es handelt sich also bei der Zertifizierung immer nur um eine Momentaufnahme – dass das Unternehmen sich dann bis zur nächsten Überprüfung auch an die Vorgaben hält, kann mit einem Zertifikat nicht gewährleistet werden. Dies muss vielmehr durch die verantwortlichen Personen im Unternehmen als Daueraufgabe sichergestellt werden.

Mit dem Erwerb eines Zertifikats verpflichtet sich die Führungsebene des Unternehmens nicht nur, sich an die – zum Teil über die gesetzlichen Mindestanforderungen hinausgehenden – allgemein anerkannten Vorgaben zu halten, sondern auch dazu, dies regelmässig von unabhängigen Stellen überprüfen zu lassen. Eine erfolgreiche Zertifizierung kann somit als Hinweis darauf gewertet werden, dass die verantwortlichen Personen im Unternehmen ihre diesbezüglichen Pflichten wahrnehmen. Wenn allerdings Fehler passieren, welche darauf zurückzuführen sind, dass die Kontrollmechanismen, welche gemäss Zertifikat vorhanden und implementiert sind, in der Realität nicht angewandt werden, dann vermag auch ein Zertifikat nichts an der Haftung der verantwortlichen Führungskraft zu ändern. ■