Corporate Compliance Checklisten

Rechtliche Risiken im Unternehmen erkennen und vermeiden

Herausgegeben von

RA Dr. Karsten Umnuß
FA für Arbeitsrecht

Mit einer Einführung von
RA Dr. Christoph E. Hauschka

Bearbeitet von
RA Dr. Ansgar Becker, FA für Steuerrecht
Dipl.-Region.-Wiss. Claus Cammerer
RA Christian Dworschak, FA für Arbeitsrecht
RA Dr. Gernot-Rüdiger Engel
RA Eike Fietz
RAin Dr. Nicole Franke
RA Dr. Thomas Kapp, LL.M.
RA und StB Dr. Hanno Kiesel
RA Christian Kuß, LL.M.
RA Dr. Markus Lohmeier
RAin Dagmar Noll
RA Dr. Michael Rath, FA für IT-Recht
RA Boris Salzmann, LL.M.
RA Volker Schlegel, Botschafter, Staatsrat a. D.
RAin Claudia Schoppen
RA Dr. Volker Schulenburg, FA für Handels- und Gesellschaftsrecht
RAin Sima Shahhosseini
RA Dr. Karsten Umnuß, FA für Arbeitsrecht
RAin Dr. Ulrike Unger; FAin für Handels- und Gesellschaftsrecht
RA Reinhard Willemsen

3., neu bearbeitete Auflage 2016

C.H.BECK

8. Kapitel. IT-Compliance: Anforderungen an die Informationstechnologie und den Datenschutz

Literatur:

Geercken/Holden/Rath/Surguy/Stretton, Cross Border E-Discovery, CRi 2010, 65–74; *Grützmacher,* Lizenzgestaltung für neue Nutzungsformen im Licht von § 69d UrhG (Teil 1), CR 2011, 485; *Grützmacher,* Lizenzgestaltung für neue Nutzungsformen im Licht von § 69d UrhG (Teil 2), CR 2011, 697; *Härting,* CR 2007, 311; *Hauschka,* ZRP 2006, 258 ff.; *Heckmann,* MMR 2006, 280 ff.; *Huppertz/Schneider,* Software-Lizenzaudits im Unternehmen, ZD 2013, 427; *Intveen,* Softwarelizenzaudits aus Anwendersicht, ITRB 2012, 208; *Intveen/Karger,* Erfolgreiche Durchführung von Software-Audits, ITRB 2014, 39; *Kotthoff/Wieczorek,* Rechtsrahmen von Softwarelizenzaudits, MMR 2014, 3; *Ohrtmann/Kuß,* Der digitale Flohmarkt, BB 2012, 2262; *Rath,* Hinweise zur Ausgestaltung von Service Level Agreements, K&R 2007, 362–366; *Rath/Karner,* Internetnutzung und Datenschutz am Arbeitsplatz, K&R 2010, 469–475; *Rath/Karner,* Private Internetnutzung am Arbeitsplatz – Rechtliche Zulässigkeit und Kontrollmöglichkeiten des Arbeitgebers, K&R 2007, 446–452; *Rath/Klug,* E-Discovery in Germany, K&R 2008, 596–600; *Rath/Kuß/Bach,* Das neue IT-Sicherheitsgesetz, K&R 2015, 437; *Rath/Maiworm,* Weg frei für Second-Hand-Software?, WRP 2012, 1051; *Rath/Sponholz,* IT-Compliance, 2. Aufl. 2014; *Roth/Schneider,* ITRB 2005, 19 ff.; *Schrey/Krupna,* Softwarelizenzmanagement, CCZ 2012, 141; *Steger,* CR 2007, 137 ff.; *Strittmatter/Harnos,* Softwareaudits, CR 2013, 621.

A. Einführung

Angesichts der stetig zunehmenden Komplexität von Geschäftsprozessen in einem Unternehmen und der Abhängigkeit des Unternehmens vom Funktionieren der EDV ist die Steuerung eines Unternehmens ohne den Einsatz von Informationstechnologie (IT) nicht mehr vorstellbar. Corporate Governance und Compliance sind damit untrennbar mit IT-Compliance verbunden, also dem verantwortungsvollen Umgang mit allen Aspekten von IT. Der Begriff IT-Compliance reicht dabei von der Einhaltung von Datenschutz und der Sicherstellung von IT-Sicherheit über den rechtskonformen Umgang mit Lizenzen bis hin zur gesetzeskonformen E-Mail-Archivierung und Kontrolle der IT-Nutzung der Mitarbeiter. Angesichts der Komplexität von IT-Compliance und der zugehörigen Anforderungen werden nachfolgend nur exemplarisch ausgewählte Themen dargestellt. 1

Auch IT-Compliance stellt jedoch (trotz der erforderlichen Fachkenntnisse im Bereich IT) keine Aufgabe dar, die allein von der IT-Abteilung oder dem CIO (Chief Information Officer) bewältigt werden kann. Vielmehr ist es oft erforderlich, in diesem Bereich interdisziplinär mit den Bereichen Recht, Datenschutz und Procurement zusammen zu arbeiten, um „compliant" zu sein. Durch eine aktiv gelebte Vorbildfunktion, die Bereitstellung ausreichender Budgets für die Einführung notwendiger Prozesse und die Kontrolle delegierter Aufgaben kann eine (persönliche) Haftung des Vorstandes oder des Geschäftsführers vermieden werden. Dies gilt insbesondere für den Bereich IT-Sicherheit, denn auch ein sog „Informationssicherheitsmanagementsystem (ISMS)" (vgl. dazu noch → Rn. 10) kann nur dann erfolgreich eingeführt und aufrechterhalten werden, wenn die notwendige „Management Attention" sichergestellt ist. 2

IT-Compliance muss sich zwangsläufig auch mit dem Softwarelizenzmanagement befassen. Fehlen Softwarelizenzen oder werden Computerprogramme über die vereinbarte Art und Weise hinaus genutzt, verstößt das Unternehmen gegen die Rechte des Softwareherstellers. Dies kann zu Unterlassungs- und Schadensersatzansprüchen führen. Gleichzeitig führen die Softwarehersteller verdachtsunabhängige Lizenzaudits durch, um den ordnungsgemäßen Einsatz ihrer Computerprogramme im Unternehmen zu überprüfen. Als Unternehmen sollte man darauf vorbereitet sein, um etwaige Haftungsrisiken zu vermeiden. Dies gelingt durch ein proaktives Lizenzmanagement. 3

Die IT eines Unternehmens und die damit einhergehende Datenverarbeitung sind zwangsläufig auch mit Fragen des Datenschutzes verknüpft. Wichtig ist, dass unternehmensintern eine Datenschutzorganisation aufgebaut ist, wodurch der Datenschutzbeauf- 4

tragte aktiv in die datenschutzrechtlich relevanten Prozesse eingebunden ist. Daneben müssen die konzerninternen Datenflüsse legitimiert sein. Insbesondere bei international aufgestellten Unternehmen stellen sich Fragen beim grenzüberschreitenden Datentransfer. Zudem müssen natürlich die Vertragsverhältnisse mit Dritten den datenschutzrechtlichen Anforderungen genügen.

B. Erläuterungen zur Checkliste

I. Informationstechnologie

1. IT-Sicherheit

a) Gibt es ein aktuelles Informationssicherheitskonzept?

5 Wesentliche Eckpfeiler von IT-Compliance sind die Gewährleistung von IT-Sicherheit (IT-Security) und der Schutz von geschäftskritischen Informationen. Die Geschäftsleitung ist zur Sicherstellung von IT-Security im Unternehmen verpflichtet, selbst wenn es sich hierbei nicht um eine sog „kritische Infrastruktur" im Sinne des IT-Sicherheitsgesetzes handelt (hierzu sogleich). Denn nach § 93 Abs. 1 AktG und § 43 GmbHG haben die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Angesichts der besonderen Bedeutung von IT für das Funktionieren und den Fortbestand des Unternehmens gehört es damit auch zu den Pflichten der Geschäftsleitung, das Unternehmen vor erkennbaren Gefahren im Bereich Informationstechnologie zu schützen. Die Unternehmensleitung ist daher auch zur Etablierung effektiver Sicherheitsmaßnahmen für die IT verpflichtet.[1] Dies verlangt zudem ein angemessenes Risikomanagement hinsichtlich der im Unternehmen vorhandenen IT-Systeme und deren Sicherheit. Dies wird auch im neuen IDW-Standard FA IT 5 ausdrücklich betont.

b) Werden Maßnahmen im Sinne des IT-Sicherheitsgesetzes umgesetzt?

6 Im Juli 2015 ist das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme", kurz IT-Sicherheitsgesetz, in Kraft getreten.[2] Das IT-Sicherheitsgesetz richtet sich zunächst nur an Betreiber sogenannter „kritischer Infrastrukturen". Hierunter fallen Unternehmen, die zwei (relativ offen formulierte) Voraussetzungen erfüllen: Erstens muss es sich um ein Unternehmen handeln, dass einem der neun im Gesetz benannten Sektoren unterfällt. Dazu zählen die Sektoren Energie, Informationstechnik, Telekommunikation, Transport, Verkehr, Gesundheit, Wasser, Ernährung sowie das Finanz und Versicherungswesen. Zweitens muss die vom Unternehmen betriebene Infrastruktur (gemeint ist nicht die IT-Infrastruktur), also die Einrichtungen und Anlagen des Unternehmens oder wenigstens Teile davon, „von hoher Bedeutung für das Funktionieren des Gemeinwesens" sein. Das ist dann der Fall, wenn durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder eine Gefährdung der öffentlichen Sicherheit eintreten würde. Da diese abstrakt formulierten Kriterien in der Praxis wenig hilfreich sind, werden diese durch Rechtsverordnungen konkretisiert werden. Hierin sollen spezifische Schwellenwerte für die Betreiber kritischer Infrastrukturen definiert werden, wobei die jeweils

[1] Siehe zu den rechtlichen Verpflichtungen zur Gewährleistung von IT-Security und zur Einführung einer Notfallplanung im IT-Bereich *Steger* CR 2007, 137 ff.; *Heckmann* MMR 2006, 280 ff.; *Roth/Schneider* ITRB 2005, 19 ff.

[2] Siehe zum IT-Sicherheitsgesetz insgesamt *Rath/Kuß/Bach* K&R 2015, 437.