

IT-Compliance an Hochschulen

Bearbeitet von
Dr. Ingo Schöttler

1. Auflage 2010. Taschenbuch. 240 S. Paperback
ISBN 978 3 415 04465 4
Format (B x L): 14,5 x 20,8 cm

Weitere Fachgebiete > Pädagogik, Schulbuch, Sozialarbeit > Schulen, Schulleitung >
Universitäten, Hochschulen

Zu Leseprobe

schnell und portofrei erhältlich bei


DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Inhaltsverzeichnis

Vorwort	5
Literaturverzeichnis	17
1. Kapitel Einleitung	23
2. Kapitel Der Begriff der IT-Compliance	26
A. IT-Compliance als rechtliche Kategorie	26
I. Der Begriff der „Compliance“	26
II. Die Entwicklung des Begriffes	27
III. Die Ziele und der Zweck einer Compliance	28
1. Sicherstellung rechtskonformen Verhaltens	28
2. Schadensprävention	29
3. Haftungsreduzierung der Unternehmensleitung	30
4. Vermeidung von Ansehensverlusten	30
IV. Compliance-Programme als rechtliche Notwendigkeit?	31
1. Die Vorgaben des Aktiengesetzes	31
2. Vorgaben aus § 130 OWiG	33
3. Vorgaben in Spezialgesetzen	34
4. Vorgaben für andere Organisationen	35
B. Die Durchführung beziehungsweise Herstellung von Compliance	36
I. Aufbau einer Compliance-Organisation	36
1. Klärung der Zuständigkeiten	36
2. Verfassen eines „Mission Statements“	37
II. <i>Sonderfall:</i> Outsourcing der Compliance	38
III. Die konkrete Durchführung	38
1. „Ist/Soll-Analyse“	38
a) Feststellung des Ist-Zustands	38
b) Abgleich mit dem Soll-Zustand	38
2. Erstellen eines Maßnahmen-Kataloges	39
3. Umsetzung der Maßnahmen	40
a) Information der Mitarbeiter	40
b) Schaffung einer Kontaktstelle	40
c) Entwicklung neuer Organisations-Richtlinien	41
d) Controlling-Maßnahmen	41
IV. <i>Übersicht 1:</i> Aufbau einer Compliance-Organisation und Durchführung von Compliance-Maßnahmen	43
C. Der Sonderbereich der „IT-Compliance“	44
I. Der Begriff der „IT-Compliance“	44
II. Betroffene Rechtsgebiete	45

III.	„IT-Compliance“-Maßnahmen	46
1.	Klärung der Verantwortlichkeiten	46
2.	Ist-Analyse & Maßnahmenplanung	46
3.	Umsetzung der Maßnahmen	47
a)	Information der Mitarbeiter	47
b)	Schaffung einer Kontaktstelle	48
c)	Entwicklung neuer Organisations-Richtlinien	48
d)	Controlling-Maßnahmen	48
4.	Übersicht 2: IT-Compliance-Maßnahmen	50
D.	IT-Compliance-Maßnahmen an Hochschulen	51
I.	Überblick	51
II.	Compliance für öffentliche Stellen?	51
III.	Die Bedeutung von IT-Compliance-Systemen für Hochschulen	52
1.	Der verstärkte Einsatz von IT-Systemen	52
2.	Weiterentwicklung der gesetzlichen Vorgaben und der Rechtsprechung	52
3.	Verstärkter Wettbewerb und Marketing	53
4.	Zunehmende Sensibilität bei den betroffenen Studenten	53
5.	Hochschulen als Ort spezifischer IT-Rechtsverstöße	53
IV.	Folgerungen für Hochschulen	54
3. Kapitel	IT-Einsatz an Hochschulen	56
A.	Überblick über die Entwicklung des IT-Einsatzes an Hochschulen	56
I.	Die Zeit bis 1990	56
II.	Die Zeit von 1990 bis 2000	57
III:	Die Zeit ab dem Jahre 2000	58
B.	Haupteinsatzgebiete von IT in der Hochschule	58
I.	Einzelne Rechnerarbeitsplätze	58
1.	Definition und Charakteristika	58
2.	Spezifische Risiken	59
a)	Softwarelizenzen	59
b)	Schadprogramme	60
c)	Rechtsverletzungen durch Nutzer	61
II.	Hochschulverwaltung	62
1.	Überblick	62
2.	Mögliche Risiken	62
a)	Gefahr von Lizenzverletzungen	62
b)	Datenschutzrechtliche Anforderungen	62
III.	Hochschulbibliothek	63
1.	Überblick	63
2.	Spezifische Risiken	63

IV.	Hochschullehre (<i>Stichwort</i> : E-Learning)	64
1.	Überblick	64
2.	Spezifische Risiken	64
V.	Forschung (<i>Stichwort</i> : E-Science)	65
1.	Überblick	65
2.	Spezifische Risiken	65
a)	Datenschutzverstöße bei der empirischen Daten- gewinnung	65
b)	Urheberrechtsverstöße bei dem Aufbau von multi- medialen Datenbanken	66
VI.	Internetauftritt der Hochschule	66
1.	Erscheinungsformen	66
2.	Spezifische Risiken	67
C.	<i>Ausblick</i> : Zukünftige Entwicklungen des IT-Einsatzes an Hoch- schulen	67
I.	„Ubiquitous Computing“	68
1.	Begriffsbestimmung	68
2.	Mögliche Risiken	68
II.	Modell einer umfassenden integrierten Informationsversorgung von Mitarbeitern und Studenten mit Hilfe eines „Single Sign On“	69
1.	Skizzierung des Modells	69
2.	Mögliche Risiken	70
III.	Universitätsübergreifendes „synchrones Lernen“	70
IV.	Grid-Computing-Ansätze, insbesondere im Bereich der Forschung	71
D.	Fazit	71
4. Kapitel	Überblick über die gesetzlichen Anforderungen für Hoch- schulen im IT-Bereich	73
A.	Systematik der Regelungen	73
I.	IT-spezifische und allgemeine Gesetze	73
II.	Hochschulspezifische und allgemeine Gesetze	75
III.	Die nicht zu berücksichtigenden Gesetze	76
IV.	Zusammenfassung	76
V.	<i>Übersicht</i> : Relevanz gesetzlicher Bestimmungen für IT-Compliance an Hochschulen	78
B.	Die einzelnen gesetzlichen Vorgaben	78
I.	Hochschulspezifische Gesetze	78
1.	Das Hochschulrahmengesetz	78
2.	Die Landeshochschulgesetze (<i>hier</i> am Beispiel Bayerns)	79
a)	Datenschutzrechtliche Vorgaben	80

b)	Nutzung der Informations- und Kommunikationstechniken	80
c)	Anerkennung „virtueller“ Studien- und Prüfungsleistungen	80
II.	IT-spezifische Gesetze	81
1.	Das Telekommunikationsgesetz	81
a)	Die Eröffnung des Anwendungsbereichs	81
b)	Für Hochschulen relevante Regelungsbereiche des TKG	82
2.	Das Telemediengesetz	83
a)	Die Eröffnung des Anwendungsbereichs	83
b)	Durch Hochschulen angebotene Telemedien	84
c)	Die einzelnen Regelungsbereiche des TMG	84
3.	Öffentlich-rechtliche IT-spezifische Vorgaben	87
a)	Barrierefreiheit	87
b)	Die ergänzenden Vertragsbedingungen für IT-Dienstleistungen (EVB-IT)	88
c)	Vorgaben der IuK-Strategie für die bayerische Staatsverwaltung (BayIuKS)	89
III.	Die „allgemeinen“ Gesetze	90
1.	Die Landesdatenschutzgesetze	90
2.	Das Urheberrechtsgesetz	91
a)	Der Schutzbereich des UrhG	91
b)	Die Rechte des Urhebers	91
c)	Die Regelungen des UrhG beim IT-Einsatz durch Hochschulen	92
3.	Das Patentgesetz	94
4.	Das Markengesetz	95
5.	Das Strafgesetzbuch	95
a)	Überblick	95
b)	Inkriminierte Inhalte	96
c)	Angriffe auf fremde IT-Infrastrukturen	97
d)	Straftatbestände in Bezug auf das Fernmeldegeheimnis (§ 206 StGB)	98
6.	Spezielle öffentlich-rechtliche Vorgaben	99
a)	Vorschriften im Bereich des Vergaberechts	99
b)	Personalvertretungsrecht	99
IV.	<i>Sonderfall:</i> Standards im IT-Bereich	100
C.	Fazit	100

5. Kapitel	Rechtsfolgen mangelhafter IT-Compliance	102
A.	Überblick über die Haftungsebenen	102
B.	Rechtsfolgen für den „Handelnden“	103
I.	Straftatbestände und Ordnungswidrigkeiten	103
1.	Straftatbestände im StGB	103
a)	Ausspähen von Daten (§ 202a StGB)	104
b)	Datenveränderung (§ 303a StGB)	104
c)	Verletzung des Fernmeldegeheimnisses (§ 206 StGB)	105
2.	Urheberrechtsverletzungen (§ 106 UrhG)	106
3.	Verstöße gegen das Datenschutzrecht	106
II.	Zivilrecht	107
1.	Überblick	107
2.	Haftung für Urheberrechtsverletzungen	107
3.	Weitere deliktische Haftung	107
4.	Relevanz der Amtshaftung bei IT-Verstößen	108
a)	Anvertrautes öffentliches Amt	108
b)	Rechtsverletzung in Ausübung dieser Amtspflicht	109
c)	Gegenüber Dritten bestehende Amtspflicht	109
III.	Arbeitsrecht/Dienstrecht	110
1.	Innenregress bei Amtshaftung	110
2.	Weitere dienstrechtliche/arbeitsrechtliche Folgen	111
C.	Rechtsfolgen für die Hochschulleitung	112
I.	Strafrecht	112
1.	Anstiftung	112
2.	Beihilfe	112
II.	Haftung gegenüber der eigenen Hochschule?	113
1.	Zivilrechtliche Haftung gegenüber Verletzten	114
2.	Arbeitsrecht/Dienstrecht	114
D.	Rechtsfolgen für die Hochschule als Körperschaft	114
I.	Übersicht über die verschiedenen Haftungsgrundlagen	114
II.	Die Haftung der Hochschule als „Verletzer“	115
1.	Marken- und Urheberrechtsverletzungen	115
2.	Datenschutzverstöße	116
3.	Weitere deliktische Ansprüche	116
III.	Die Haftung der Hochschule als „Störer“	117
IV.	Haftung für „fremde“ Rechtsverletzungen?	118
1.	Schadensersatzansprüche	118
2.	Bereicherungsansprüche	119
3.	Sonderkonstellation des § 100 UrhG	119
V.	Maßnahmen der Aufsichtsbehörden	119
E.	Haftung des Landes	120
F.	Fazit	120

6. Kapitel	Verantwortlichkeit für IT-Compliance an Hochschulen	122
A.	„Klassische“ Aufgabenzuweisung im Bereich der Privatwirtschaft	122
B.	Übertragung auf den Hochschulbereich	123
I.	Die Aufgaben der Hochschulleitung	123
1.	Allgemeine Zuständigkeit der Hochschulleitung	123
2.	Einzelne Zuständigkeiten der Hochschulleitung	123
a)	Grundsätze der hochschulpolitischen Zielsetzung und Entwicklung der Hochschule	123
b)	Aufstellung von Grundsätzen für die Evaluierung und Qualitätssicherung	124
3.	Rechtsaufsicht der Hochschulleitung	124
II.	Der Aufgabenbereich des Kanzlers	125
III.	Abgrenzung der Aufgabenbereiche von Hochschulleitung und Kanzler	126
IV.	Die Sonderstellung des behördlichen Datenschutzbeauftragten	126
1.	Pflicht zur Bestellung eines Datenschutzbeauftragten	126
2.	Die Einbindung des behördlichen Datenschutzbeauftragten in das Organisationsgefüge	126
3.	Die Aufgaben des behördlichen Datenschutzbeauftragten	127
V.	Mitwirkungspflichten der übrigen Beteiligten	128
C.	Neue Ansätze bei der Organisation der IT-Compliance	129
I.	Ernennung eines <i>Compliance</i> -Beauftragten?	129
II.	Aufgabenzuweisung an einen Chief Information Officer (CIO)	129
1.	Der CIO an Hochschulen	129
2.	Der CIO als Compliance-Beauftragter	130
D.	Fazit	131
7. Kapitel	Notwendige Bestandteile eines IT-Compliance-Konzeptes für Hochschulen	133
A.	Ausgangsüberlegungen	133
B.	Klärung und Festlegung der Verantwortlichkeiten	133
C.	Ist-Analyse und Maßnahmenplanung	134
I.	Durchführung einer Ist-Analyse	134
1.	Erfassung der Hard- und Software	134
2.	Feststellung des Lizenzbestandes	135
3.	Feststellung der Zugriffsrechte	135
4.	„Sichtung“ der Webseiten	135
II.	Einsatz von Checklisten	135
1.	Überblick über die Einsatzmöglichkeiten	135
2.	Beispiel für eine entsprechende Checkliste	136

D.	Planung und Durchführung von Maßnahmen	144
I.	Information der Mitarbeiter und Studenten	144
1.	Hinweise und Unterrichtung über gesetzliche Vorgaben	144
2.	Form der Information	145
a)	Durchführung von Schulungen	145
b)	Nutzung des Internets	145
II.	Schaffung einer Kontaktstelle	146
III.	Entwicklung neuer Benutzungsordnungen/ Dienstanweisungen	146
IV.	Controlling	147
8. Kapitel <i>Schwerpunkt der IT-Compliance: Datenschutzrechtliche</i>		
	Vorgaben	148
A.	Bedeutung des Datenschutzes an Hochschulen	148
B.	Datenschutzrechtliche Grundsätze bei der Erhebung von per- sonenbezogenen Daten an Hochschulen	149
I.	Grundsatz des Verbotes mit Erlaubnisvorbehalt	149
II.	Erforderlichkeitsgrundsatz	150
III.	Zweckbindungsgrundsatz	151
IV.	Technischer und organisatorischer Datenschutz	151
C.	Praxisrelevante Problembereiche im Detail	152
I.	Veröffentlichung von personenbezogenen Daten im Internet	152
1.	Veröffentlichung von Mitarbeiterdaten im Internet	152
a)	Vorliegen personenbezogener Daten	152
b)	Ermächtigungsgrundlagen für die Veröffentlichung von Mitarbeiterdaten im Internet	154
c)	Veröffentlichung von Mitarbeiterfotos	158
2.	Veröffentlichung von Studentendaten im Rahmen von Alumni-Netzwerken	158
II.	IT-gestützte Durchführung von Klausuren und Prüfungen	159
1.	Anmeldung und Durchführung von Klausuren und Prü- fungen	159
2.	Bekanntgabe von Klausur- und Prüfungsergebnissen im Internet	160
III.	Nutzung von Lernplattformen	163
1.	Anwendbares Rechtsregime	163
2.	Zulässige Datenerhebungen und -speicherungen inner- halb von Lernplattformen	164
a)	Registrierung bei der Lernplattform	165
b)	Anfallende Daten bei der Nutzung der Lernplattform	168
IV.	IT-gestützte Behandlung von Anfragen nach Daten	169
V.	Einsatz von Smart-Cards	170

VI.	IT-gestützte Lehrevaluationen	172
1.	Gesetzliche Grundlage der Lehrevaluation	172
2.	Datenschutzrechtliche Risiken bei der Weitergabe und Veröffentlichung der Evaluationsdaten	173
D.	Zusammenfassende Checkliste	175
I.	Einsatzbereich	175
II.	Die Checkliste im Detail	175
9. Kapitel	Schwerpunkt der IT-Compliance: IT-Sicherheitsrecht . .	181
A.	Der Begriff des „IT-Sicherheitsrechts“ im Hochschulbereich . . .	181
B.	Sicherung von Informationen gegen Angriffe von „außen“	182
I.	Analyse der relevanten Gefährdungspotentiale	182
1.	Schadprogramme	183
a)	Viren	183
b)	Würmer	183
c)	Trojanische Pferde	183
2.	DoS-Angriffe	184
3.	Spam-E-Mails	184
4.	Weitere Angriffsformen	184
II.	Rechtskonforme Sicherheitsvorkehrungen	185
1.	Technische Schutzmaßnahmen	185
a)	Einsatz von Firewalls	185
b)	Einsatz von Virenfiltern	186
c)	Einsatz von Spam-Filtern	187
d)	Sperrung von Internetseiten	189
e)	Kontrolle des Internetverkehrs	191
f)	Kontrolle der E-Mail-Nutzung	193
g)	Einwilligung der Betroffenen in weitergehende Kon- trollen bei zugelassener Privatnutzung	198
2.	Sonstige Sicherheitsmaßnahmen	199
C.	Sicherung der Informationen gegen Angriffe von „innen“	199
I.	Analyse der relevanten Gefährdungspotentiale	199
1.	Unberechtigter Zugriff auf Daten	199
2.	Löschung oder Unbrauchbarmachung von Daten	200
II.	Rechtskonforme Sicherheitsvorkehrungen	201
1.	Rechte- und Zugriffsmanagement	201
2.	Kontrolle der IT-Nutzung	202
D.	Zusammenfassende Übersicht und Checkliste	203
10. Kapitel	Schwerpunkt der IT-Compliance: Urheberrechtliche Vor- gaben	207
A.	Bedeutung des Urheberrechtsgesetzes beim IT-Einsatz durch Hochschulen	207
B.	Urheberrechtliche Grundsätze an Hochschulen	208

I.	Urheberrechtlich geschützte Werke an Hochschulen	209
II.	Geschützte Verwertungshandlungen im Rahmen des IT-Einsatzes	210
	1. Überblick über die Rechte des Urhebers	210
	2. Das Vervielfältigungsrecht gemäß § 16 UrhG	211
	3. Das Recht der öffentlichen Zugänglichmachung gemäß § 19a UrhG	211
	4. Weitere Verwertungsrechte des Urhebers	214
III.	Hochschulrelevante Schranken des Urheberrechts	214
	1. Zitatrecht gemäß § 51 UrhG	214
	2. Öffentliche Zugänglichmachung für Unterricht und For- schung gemäß § 52a UrhG	215
	a) Zugänglichmachung von Werken im Unterricht (§ 52a Abs. 1 Nr. 1 UrhG)	216
	b) Zugänglichmachung von Werken für „eigene“ wis- senschaftliche Forschung (§ 52a Abs. 1 Nr. 2 UrhG)	219
	3. Relevante „neue“ Schrankenregelungen	219
C.	Praxisrelevante Problembereiche im Detail	221
I.	Urheberrechtsverletzungen durch die Hochschule beziehungsweise ihre Mitarbeiter	221
	1. Zugänglichmachung urheberrechtlich geschützter Lehrmaterialien im Internet	221
	2. Unterlizenzierung bei eingesetzter proprietärer Software	223
	3. Lizenzverletzungen im Bereich von Open-Source-Soft- ware	224
	4. Lizenzverletzungen bei Werken, die von Hochschulange- hörigen geschaffen wurden	226
II.	Haftung für Urheberrechtsverletzungen durch Studierende und Mitarbeiter	228
	1. File-Sharing über Hochschulnetzwerke	228
	2. Urheberrechtsverletzungen von Studierenden über „Web 2.0“-Portale	228
D.	Zusammenfassende Checkliste	229
11. Kapitel Zusammenfassung		234