

INHALTSVERZEICHNIS

	<u>Seite</u>
ABKÜRZUNGSVERZEICHNIS	XV
ABBILDUNGSVERZEICHNIS	XXI
EINLEITUNG	1
1 Erläuterung des Forschungsgegenstandes	2
2 Zielsetzung	5
3 Gang der Untersuchung	6
TEIL I: RISIKOMANAGEMENT UND INFORMATIONSSICHERHEIT	7
1 Einführung in das Risikomanagement	8
2 Bedeutung eines Risikomanagementsystems	9
2.1 „Risiko“ und „Risikomanagement“ – was verbirgt sich hinter diesen Begriffen?	9
2.2 Notwendigkeit eines Risikomanagements	11
2.3 Zielsetzung und Aufgabenspektrum	12
3 Risikoarten und Risikokategorien	14
3.1 Externe Risiken	16
3.2 Interne Risiken	17
4 Ablauf des Risikomanagementprozesses	21
4.1 Risikostrategie	21
4.2 Risikoidentifikation	22
4.3 Risikoanalyse	23
4.4 Risikomessung, Risikobewertung und Risikokommunikation	24
4.5 Risikosteuerung	26
4.6 Risikokontrolle und Risikodokumentation	28

5	Risikomanagement nach KonTraG	29
5.1	Regelungsbedarf des Gesetzgebers	29
5.2	Normadressat und Ausstrahlungswirkung des § 91 Abs. 2 AktG	32
5.3	Würdigung des Risikomanagementsystems im Lichte der Jahresabschlussprüfung	35
6	Ausgestaltung eines Risikomanagementsystems gemäß KonTraG	40
6.1	Auslegungsproblematik	40
6.2	Risikomanagement nach KonTraG – Erklärungsversuche in der betriebswirtschaftlichen und rechtswissenschaftlichen Literatur	40
6.3	Ansätze eines Risikomanagementsystems gemäß § 91 Abs. 2 AktG	43
6.3.1	Internes Überwachungssystem	45
6.3.2	Frühwarnsystem	46
6.3.3	(Risiko-) Controlling	46
6.4	Fazit	48
7	Risikomanagement im Konzern	51
7.1	Einführung	51
7.2	Reichweite des § 91 Abs. 2 AktG bei einer Konzernstruktur	52
7.3	Zwischenergebnis	55
7.4	Besondere Gefahren eines international operierenden Konzerns	55
7.5	Fazit	61
8	Der Einsatz moderner Informationstechnologien und das damit verbundene Gefahrenpotenzial	62
8.1	Der Faktor „IT-Sicherheit“	62
8.1.1	Begriff und Stellenwert im 21. Jahrhundert	62
8.1.2	Adressaten der IT-Sicherheit und Schutzziele	66
8.2	Notwendigkeit zur Schaffung einer angemessenen IT-Sicherheit	69
8.2.1	Wirtschaftliche Erwägungen	69
8.2.2	Juristische Beweggründe im Überblick	72
a)	Datenschutzrechtliche Aspekte	72
b)	Haftungs- und Strafbarkeitsprophylaxe	73

aa)	Haftungsrelevante Szenarien	73
bb)	Strafrechtlich relevante Szenarien	76
c)	Haftungsrechtliche Konsequenzen	77
8.3	Risiken und Gefahrenbereiche für die Informationssicherheit	78
8.4	Internetspezifische Risiken	86
8.4.1	Einführung	86
8.4.2	Chancen und Bedrohungen im E-Business	87
8.4.3	Potenzielle Schadensszenarien und Haftungsrisiken speziell im Lichte der Internetnutzung durch Arbeitnehmer in Deutschland ..	90
a)	Beispielfälle	90
b)	Zurechnungs- bzw. Haftungsnormen des deutschen Rechts	95
c)	Private Internetnutzung – ein personalwirtschaftliches Risiko?	96
8.5	Lösungsmöglichkeiten	97
8.5.1	IT-Risikomanagement – Illustration insbesondere internet- basierter Risiken anhand des Risikomanagementprozesses	97
8.5.2	Der Beitrag von Internetkontrollen zur Informationssicherheit und Haftungsvermeidung	114
8.6	Zwischenergebnis	116
9	Kommunikations- und datenschutzrechtliche Schranken	118
 TEIL II: ZUR KONTROLLE DES INTERNETARBEITSPLATZES - DIE RECHTSLAGE IN DEUTSCHLAND		
1	Einführung	120
2	Erlaubnis durch den Arbeitgeber	122
2.1	Dienstliche versus private Nutzung	122
2.2	Entscheidungsbefugnis des Vorgesetzten	122
2.3	Erlaubnistatbestände und deren Rücknahmemöglichkeiten	123
2.3.1	Ausdrückliche Erlaubnis	123
2.3.2	Konkludente Einwilligung	124
2.3.3	Erlaubnis durch betriebliche Übung	125

a) Entstehung	125
b) Beseitigung	128
2.4 Nutzungsumfang	130
3 Die Kontrolle bei der Nutzung des dienstlichen Internetarbeitsplatzes zu privaten Zwecken	132
3.1 Verfassungsrechtliche Grundsätze	133
3.1.1 Rechtsquellen des Arbeitsrechts	133
3.1.2 Drittwirkung der Grundrechte im Arbeitsverhältnis	134
3.1.3 Allgemeines Persönlichkeitsrecht	136
a) Einführung	136
b) Erscheinungsformen	137
3.1.4 E-Mail- und World Wide Web-Überwachung im Lichte des allgemeinen Persönlichkeitsrechts	143
a) Erfordernis der Rechtfertigung von Kontrollaktivitäten	143
b) Reichweite des Persönlichkeitsschutzes	144
c) E-Mail-Kontrolle – ist der Rückgriff auf die Rechtslage bei Telefonaten vorliegend zulässig?	146
aa) Dienstliche Nutzung	146
bb) Private Nutzung	148
d) Kontrolle der World Wide Web-Nutzung	149
aa) Dienstliche Nutzung	150
bb) Private Nutzung	150
e) Zwischenergebnis	151
3.1.5 Recht auf Freiheit der Meinung	152
3.1.6 Das Fernmeldegeheimnis gemäß Art. 10 GG	153
a) Einführung	153
b) Schutzzumfang	154
c) Zwischenergebnis	157
3.2 Einfachgesetzliche Betrachtung	158
3.2.1 Das Telekommunikationsgesetz (TKG)	159
a) Einfachgesetzliches und grundrechtlich geschütztes Fernmeldegeheimnis	159
b) Anwendbarkeit im Arbeitsverhältnis	159
c) Funktion des § 88 Abs. 3 TKG	162

d)	Zulässigkeit der Überwachung von E-Mails und aufgerufener Internetseiten nach dem Telekommunikationsgesetz	164
aa)	Kontrolle von E-Mails	164
bb)	Überwachung der World Wide Web-Nutzung	166
cc)	Zwischenergebnis	168
3.2.2	Relevanz der Vorschriften des Telemediengesetzes (TMG)	168
a)	Einführung	168
b)	Die Rechtslage vor Inkrafttreten des Telemediengesetzes ...	169
c)	Die Situation nach der Verabschiedung des Gesetzes	171
d)	Zwischenergebnis	174
4	Die ausschließlich dienstliche Nutzung des Internetarbeitsplatzes	176
4.1	Nichtanwendbarkeit der bereichsspezifischen Gesetze	176
4.2	Verfassungsrechtliche Aspekte	176
4.3	Die einschlägigen Vorgaben des Bundesdatenschutzgesetzes	177
4.3.1	Anwendbarkeit im Arbeitsverhältnis	177
4.3.2	Datenverarbeitung nach den Grundsätzen des Gesetzes	178
a)	Betriebsvereinbarung	179
b)	Einwilligung des Betroffenen	179
c)	Überwachung gemäß § 28 BDSG	180
d)	Weitere relevante Normen des Bundesdatenschutzgesetzes (Auszug)	182
e)	Zwischenergebnis	184
4.4	Kontrollbefugnisse des Arbeitgebers	185
4.5	Besondere Beschäftigungsgruppen	187
5	Problemfeld „Mischnutzung“	189
6	Rechtsfolgen bei der Verletzung von Rechtsnormen im Rahmen der Internetkontrolle durch den Arbeitgeber	191
6.1	Strafrechtlich relevantes Fehlverhalten	191
6.1.1	Strafbarkeit wegen Verletzung des Briefgeheimnisses	191
6.1.2	Strafbarkeit wegen Ausspähöns von Daten	191
6.1.3	Strafbarkeit wegen Verletzung des Post- oder Fernmeldegeheimnisses	192
a)	Einführung	192

b)	Der Tatbestand des § 206 Abs. 1 StGB	193
c)	Der Tatbestand des § 206 Abs. 2 StGB	195
d)	Urteil des OLG Karlsruhe vom 10. Januar 2005	195
e)	Zwischenergebnis	199
6.2	Sanktionen bei Verstößen gegen das Bundesdatenschutzgesetz	199
6.3	Zivilrechtliche Ansprüche des Geschädigten	201
7	Rechtsfolgen im Fall einer rechtsmissbräuchlichen Nutzung des Internetarbeitsplatzes durch den Arbeitnehmer	203
7.1	Arbeitsvertragswidrige Internetnutzung	203
7.2	Strafrechtlich relevante Verhaltensweisen	207
7.3	Reaktionsmöglichkeiten des Arbeitgebers unter Berücksichtigung einschlägiger Rechtsprechung	210
7.4	Fragen der Beweisverwertung	216
8	(Mit-) Verantwortlichkeit des Arbeitgebers für Vergehen seiner Mitarbeiter	222
8.1	Zivilrechtliche Haftung	222
8.2	Strafrechtliche Verantwortlichkeit	223
8.3	Fazit	224
9	Die Interaktion zwischen den einschlägigen Gesetzen	225
TEIL III: DIE RECHTSLAGE IM VEREINIGTEN KÖNIGREICH (U. K.)		227
1	Einführung	228
2	Das englische Rechtssystem im Überblick	230
3	Die Bedeutung des „Human Rights Act 1998“	234
3.1	Die Konvention zum Schutze der Menschenrechte und Grundfreiheiten – die europäische Vorgabe	235
3.1.1	Rechtlicher Status der Menschenrechtskonvention	235
3.1.2	Der innewohnende Sanktionsmechanismus der Konvention	238
3.1.3	Der Schutzbereich von Menschenrechten am Beispiel des Art. 8 EMRK	240
3.1.4	Eingriff in den Schutzbereich von Art. 8 EMRK	242

a)	Gesetzliche Grundlage	243
b)	Eingriffsgrund	244
c)	Notwendigkeit des Eingriffs in einer demokratischen Gesellschaft	245
3.2	Persönlichkeitsschutz im Vereinigten Königreich und die Rolle des Human Rights Act 1998	245
3.3	Die Verantwortlichkeit nach dem Human Rights Act 1998	249
3.3.1	Problemstellung	249
3.3.2	Abgrenzungsprobleme – gemischt-öffentliche versus (rein) öffentliche Behörden	250
3.3.3	Die auslegende Funktion des Gesetzes – der sogenannte „Horizontaleffekt“	254
3.3.4	Grenzen des Horizontaleffekts	257
3.4	Anwendungspotenzial des Gesetzes im Lichte der Thematik unter Berücksichtigung einschlägiger Urteile des Europäischen Gerichts- hofes für Menschenrechte	260
3.4.1	Das Verfahren „Niemietz gegen Deutschland“	261
3.4.2	Der Fall „Halford gegen das Vereinigte Königreich“	263
3.4.3	Die Angelegenheit „Copland gegen das Vereinigte Königreich“ ..	266
3.4.4	Das Verfahren „Malone gegen das Vereinigte Königreich“	269
3.4.5	Ergebnis	271
4	Die Vorgaben des „Regulation of Investigatory Powers Act 2000“	275
4.1	Introduktion	275
4.2	Anwendung auf E-Mail und andere Internetdienste	278
4.3	Problematik	281
5	Die Bedeutung der „Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000“ im Lichte der Online-Überwachung	284
5.1	Status und Zweck der Regulations	284
5.2	Rechtmäßigkeit von Internetkontrollen nach Maßgabe der Regulations .	286
6	Datenverarbeitung nach Maßgabe des „Data Protection Act 1998“	292
6.1	Einführung	292

6.2	Grundzüge des Data Protection Act 1998	293
6.3	Die Rolle des <i>Information Commissioners</i>	300
6.4	Rechtmäßigkeit von Überwachungsmaßnahmen nach Maßgabe des Data Protection Act 1998	305
7	„Code of Practice“ – Mittel zur Konfliktvermeidung?	308
7.1	Status und Einordnung	308
7.2	Bedeutung des Code of Practice für die untersuchte Thematik	309
7.3	Konkrete Lösungsvorschläge des <i>Information Commissioners</i>	312
8	Rechtsfolgen bei Fehlverhalten des Arbeitgebers oder Arbeitnehmers	318
9	Verantwortlichkeit des Arbeitgebers für Vergehen seiner Beschäftigten ...	321
10	Interaktion zwischen den einschlägigen Gesetzen und Zusammenfassung	327
TEIL IV: SCHLUSSBETRACHTUNG		333
1	Zusammenfassung der Ergebnisse	334
2	Ausblick	342
LITERATURVERZEICHNIS		345
RECHTSPRECHUNGSVERZEICHNIS		365