

# **Das Spannungsfeld zwischen Datenschutz - Anforderungen und dem Aufbau und Betrieb eines internen Kontrollsystems**

**Die Zulässigkeit von automatischen Datenanalysen  
aus der Sicht eines IT-Dienstleistungsunternehmens**

**Diplomarbeit von  
Julian Schenten**

Diplomarbeit im Studiengang Informationsrecht · Hochschule Darmstadt

Vorgelegt am 31. Mai 2010

Referent: Prof. Dr. Martin Führ

Korreferent: Prof. Dr. Thomas Wilmer

Themenvorschlag „Das Spannungsfeld zwischen Datenschutzbestimmungen und dem  
Aufbau und Betrieb eines internen Kontrollsystems“ von Hubertus Gottschalk

<b>Inhaltsverzeichnis</b> .....	<b>III</b>
Abkürzungsverzeichnis .....	VI
<b>1 Einleitung</b> .....	<b>1</b>
1.1 Problemlage .....	1
1.2 Ziel der Arbeit und Eingrenzung des Themas .....	4
1.3 Methodisches Vorgehen .....	6
1.4 Aufbau der Arbeit .....	6
1.5 Glossar .....	7
1.5.1 Corporate Governance und Compliance .....	7
1.5.2 Internes Kontrollsystem .....	7
1.5.3 Fraud, Wirtschaftsdelikt, Straftat .....	8
1.5.4 Datenverarbeitende Stelle, Konzernleitung, Vorstand, Arbeitgeber .....	8
1.5.5 Arbeitnehmer, Beschäftigter, Betroffener .....	9
1.5.6 Personenbezogene Daten und der Umgang mit ihnen .....	9
<b>2 Gesetzliche und andere Anforderungen an Unternehmen zur Errichtung interner Kontrollsysteme</b> .....	<b>11</b>
2.1 Anforderungen aus dem deutschen Wirtschafts- und Gesellschaftsrecht, unter Berücksichtigung der europäischen Vorgaben .....	11
2.1.1 Überwachungspflicht und Haftung des Vorstands nach dem Aktiengesetz .....	11
2.1.1.1 Organisationspflicht des Vorstands: Errichtung eines Überwachungssystems .....	11
2.1.1.2 Sorgfaltspflicht und Verantwortung der Vorstandsmitglieder .....	14
2.1.1.3 Haftung des Vorstands .....	15
2.1.2 Überwachungspflicht und Haftung des Aufsichtsrates nach dem Aktiengesetz .....	17
2.1.2.1 Überwachung der Wirksamkeit des internen Kontrollsystems .....	17
2.1.2.2 Überprüfung von Konzernabschluss und -lagebericht .....	18
2.1.2.3 Haftung des Aufsichtsrates .....	19
2.1.3 Erklärung zum Deutschen Corporate Governance Index .....	20
2.1.3.1 Der Deutsche Corporate Governance Kodex .....	20
2.1.3.2 Auswirkungen für die Organe der Gesellschaft .....	21
2.1.4 Erwartungen an das Interne Kontrollsystem aus handelsrechtlicher Sicht .....	23
2.1.4.1 Konzernlagebericht .....	23
2.1.4.2 Feststellungen im Prüfungsbericht zur Wirksamkeit des Überwachungssystems .....	24
2.1.5 Branchenbezogene Spezialvorschriften mit Ausstrahlungswirkung auf andere Wirtschaftszweige .....	26
2.1.5.1 Technische Schutzmaßnahmen, § 109 TKG .....	26
2.1.5.2 Spezialvorschriften des KWG i.V.m. MaRisk .....	27
2.1.5.3 Basel II .....	28
2.1.5.4 Organisationspflichten, § 33 WpHG .....	28
2.2 Ordnungswidrigkeit der Verletzung von Aufsichtspflichten .....	29

2.3 Der Sarbanes-Oxley Act: Erweiterte Offenlegung von Unternehmensdaten und interne Kontrollsysteme .....	30
2.3.1 Anwendungsbereich .....	32
2.3.2 Pflichten der Geschäftsführung .....	33
2.3.2.1 Organisationspflichten .....	33
2.3.2.1.1 Disclosure controls and procedures .....	34
2.3.2.1.2 Internal control over financial reporting .....	34
2.3.2.2 Jahresabschlussbericht und Bestätigungserklärung .....	35
2.3.2.2.1 Beurteilungspflichten im Jahresabschlussbericht .....	35
2.3.2.2.2 Bestätigungserklärung nach sec. 302 SOA .....	36
a) Inhalt der Bestätigungserklärung .....	36
b) Mögliche Rechtsfolge bei unwahrer Bestätigungserklärung .....	37
2.3.2.2.3 Bestätigungserklärung nach sec. 906 SOA .....	38
2.3.3 Abschlussprüferbericht .....	38
2.4 Zusammenfassende Anforderungen an das interne Kontrollsystem .....	39
<b>3 Datenschutzrechtliche Vorgaben .....</b>	<b>43</b>
3.1 Anwendbarkeit bereichsspezifischer Regelungen aus TKG und TMG .....	43
3.2 Anwendbarkeit des BDSG .....	44
3.3 Grundsätze des Datenschutzrechts .....	44
3.4 Ermächtigungsgrundlagen für die Verwendung personenbezogener Beschäftigtendaten .....	46
3.4.1 Einwilligung des betroffenen Beschäftigten .....	47
3.4.2 Betriebsvereinbarung .....	49
3.4.3 Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses im Allgemeinen, § 32 Abs. 1 Satz 1 BDSG .....	51
3.4.3.1 Die Ermächtigungsgrundlagen im Einzelnen .....	52
3.4.3.1.1 Begründung des Beschäftigungsverhältnisses .....	52
3.4.3.1.2 Durchführung des Beschäftigungsverhältnisses .....	53
3.4.3.1.3 Beendigung des Beschäftigungsverhältnisses .....	54
3.4.3.2 Erforderlichkeit .....	54
3.4.3.2.1 Der datenschutzrechtliche Begriff der Erforderlichkeit .....	55
3.4.3.2.2 Anknüpfungspunkt für die Erforderlichkeit .....	57
3.4.4 Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten gemäß § 32 BDSG im Besonderen zur Aufdeckung und Prävention von Straftaten und anderen Rechtsverstößen .....	58
3.4.4.1 Anwendung von § 32 Abs. 1 Satz 2 BDSG zur Aufdeckung von Straftaten .....	58
3.4.4.1.1 Aufdeckung .....	59
3.4.4.1.2 Straftat im Beschäftigungsverhältnis .....	59
3.4.4.1.3 Tatsächliche zu dokumentierende Anhaltspunkte, die den Verdacht einer Straftat begründen .....	60
3.4.4.1.4 Verhältnismäßigkeit .....	62
a) Geeignetheit .....	63
b) Erforderlichkeit .....	63
c) Angemessenheit .....	64
i. Rechte der Arbeitnehmer .....	64
ii. Rechte der Arbeitgeber .....	65
iii. Praktische Konkordanz .....	66

3.4.4.2 Anwendung von § 32 Abs. 1 Satz 1 BDSG zur Prävention von Straftaten.....	67
3.4.4.3 Würdigung.....	68
3.4.5 Datenerhebung und -speicherung für eigene Geschäftszwecke.....	71
<b>4 Unternehmensinterne Kontroll-Maßnahmen und ihre Beurteilung nach deutschem Datenschutzrecht.....</b>	<b>72</b>
4.1 Grundlegende organisatorische Kontroll-Maßnahmen des Anti-Fraud-Managements ...	73
4.2 Präventive Datenanalysen .....	76
4.2.1 Beschreibung des Vorgangs: Abgleich von Mitarbeiter- und Lieferantendaten zur Aufdeckung von Fraud.....	76
4.2.2 Datenschutzrechtliche Überprüfung .....	79
4.2.2.1 Zulässigkeit der Verwendung der Lieferantendaten .....	79
4.2.2.2 Zulässigkeit der Verwendung der Beschäftigtendaten .....	79
4.2.2.2.1 Ermächtigungsgrundlage .....	80
4.2.2.2.2 Verhältnismäßigkeit .....	81
a) Geeignetheit .....	81
b) Erforderlichkeit .....	81
c) Angemessenheit.....	83
i. Praktische Konkordanz .....	84
ii. Würdigung des Urteils vom ArbG Berlin zur Massendatenanalyse der Bahn AG .....	88
iii. Würdigung der Vorgaben aus der jüngeren Rechtsprechung des BVerfG.....	90
iv. Würdigung der Vorgaben des europäischen Gemeinschaftsrechts .....	94
4.2.3 Rechte der Arbeitnehmervertretung .....	97
4.2.4 Schlussfolgerungen.....	99
4.3 Aufdeckung bereits begangener Straftaten.....	101
4.3.1 Beschreibung des Vorgangs: Weiterverfolgung der Verdachtsmomente, welche durch die in Abschnitt 4.2.1 beschriebene Datenanalyse gewonnen wurden.....	101
4.3.2 Rechtliche Überprüfung .....	102
4.3.2.1 Arbeitsvertrag, Hausrecht und Direktionsrecht des Arbeitgebers.....	102
4.3.2.2 Datenschutzrechtliche Überprüfung.....	104
4.3.2.2.1 Aufdeckung.....	105
4.3.2.2.2 Straftat im Beschäftigungsverhältnis.....	105
4.3.2.2.3 Tatsächliche zu dokumentierende Anhaltspunkte, die den Verdacht einer Straftat begründen .....	106
4.3.2.2.4 Verhältnismäßigkeit .....	107
4.3.2.3 Rechte der Arbeitnehmervertretung .....	109
4.3.2.4 Schlussfolgerungen.....	110
<b>5 Zusammenfassung und Handlungsempfehlung .....</b>	<b>112</b>
5.1 Zusammenfassung .....	112
5.2 Handlungsempfehlung .....	114
<b>6 Literatur- und Quellenverzeichnis.....</b>	<b>117</b>