

Inhaltsübersicht

<i>Vorwort</i>	V
<i>Aus dem Vorwort zur 1. Auflage</i>	VII
<i>Bearbeiterverzeichnis</i>	IX
<i>Inhaltsverzeichnis</i>	XIII
<i>Abkürzungsverzeichnis</i>	XXI
<i>Literaturverzeichnis</i>	XXVII
1. Kapitel Einführung	1
2. Kapitel Grundprinzipien eines Compliance Management Systems	15
3. Kapitel Pflicht zur Einführung eines Hinweisgebersystems	31
4. Kapitel Weichenstellungen bei der Implementierung	51
5. Kapitel Beachtung datenschutzrechtlicher Vorgaben	101
6. Kapitel Informationen aus Hinweisgebersystemen im Lichte strafprozessualer Ermittlungshandlungen	125
7. Kapitel Praktische Herausforderungen und Lösungen	141
8. Kapitel Länderteil Österreich	165
9. Kapitel Länderteil Schweiz	191
<i>Stichwortverzeichnis</i>	225

Inhaltsverzeichnis

<i>Vorwort</i>	V
<i>Aus dem Vorwort zur 1. Auflage</i>	VII
<i>Bearbeiterverzeichnis</i>	IX
<i>Inhaltsübersicht</i>	XI
<i>Abkürzungsverzeichnis</i>	XXI
<i>Literaturverzeichnis</i>	XXVII

1. Kapitel

Einführung

I. Der Begriff „Whistleblowing“ als Ausgangspunkt	2
II. Implikationen für den Hinweisgeber und die betroffene Organisation	3
III. EU-Hinweisgeberrichtlinie und Hinweisgeberschutzgesetz	5
IV. Missbrauch von Hinweisgebersystemen – Eine empirische Untersuchung	7
1. Einleitung	7
2. Die Kernthesen	8
a) KT1: Fast 90 % aller Hinweise werden in guter Absicht abgegeben	9
b) KT2: Der Prozentsatz missbräuchlicher Meldungen ist unabhängig davon, ob der Hinweis anonym abgegeben worden ist oder nicht	9
c) KT3: Die Öffnung des Hinweisgebersystems für Externe führt nicht zu einer Erhöhung missbräuchlicher Meldungen	10
3. Untersuchungsergebnisse im Detail	10

2. Kapitel

Grundprinzipien eines Compliance Management Systems

I. Grundlagen	15
1. Ziele	15
2. Rechtsgrundlagen im deutschen Recht	15
3. Internationale Vorgaben und Ansätze zum Aufbau eines Compliance Management Systems	16
a) Internationale Standards zur Korruptionsbekämpfung	17
aa) US Foreign Corrupt Practices, DOJ- und SEC-Vorgaben, sowie Sentencing Guidelines	17
bb) UK Bribery Act und adequate procedures	18
cc) Sapin II	18
dd) ISO 37001	18
ee) Spezielle Vorgaben für Pharma und Medizintechnik	19
b) Internationale Standards im Bereich Kartellrecht	19
aa) USA	19
bb) ICC-Toolkit	20
c) Internationale Standards im Bereich Außenwirtschaftsrecht	20
d) Internationale Standards im Bereich Datenschutz	20

II. Der Weg zu einem effektiven Compliance Management System	21
1. Führungskultur und Compliance-Organisation	21
2. Risikoanalyse	22
a) Top-Down-Analyse	23
b) Risikoszenarioanalyse	23
c) Risikofaktorenanalyse	23
d) Fazit	24
3. Richtlinien und Kontrollen	24
a) Grundsätze der Ausarbeitung von Richtlinien	24
b) Anzahl und inhaltliche Ausgestaltung der Richtlinien	25
c) Implementierung der Richtlinien	26
4. Schulungen und Kommunikation	26
5. Überwachung und Revision	27
6. Reaktion auf Verstöße und Nachhaltigkeit	28

3. Kapitel

Pflicht zur Einführung eines Hinweisgebersystems

I. Rechtspflicht zur Implementierung eines Hinweisgebersystems?	31
1. Allgemeine Erforderlichkeit von Hinweisgebersystemen	32
a) Schutzbedürftigkeit der Hinweisgeber	32
b) Schutzbedürftigkeit der Interessen der Allgemeinheit	33
2. Künftige allgemeine Rechtspflichten nach Maßgabe der Richtlinie zum Schutz von Hinweisgebern	34
a) Historische Entwicklung hin zur Pflicht einer Implementierung von Hinweisgebersystemen für deutsche Unternehmen	35
b) Grundsätze einer generellen Implementierungspflicht	37
aa) Ziel der EU-Hinweisgeberrichtlinie	38
bb) Pflicht zur Einrichtung interner Meldekanäle	38
(1) Sachlicher Anwendungsbereich	39
(2) Persönlicher Anwendungsbereich	39
c) Inhaltliche Ausgestaltung der Implementierung eines Hinweisgebersystems	40
aa) Vertraulichkeitsgebot	41
bb) Information des Hinweisgebers	42
cc) Dokumentation der Meldungen	42
dd) Schutzmaßnahmen	43
(1) Schutz vor Repressalien	43
(2) Schutz vor Haftung des Hinweisgebers	45
(3) Schutz der betroffenen Person	45
d) Exkurs: Pflicht zur Errichtung externer Meldekanäle	45
3. Bereichsspezifische Pflichten zur Einführung von Hinweisgebersystemen nach (deutschem) Recht	46
a) Rechtspflicht nach dem Kreditwesengesetz	46
b) Rechtspflicht nach der Marktmissbrauchsverordnung	46
c) Rechtspflicht nach Versicherungsaufsichtsgesetz	46
d) Rechtspflicht nach dem Finanzdienstleistungsaufsichtsgesetz	46

e) Rechtspflicht nach dem Allgemeinen Gleichbehandlungsgesetz	47
f) Rechtspflicht nach dem Betriebsverfassungsgesetz	48
g) Weitere Regelungen zum Schutz von Hinweisgebern	48
aa) Schutz von Hinweisgebern im Arbeitsschutzgesetz	48
bb) Schutz von Hinweisgebern nach dem Geschäftsgeheimnisgesetz	48
cc) Schutz von Hinweisgebern nach dem Geldwäschegesetz, dem Wertpapierhandelsgesetz, dem Bürgerlichen Gesetzbuch	49
4. Wieso ein Hinweisgebersystem auch ohne gesetzliche Pflicht Sinn ergibt	49
5. Fazit	50

4. Kapitel

Weichenstellungen bei der Implementierung

I. Weichenstellung innerhalb der Unternehmensleitung	51
II. Rahmenbedingungen eines Hinweisgebersystems	54
1. Vertikale Delegation und Berichterstattung	54
2. Einleitung interner Untersuchungen durch den Aufsichtsrat	55
3. Verankerung des Hinweisgebersystems innerhalb des Unternehmens ...	56
a) Thematische Zuständigkeit	58
b) Zuständigkeit für Bearbeitungsschritte	59
aa) Hinweiseingangsstelle	59
bb) Untersuchende Stelle	60
cc) Untersuchungskoordination	61
dd) Remediation	61
4. Schnittstellenzusammenarbeit	61
a) Compliance-Abteilung und interne Revision	62
b) Personalabteilung	62
c) Rechtsabteilung	62
d) Datenschutzabteilung und Betriebsrat	63
e) Weitere Schnittstellen	63
5. Hinweispflicht der Mitarbeiter	65
a) Rechtliche Grenzen einer Ausweitung bestehender Hinweispflichten	66
b) Vor- und Nachteile einer Ausweitung von Hinweispflichten	67
c) Empfehlung zur konkreten Umsetzung	68
6. Datenschutzrechtliche Abstimmung	68
7. Information und Schulung potentieller Hinweisgeber	69
8. Implementierung im Unternehmen	70
a) Implementierung im Rahmen eines Verhaltenskodex	70
b) Implementierung im Rahmen einer Richtlinie	71
c) Möglichkeiten der Einführung entsprechender Regelungen in das Arbeitsverhältnis	72
aa) Weisung (§ 106 GewO)	72
bb) Arbeitsvertragliche Regelungen	73
cc) Betriebsvereinbarung	75
dd) Tarifvertrag	76
ee) Zusammenfassung	76

III. Beachtung von Mitbestimmungsrechten des Betriebsrats	77
1. Zwingende Mitbestimmung	78
a) Mitbestimmung nach § 87 Abs. 1 Nr. 1 BetrVG	78
b) Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG	79
2. Freiwillige Mitbestimmung und Kooperation mit dem Betriebsrat	80
3. Zuständigkeitsfragen	80
a) Betriebsrat	80
b) Gesamtbetriebsrat	81
c) Konzernbetriebsrat	81
IV. Ausgestaltung des Meldeprozesses	82
1. Schutz des Hinweisgebers	83
2. Hinweis	83
a) Schranken privater Lebenssachverhalte	84
b) Inhaltliche Bestimmung	85
c) Hinweisgeberkreis	86
d) Zeitliche Komponente	86
e) Fehlverhalten Dritter	87
f) Weitere Einschränkungen	87
3. Meldekanäle	88
a) Gesetzliche Rahmenbedingungen	88
b) Vertraulichkeit des Hinweisgebersystems	89
c) Praktische Umsetzung	91
d) Einzelne Meldekanäle	91
aa) Elektronische Meldekanäle	92
bb) Telefon-Hotline	92
cc) Fachabteilungen und Management	92
dd) Externe Ombudsperson	93
V. Aufklärung	93
1. Prozess	94
2. Untersuchungsschritte	94
a) Kommunikation mit dem Hinweisgeber	95
b) Vorprüfung	95
c) Kategorisierung	95
d) Vorbereitung der internen Untersuchung	96
3. Handlungsprinzipien	97
4. Abschluss der internen Untersuchung	98
VI. Remediation	98

5. Kapitel

Beachtung datenschutzrechtlicher Vorgaben

I. Einleitung und Begriffsbestimmung	101
II. Rechtlicher Rahmen	102
III. Anwendungsbereich	103
1. Anwendungsbereich der DSGVO	103
2. Anwendungsbereich des BDSG n.F.	103

IV. Grundlegende Erwägungen vor der Einführung eines Hinweisgebersystems	104
V. Rechtsgrundlage für die Datenverarbeitung	105
1. Rechtmäßigkeit der Verarbeitung – Art. 6 DSGVO	105
a) Einwilligung, Art. 6 Abs. 1 lit. a) DSGVO	106
aa) Freiwilligkeit	106
bb) Bestimmtheit und Information	107
cc) Keine Einwilligung in die Verarbeitung von Daten Dritter	107
dd) Widerruflichkeit der Einwilligung	107
b) Vertragliche Zwecke, Art. 6 Abs. 1 lit. b) DSGVO	108
c) Rechtliche Verpflichtung, Art. 6 Abs. 1 lit. c) DSGVO	108
d) Berechtigte Interessen, Art. 6 Abs. 1 lit. f) DSGVO	109
2. Nationale Erlaubnisnormen auf der Grundlage von Art. 88 DSGVO:	
§ 26 BDSG n.F.	111
a) § 26 Abs. 1 S. 1 BDSG n.F.	111
b) § 26 Abs. 1 S. 2 BDSG n.F.	111
c) Betriebsvereinbarung, § 26 Abs. 4 BDSG n.F.	112
VI. Verarbeitung strafrechtlich relevanter Daten – Art. 10 DSGVO	112
VII. Anonymität des Hinweisgebers	113
VIII. Interner vs. externer Betrieb des Hinweisgebersystems, Datenübermittlungen	116
IX. Information der betroffenen Person	118
X. Sicherheit der Datenverarbeitung	120
XI. Einbindung des Datenschutzbeauftragten und Datenschutzfolgenabschätzung	121
XII. Einbindung des Betriebsrats	122
XIII. Datenlöschung	122
XIV. Empfehlungen aus datenschutzrechtlicher Sicht	123

6. Kapitel

Informationen aus Hinweisgebersystemen im Lichte strafprozessualer Ermittlungshandlungen

I. Staatliche Ermittlungsmaßnahmen gegenüber interner Ombudsperson	126
1. Vernehmung als Zeuge	126
2. Durchsuchung und Beschlagnahme	126
3. Syndikusanwalt als interne Ombudsperson	127
II. Strafprozessuale Ermittlungsmaßnahmen bei externer Ombudsperson	128
1. Vernehmung als Zeuge	129
2. Durchsuchung und Beschlagnahme bei externer Ombudsperson	130
3. Grundsätze der Beschlagnahme von Informationen aus internen Untersuchungen	132

III. Beschlagnahmeschutz durch Regelungen in EU-Hinweisgeberrichtlinie und Hinweisgeberschutzgesetz?	136
IV. Ausblick auf mögliche Änderungen durch das Verbandssanktionengesetz	138

7. Kapitel

Praktische Herausforderungen und Lösungen

I. Einleitung	141
II. Herausforderungen meistern	144
1. Meldekultur sicherstellen	144
a) Verhaltenskodex und interne Hinweisgeber-Richtlinie	145
b) Die Rolle des Managements	146
c) Vorteile und Nutzen verständlich kommunizieren	147
2. Konkrete Ausgestaltung des Hinweisgebersystems – organisatorische und technische Maßnahmen, um hilfreiche Meldungen zu erhalten	149
a) Organisatorische und technische Anforderungen	149
b) Anforderungen an Hinweisempfänger	150
c) Vertraulichkeit sicherstellen	151
d) Welche Kanäle sollen angeboten werden?	151
3. Kreis möglicher Hinweisgeber und zulässiger Hinweisgegenstände	153
4. Verpflichtungen zu und Prämien für Meldungen?	155
5. Risiko des Missbrauchs und Sanktionen gegen böswillige Falschmeldungen	156
6. Kommunikation und Training – Bekanntheit der Kanäle sicherstellen und Hilfe zur Nutzung bieten	157
7. Die ersten Schritte nach dem Eingang eines Hinweises – Plausibilisierung, Kategorisierung und Feedback	159
8. Ermittlungen und Folgemaßnahmen	161
9. Monitoring und Reporting	162

8. Kapitel

Länderteil Österreich

I. Einleitung	165
1. Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption (WKStA)	165
2. Finanzmarktaufsichtsbehörde	166
II. Rechtspflicht zur Einführung von Hinweisgebersystemen in österreichischen Unternehmen?	166
1. § 99g BWG	167
2. §§ 95 Abs. 1, 195 Abs. 1 BörseG	167
3. § 40 Abs. 1 FM-GwG	167
4. Bislang Ermessensspielraum in sonstigen Fällen	168
III. Beachtung arbeitsrechtlicher Vorgaben	169
1. § 96 Abs. 1 Ziff. 3 ArbVG	169
2. § 10 AVRAG	170

IV. Beachtung datenschutzrechtlicher Vorgaben	171
1. Begriffsbestimmung	171
2. Rechtlicher Rahmen	172
3. Anwendungsbereich der DSGVO	173
4. Grundlegende Erwägungen vor der Einführung eines Hinweisgebersystems	173
5. Rechtsgrundlage für die Datenverarbeitung	174
a) Rechtmäßigkeit der Verarbeitung – Art. 6 DSGVO	174
aa) Einwilligung, Art. 6 Abs. 1 lit. a) DSGVO	175
(1) Freiwilligkeit	175
(2) Bestimmtheit und Information	175
(3) Keine Einwilligung in die Verarbeitung von Daten Dritter	176
(4) Widerruflichkeit der Einwilligung	176
bb) Vertragliche Zwecke, Art. 6 Abs. 1 lit. b) DSGVO	176
cc) Rechtliche Verpflichtung, Art. 6 Abs. 1 lit. c) DSGVO	177
dd) Berechtigte Interessen, Art. 6 Abs. 1 lit. f) DSGVO	177
b) Verarbeitung strafrechtlich relevanter Daten – Art. 10 DSGVO	179
c) Betriebsvereinbarung oder arbeitsrechtliche Zustimmung	179
6. Anonymität des Hinweisgebers	180
7. Interner vs. externer Betrieb des Hinweisgebersystems, Datenübermittlungen	182
8. Konzerninterne Datenübermittlung	184
9. Information der betroffenen Person	185
10. Sicherheit der Datenverarbeitung	187
11. Einbindung des Datenschutzbeauftragten und Datenschutzfolgenabschätzung	187
12. Datenlöschung	188
13. Empfehlungen für die Implementierung in Österreich	189

9. Kapitel

Länderteil Schweiz

I. Einleitung	191
II. Anforderungen an Compliance-Programme, einschließlich Hinweisgebersysteme	193
1. Grundlegendes	193
2. Gesellschaftsrechtliche Vorgaben	194
3. Strafrechtliche Sanktionierung	195
4. Verwaltungs(straf)recht	197
5. Ausgestaltung des Compliance-Programms	197
III. Whistleblowing aus Sicht des Hinweisgebers	199
1. Ausgangspunkt und Umfeld von Hinweisen	199
2. Melderecht oder Meldepflicht? Je nach Stellung im Unternehmen	201
3. Adressat der Meldung	206
4. Kaskade der Meldeadressaten gem. bundesgerichtlicher Rechtsprechung	208

IV. Whistleblowing aus Sicht des Unternehmens	210
1. Pflicht zur Entgegennahme und Bearbeitung von Hinweisen?	210
2. Verfahren im Allgemeinen und Vorgehen bei internen Untersuchungen	211
3. Maßnahmen aufgrund festgestellter Ergebnisse; Kündigungsschutz ...	214
V. Whistleblowing aus Sicht der betroffenen Personen	215
1. Mitwirkungspflicht bei internen Untersuchungen	215
2. Schutzmaßnahmen und Verteidigungsrechte	216
VI. Hinweisgebersysteme in internationalen Konzernen	218
VII. Melde- und Informationspflichten betreffend den Betrieb von Hinweisgebersystemen	221
VIII. Zusammenfassung und Empfehlungen für die Implementierung in der Schweiz	222
<i>Stichwortverzeichnis</i>	225