

Inhaltsverzeichnis

Vorwort	V
Verzeichnis der Autorinnen und Autoren	XV
Abkürzungsverzeichnis	XVII

1. Teil Hinweisgebersysteme in Unternehmen

1. Kapitel Rechtsgrundlagen von Hinweisgebersystemen	1
I. Einleitung	2
II. Hinweisgebersysteme als effektiver Bestandteil eines CMS	2
A. Der Begriff „Whistleblowing“	3
B. Implikationen für die hinweisgebende Person und die betroffene Organisation	4
III. Internationale Standards und Vorgaben	4
A. US Foreign Corrupt Practices, DOJ- und SEC-Vorgaben sowie Sentencing Guidelines	5
B. UK Bribery Act und adequate procedures	6
C. Sapin II	7
D. ISO 37001	7
IV. EU-Hinweisgeberrichtlinie	7
V. Nationale Rechtsgrundlagen	9
A. § 99g BWG	9
B. §§ 95 Abs 1, 195 Abs 1 BörseG	10
C. § 40 Abs 1 FM-GwG	10
D. HinweisgeberInnenschutzgesetz	10
2. Kapitel Das HinweisgeberInnenschutzgesetz in der Unternehmenspraxis	13
I. Einleitung	15
II. Persönlicher Geltungsbereich	16
III. Sachlicher Geltungsbereich	17
IV. Schutzwürdigkeit von Hinweisgebenden	18
V. Arbeitsrechtliche Vorgaben bei der Implementierung	21
A. §§ 96, 96a ArbVG	21
B. § 10 AVRAG	23
C. (Keine) Erforderlichkeit einer Zustimmung	23
VI. Datenschutzrechtliche Vorgaben	24
VII. Detailfragen der Praxis nach Inkrafttreten des HSchG	26
A. Keine Sanktionierung ohne Einrichtung	26
B. Das Verhältnis von internen und externen Meldestellen	27
C. Das Verhältnis zu bereits bestehenden Systemen für Hinweisgebende	27
D. Sicherstellung des Identitätsschutzes	28
E. Ungerechtfertigte Maßnahmen gegen Hinweisgebende	28
F. Sanktionen bei Verstößen	29
VIII. Praktische Weichenstellungen, Herausforderungen und Lösungen	29
A. Interne Meldungen versus externe Meldungen bzw Offenlegung	29
B. Speak-Up-Kultur: Das Fundament für wertvolle Hinweise	30
C. Geeignete Meldekanäle wählen	30
1. Grundsätzliches zu den Meldekanälen	31

VII

2. Mündliche Hinweiserteilung	31
3. Schriftliche Hinweiserteilung	32
4. Fazit	32
D. Kreis der akzeptierten Hinweisgeber und Meldegegenstände	32
E. Anonyme Hinweise	34
F. Kommunikation	35
1. Hilfreiche Meldungen fördern	35
2. Formelle Anforderungen an die Kommunikation	36
G. Anforderungen an eine interne Meldestelle	37
H. Hinweisgebersysteme im Konzern	38
IX. Tipps für Organisationen	40
X. Tipps für hinweisgebende Personen	41
XI. Fazit	43
3. Kapitel Arbeitsrechtliche Aspekte von Hinweisgebersystemen	45
I. Einleitung	45
II. Individualarbeitsrechtlicher Schutz	46
A. Vertraulichkeit, Verschwiegenheitspflicht und Schutz der Identität	46
B. Schutz vor Vergeltungsmaßnahmen	47
III. Betriebsverfassungsrechtliche Aspekte	48
A. § 96 Abs 1 Z 3 ArbVG	48
B. § 96a Abs 1 Z 1 ArbVG	50
C. § 97 Abs 1 Z 1 ArbVG	50
D. Betriebe ohne Betriebsrat (§ 10 AVRAG)	51
IV. Zusammenfassung	52
4. Kapitel Datenschutzrechtliche Aspekte von Hinweisgebersystemen	53
I. Datenschutzrechtliche Grundsätze	53
II. Rechtsgrundlagen für die Datenverarbeitung	55
A. Überblick	55
B. Rechtsgrundlage nach Art 6 Abs 1 DSGVO	56
C. Ausnahmetatbestand für Daten nach Art 9 und 10 DSGVO	56
III. Datenschutzrechtliche Regelungen im HinweisgeberInnenschutzgesetz	57
A. Anwendungsbereich und Erlaubnistratbestände des § 8 HSchG	57
1. Verhältnis zur DSGVO	57
2. Datenkategorien und Zwecke	58
3. Betroffene Personen	61
B. Abgrenzung der datenschutzrechtlichen Rollen	62
C. Einschränkung der Betroffenenrechte	64
D. Aufbewahrungspflicht und Datenlöschung	66
E. Datenschutz-Folgenabschätzung	68
F. Technische und organisatorische Maßnahmen	69
G. Identität und Anonymität des Hinweisgebers	70
IV. Konzerninterne und sonstige Datenübermittlung	71
V. Praxisempfehlungen für die Implementierung	72

2. Teil Untersuchungen im Unternehmen

5. Kapitel Organisation, Planung und Durchführung von internen Untersuchungen	75
I. Grundlagen interner Untersuchungen	77
A. Der Begriff „Interne Untersuchung“	78
B. Pflicht zur Sachverhaltaufklärung	79

C. Plausibilitätsprüfung	80
1. Vorgelagerte Plausibilitätsprüfung	80
2. Definition der relevanten „Aufgreifschwelle“	81
3. Rechtliche Erstbewertung des Verdachts	82
4. Dokumentation des Prüfungsergebnisses	83
D. Sofortmaßnahmen	83
E. Einbeziehung des Betriebsrats	83
F. Entscheidung über Kooperations- und Amnestievereinbarungen	84
1. Grundsätze der Ausgestaltung von Amnestieprogrammen	84
2. Risiken bei Übernahme von Verfahrens- oder Verteidigungskosten, Geldstrafen, Geldbußen und Geldauflagen	86
G. Zuständigkeit für interne Untersuchungen im Unternehmen	87
1. Aktiengesellschaft	87
2. GmbH	87
H. Internes Untersuchungsteam oder externer Rechtsanwalt	88
I. Umgang mit Behörden	89
1. Zu treffende Entscheidungen ohne laufendes Ermittlungsverfahren	89
a) Prüfung und Vorbereitung einer tätigen Reue	89
b) Prüfung einer Anzeigepflicht nach § 139 BAO	92
c) Prüfung und Vorbereitung einer Selbstanzeige (§ 29 FinStrG) bei Finanzvergehen	93
d) Prüfung einer Inanspruchnahme von Kronzeugenregelungen	94
e) Prüfung einer frühzeitigen Kontaktaufnahme zu Ermittlungsbehörden	95
2. Parallel staatliche Ermittlungsmaßnahmen	96
3. Interne Untersuchung aufgrund eines staatlichen Ermittlungsverfahrens	97
II. Untersuchungsauftrag und Einleitung der internen Untersuchung	97
III. Erstellen eines Untersuchungsplans	98
A. Konzeption	99
B. Ablaufplanung und Untersuchungschronologie	100
C. Ressourcenplanung	101
D. Controlling	102
E. Qualitätssicherung	102
F. Steuerung	103
IV. Durchführung der internen Untersuchung	103
A. Identifikation der relevanten Informationen, Daten und Dokumente sowie betroffenen Beschäftigten	103
B. Prüfung der rechtlichen Rahmenbedingungen	104
C. Untersuchungsmaßnahmen	104
D. Laufende Berichterstattung	105
1. Laufende Berichterstattung innerhalb des Untersuchungsteams	105
2. Laufende Berichterstattung an Auftraggeber	105
3. Laufende Berichterstattung an Behörden	105
V. Abschlussbericht	105
A. Anlass der internen Untersuchung	106
B. Gang der internen Untersuchung	106
C. Ergebnisse der internen Untersuchung	106
D. Sanktion oder Rehabilitation gegenüber Beschäftigten	106
E. Entscheidung über Strafanzeige oder Strafantrag	107
F. Empfehlungen zu Reaktions- und Präventionsmaßnahmen im CMS	108
1. Prozess-Analyse	108
2. Schwachstellen im internen Kontrollsystem	108
3. Zuständigkeiten und Organisation	109
4. Verantwortlichkeit und Follow-up	109

VI.	Abschluss der internen Untersuchung sowie Information der Organe und zuständigen Stellen	109
VII.	Nachverfolgung der Umsetzung der empfohlenen Optimierungs- und Reaktionsmaßnahmen	110
VIII.	Praxisleitfaden für interne Untersuchungen	110
6. Kapitel	Zulässigkeit und Grenzen interner Untersuchungsmaßnahmen	115
I.	Einleitung	116
II.	Inaugenscheinnahme des Arbeitsplatzes	116
III.	Videoüberwachung	117
IV.	Einsicht und Auswertung dienstlicher Akten und Unterlagen	117
V.	Befragung von Mitarbeitern	118
A.	Teilnahmepflicht	118
B.	Auskunftspflicht	118
C.	Hinzuziehung eines Rechtsanwaltes oder Betriebsratsmitglieds	121
D.	Belehrungspflicht	121
VI.	Kontrolle von Telefongesprächen	122
VII.	Tonbandaufnahme von Gesprächen	123
VIII.	Standesrechtliche Risiken für externe Rechtsanwälte oder Wirtschaftsprüfer	123
IX.	Überwachung und Auswertung von E-Mails	124
X.	Richtlinie für interne Untersuchungen	125
7. Kapitel	Arbeitsrechtliche Aspekte interner Untersuchungen	127
I.	Einleitung	128
II.	Individualarbeitsrechtliche Aspekte	129
A.	Fürsorgepflicht	129
B.	Treuepflicht	130
C.	Melde- und Anzeigepflichten	131
D.	Mitwirkungspflicht bei Befragungen	131
E.	Aussageverweigerungsrecht	132
III.	Betriebsverfassungsrechtliche Aspekte	133
A.	Präventive Kontrollmaßnahmen und Betriebsrat	133
1.	Allgemeines	133
2.	Kontrollmaßnahmen, die die Menschenwürde berühren	133
3.	Sonstige Kontrollmaßnahmen	135
B.	Konkrete Untersuchungen und Betriebsrat	135
1.	Mitwirkungsrechte	135
2.	Beziehung des Betriebsrates bei Befragungen	136
C.	Beispiele für Kontroll- und Untersuchungsmaßnahmen	137
1.	Mitarbeiterinterviews	137
2.	Telefonanlagen	137
3.	E-Mail und Internet-Nutzung	138
4.	Videoüberwachung	139
5.	Detektiv	139
IV.	Arbeitsrechtliche Konsequenzen	140
A.	Allgemeines	140
B.	Dienstfreistellung	140
C.	Verwarnung	141
D.	Beendigung des Dienstverhältnisses	142
1.	Kündigung	142
2.	Entlassung	143
E.	Schadenersatzansprüche gegen den Arbeitnehmer	144

8. Kapitel Datenschutzrechtliche Aspekte interner Untersuchungen	147
I. Einführung und datenschutzrechtliche Rechtsgrundlagen	148
II. Zwecke der Datenverarbeitung	154
III. Untersuchungsmethoden	157
A. Screening von Inhalten	157
B. Mitarbeiterinterviews	159
C. Sonderfall Videoüberwachung	159
IV. Verarbeitung besonderer Kategorien von personenbezogenen Daten	160
V. Verarbeitung strafrechtlich relevanter Daten	161
VI. Betroffenenrechte	162
A. Recht auf Auskunft (Art 15 DSGVO)	162
B. Recht auf Berichtigung (Art 16 DSGVO)	163
C. Recht auf Widerspruch (Art 21 DSGVO)	164
D. Recht auf Löschung und Speicherbegrenzung	165
9. Kapitel Computerforensische Untersuchungen	167
I. Grundlagen der IT-Forensik	169
A. Begriffsdefinition Digitale Forensik	169
B. Arten der Datenspeicherung	169
C. Gerichtsverwertbare Sicherung	169
D. Datenintegrität	170
E. Dokumentation	170
F. Aufbewahrung von Beweismitteln	171
G. Forensic Readiness	171
II. IT-forensische Hardware und Software	172
A. Writeblocker	172
B. Datensicherung von Smartphones	172
C. Datensicherung Internet of Things	173
D. Software für forensische Datensicherung	173
E. Software zur forensischen Analyse von unstrukturierten Daten	174
F. Software zur forensischen Analyse von strukturierten Daten	174
III. Durchführung einer IT-forensischen Untersuchung	175
A. Untersuchungsziel festlegen	175
B. Planung der Untersuchungsschritte	175
1. Identifikation der Ansprechpartner	175
2. Zugriffsmöglichkeiten	175
C. Datensicherung/Datenanalyse/Berichterstattung	176
IV. IT-forensische Datensicherung	176
A. Beweismittelkette	176
B. IT-forensische Methoden	177
1. Offline/Live-Sicherung	177
2. Physische und logische Datensicherung	177
3. Volatilität von elektronischen Informationen	178
4. Unterscheidung strukturierte und unstrukturierte Daten	178
C. IT-Landscaping	179
1. Identifikation von Datenquellen	179
a) Inventarisierungssystem	179
b) Altsysteme/Backup	179
c) Cloud	180
D. Datensicherung in der Praxis	180
1. Datenträger	180
2. Computer	181
3. RAM	182

4. Mobiltelefon	182
5. Lokale Serverdaten	183
6. Virtuelle Maschinen	184
7. Cloud-Daten	184
8. ERP-Systeme	184
9. Physische Zutrittssysteme/CCTV	185
10. Dokumentation Datensicherung	185
11. Datenträger vs RAM Sicherung	185
12. Unterschiede HDD/SSD	186
E. Datentransport/-transfer	186
V. IT-forensische Datenanalyse	187
A. Strukturierte Daten	187
1. Analyse von Log Dateien	187
2. Analyse von ERP-Daten	187
B. Unstrukturierte Daten	187
1. Analyse von Datenträgern	188
2. Analyse von mobilen Endgeräten	188
C. eDiscovery	188
1. Begriffsdefinition	188
2. EDRM-Modell	188
3. eDiscovery Tools	189
4. Grundlagen der Datenaufbereitung	190
a) Vorfilterung	190
b) Wiederherstellung gelöschter Daten	190
c) Indexierung	191
d) Texterkennung (Optical Character Recognition OCR)	191
e) Entschlüsselung	191
f) E-Mail Threading	191
5. Early Case Assessment	192
6. Suchen im Datensatz	192
7. Strukturierter Review	193
8. KI-Methoden	193
9. Production/Export der Dokumente	193
D. OSINT Recherchen	193
E. Informationsgespräche	194
VI. Berichterstattung IT-forensischer Untersuchungen	194
VII. Forensische Artefakte	194
A. Verwendete USB-Geräte	194
B. Benutzeranmeldungen und Zeitpunkte	195
C. Besuchte Webseiten und andere Browserinformationen	195
D. VPN-Verbindungen und Remote Desktop Verbindungen	195
E. Gelöschte Dateien	195
F. Cloudspeicherdienste	196
G. Zuletzt verwendete Dateien	196
H. Kommandozeilenbefehle	196
I. Geolokationsinformationen	196
J. Druckaufträge	197
K. Verschlüsselte Informationen	197
L. Lokale Mailbox-Kopien	198
M. Timeline-Analyse	198
VIII. Tatbestände in der Praxis und die Rolle der digitalen Forensik bei der Aufklärung	198
A. Data Leakage Investigations	198
B. Incident Response – Ransomware	199

C. Business E-Mail Compromise	200
D. Kartellrechtliche Untersuchungen	200
E. Unberechtigter Zugriff auf Informationen	201
F. Phishing	201
G. Unregelmäßigkeiten in ERP-Daten	202
10. Kapitel Informationen aus internen Untersuchungen im Lichte staatlicher Ermittlungsmaßnahmen	203
I. Einfluss staatlicher Ermittlungen auf interne Untersuchungen	204
A. Einleitung	204
B. Interne Untersuchung vs staatliche Ermittlung	205
C. Parallellauf von Untersuchung und Ermittlung	206
1. (Keine) Pflicht zur Informationsweitergabe an die Behörden	206
2. Freiwillige Kooperation mit den Behörden?	206
a) Gründe für und gegen eine Kooperation	206
b) Form der Kooperation	208
3. Weitergabe der Untersuchungsergebnisse nach Abschluss	208
4. Laufende Kooperation	209
a) Einleitung eines Ermittlungsverfahrens während der Durchführung der internen Untersuchung	209
b) Einleitung einer internen Untersuchung während eines laufenden Ermittlungsverfahrens	210
5. Keine Kooperation	211
II. Befragung interner Ermittler	212
A. Rechtliche Grundlagen für Zeugenbefragungen	212
B. Das Aussageweigerungsrecht	212
1. Vernehmung des Rechtsanwalts	212
2. Vernehmung von Hilfspersonen	214
3. Vernehmung unternehmensinterner Personen	215
III. Sicherstellung interner Informationen	216
A. Rechtliche Grundlagen staatlicher Zwangsmaßnahmen	216
1. Begründung von Verfügungsmacht durch Sicherstellung	216
2. Durchsuchung von Orten	217
B. Sicherstellung von Informationen	217
1. Vom Berufsgeheimnis geschützte Dokumente	217
2. Widerspruchsrecht	218
3. Rechtsträger	219
a) Berufsgeheimnisträger	219
b) Hilfskräfte	220
c) Der Mandant	220
d) Dritte	221
IV. Fazit	221
11. Kapitel Interne Untersuchungen mit internationalem Bezug	223
I. Einleitung	224
II. Pflicht zur Umsetzung internationaler Untersuchungen	225
A. Compliance-Verantwortung für ausländische Tochtergesellschaften	225
1. Compliance-Verantwortung im Konzern	226
2. Besonderheiten durch die EU-Lieferkettenrichtlinie	227
B. Formen internationaler Untersuchungen	227
1. Szenario 1: Zentral gesteuerte Untersuchung	228
2. Szenario 2: Zentral gesteuerte Untersuchung durch lokale Berater	228
3. Szenario 3: Lokal umgesetzte Untersuchung	229

III. Vorbereitung einer Auslandsuntersuchung	230
A. Festlegung des Untersuchungsgegenstandes	230
B. Auswahl und Beauftragung ausländischer Berater	232
1. Berater in der Heimatrechtsordnung	232
2. Lokale Berater	233
a) Auswahl lokaler Berater	233
b) Mandatierung lokaler Berater	233
3. Reichweite von Beschlagnahmefreiheit und Legal Privilege	234
C. Vorabprüfung des ausländischen Rechtsrahmens	235
1. Anzeige- und Meldepflichten nach ausländischem Recht	236
2. Besonderheiten im strafrechtlichen Rahmen	237
a) Strafrechtliche Bewertung des Verdachts	237
b) Erhebliche und drakonische Strafandrohungen	238
c) Strafrechtliche Grenzen der geplanten Ermittlungsmaßnahmen	238
aa) Grenzen aus dem zu untersuchenden Straftatbestand selbst	238
bb) Grenzen aus anderen Straftatbeständen	239
3. Besondere arbeits- und gesellschaftsrechtliche Anforderungen	240
4. Anforderungen an grenzüberschreitenden Datentransfer	241
IV. Ablauf einer Untersuchung im Ausland	243
A. Involviering der lokalen Geschäftsführung und lokaler Compliance-Verantwortlicher	244
B. Arbeitsteilung mit ausländischen Beratern	244
1. Forensische Auswertung	244
2. Interviewführung	245
C. Interviewführung und Umgang mit Sprachbarrieren und kulturellen Besonderheiten	245
D. Beteiligung oder Einbindung ausländischer Ermittlungsbehörden	246
1. Untersuchungen bei bereits laufenden Ermittlungen	246
2. Selbstanzeige an lokale Ermittlungsbehörden	247
3. Selbstanzeige bei Anwendbarkeit mehrerer Rechtsordnungen gleichzeitig	247
E. Untersuchungen in mehreren Rechtsordnungen gleichzeitig	248
V. Untersuchungsergebnisse und Folgemaßnahmen	249
A. Dokumentation und Kommunikation der Untersuchungsergebnisse	249
B. Umsetzung von Folgemaßnahmen und deren Kontrolle	250
VI. Besonderheiten durch unterschiedliche Umsetzung der EU-Whistleblower-Richtlinie	252
A. Vorgaben durch die Richtlinie	252
B. Besonderheiten in der Umsetzung am Beispiel ausgesuchter Rechtsordnungen	253
1. Deutschland	253
2. Schweden	254
3. Spanien	254
Stichwortverzeichnis	255