

Inhaltsverzeichnis

Einleitung	17
Gang der Untersuchung	25

1. Kapitel

Begriffsbestimmungen und Grundlagen	28
A. Whistleblowing	28
I. Internes Whistleblowing	30
II. Externes Whistleblowing	30
III. Anonymes, vertrauliches und offenes Whistleblowing	30
B. Hinweisgebersysteme	31

2. Kapitel

Hinweisgebersysteme als Compliance-Element	33
A. Compliance zur Bekämpfung von Unternehmenskriminalität	33
I. Compliance	33
1. Der Begriff (Criminal-)Compliance	34
2. Rechtsgrundlagen	35
3. Rechtspflicht	36
4. Wert von Compliance-Maßnahmen	37
a) Bußgeldausschließende Wirkung	38
b) Bußgeldmindernde Wirkung	40
c) Weitere Vorteile eines wirksamen Compliance-Systems	41
II. Neue Anreize durch ein Verbandssanktionengesetz?	43
1. Erweiterung des Sanktionsspektrums	45
2. Einführung des Legalitätsgrundsatzes	46
3. Sanktionserlass oder -milderungen bei Compliance-Maßnahmen	47
a) Vermeidung der Zurechnung	47
b) Verwarnung mit Verbandsgeldsanktionsvorbehalt	48
c) Sanktionsmilderung	48

4. Auswirkung eines VerSanG auf Hinweisgebersysteme	50
III. Compliance-Pflichten aufgrund des Lieferkettensorgfaltspflichtengesetzes	51
1. Anwendungsbereich	51
2. Sorgfaltspflichten	52
3. Verpflichtung zu internen Beschwerdestellen	53
4. Dokumentationspflichten	54
5. Zwischenfazit	54
B. Typische Merkmale von Wirtschaftsstraftaten	55
I. Erhebliches Schadenspotential	55
II. Unternehmensinterne Täter	56
III. Niedriges Entdeckungsrisiko	57
IV. Fehlendes Unrechtsbewusstsein der Täter	58
V. Fazit	59
C. Nutzen von Hinweisgebersystemen	60
I. Vorteile für Unternehmen	60
1. Frühwarnsystem	61
2. Filterfunktion und Kontrollmechanismus	61
3. Möglichkeit der Schadensabwehr	63
4. Generalpräventive Wirkung	63
5. Positive Außenwirkung	65
II. Vorteile für den Rechtsstaat	66
III. Vorteile für den Hinweisgeber	68
IV. Fazit	69
D. Conclusio	70

3. Kapitel

Rechtliche Regelungen zum Whistleblowing	72
A. Status quo der Rechtslage in der Bundesrepublik Deutschland	72
I. Pflicht zur Implementierung von Hinweisgebersystemen	72
II. Gesetzlicher Schutz von Hinweisgebern	75
1. Arbeitsrechtlicher Schutz	76
2. Strafrechtlicher Schutz	79
III. Fazit	80
B. Harmonisierung durch die Whistleblower-Direktive 2019/1937	81
I. Hintergrund	82
II. Regelungspunkte	84
1. Persönlicher Anwendungsbereich	84
2. Sachlicher Anwendungsbereich	85

3. Pflicht zu internen Whistleblowingstellen	86
4. Staatliche Whistleblowingbehörde	87
5. Offenlegung als Ultima Ratio	87
6. Vertraulichkeitsgebot	88
7. Hinweisgeberschutz	88
III. Fazit	89
C. Umsetzungsspielräume der nationalen Gesetzgeber	89
I. Hinweisgeberschutz- oder Artikelgesetz	89
II. Ausweitung auf nationales Recht	91
III. Institution der Whistleblowingbehörde	92
IV. Anonymes Whistleblowing	93
V. Whistleblowingprämie	95
VI. Fazit	97
D. Umsetzung in Deutschland	99
I. Referentenentwurf 2020 (HinSchG-E 2020)	99
II. Referentenentwurf 2022 (HinSchG-E 2022)	101
III. Regierungsentwurf 2022 (HinSchG-RegE 2022)	102
1. Anwendungsbereich	103
2. Hinweisgebersysteme	104
3. Hinweisgeberschutz	105
4. Bewertung	106
IV. Nicht fristgemäße Umsetzung	107
E. Conclusio	108

4. Kapitel

Die Strafbarkeitsrisiken des potenziellen Hinweisgebers

110

A. Strafbewehrte Offenlegungspflichten	111
I. Anzeigepflichten bei Wirtschaftsstraftaten	111
II. Handlungspflichten resultierend aus einer Garantenstellung	114
1. Garantenstellung der Unternehmensleitung	114
2. Garantenstellung des Compliance-Officer	118
3. Garantenstellung von sonstigen Arbeitnehmern	121
III. Offenlegungspflichten durch die WBRL	121
IV. Fazit	122
B. Strafrechtliche Risiken bei der Hinweisabgabe	123
I. Strafbarkeit wegen Geheimnisverrats	123
1. Schutz von Geschäftsgeheimnissen nach § 23 GeschGehG	124
a) Tatbestandsmäßigkeit „illegaler Geheimnisse“?	125

b) Tatbestandsausnahme nach § 5 GeschGehG	126
aa) Voraussetzungen	126
bb) Eskalationserfordernis?	128
c) Änderungen durch die WBRL	129
2. Zwischenergebnis	130
3. Geheimhaltungspflichten für Organmitglieder	131
II. Verletzung von Privatgeheimnissen	132
1. De lege lata	133
2. Änderungen durch die WBRL	135
III. Strafbarkeit aufgrund der Beschaffung von Informationen	137
1. De lege lata	137
2. Änderungen durch die WBRL	139
IV. Strafrechtliche Risiken bei Falschmeldungen	139
1. De lege lata	140
a) Delikte gegen die Rechtspflege	140
b) Ehrverletzungsdelikte	141
aa) Bewusste Falschmeldung	141
bb) Fahrlässige Falschmeldung	142
2. Änderungen durch die WBRL	143
V. Vorschlag eines Rechtfertigungsgrundes	145
VI. Fazit	147
C. Conclusio	148

5. Kapitel

Implementierung von internen Hinweisgebersystemen in Unternehmen	150
A. Ausgestaltung der Whistleblowing-Systeme	151
I. Abstimmung mit den Beteiligten	152
II. Vorgaben nach der WBRL	152
1. Vorgaben bezüglich der Ausgestaltung	153
2. Vorgaben bezüglich des Verfahrens	153
3. Vorgaben bei Wiederaufgreifen des VerSanG-E 2020	154
III. Umgang mit der Identität des Hinweisgebers	155
B. Einrichtungsmodalitäten	156
I. Unternehmensinterne Meldestelle	156
II. Ombudsperson	157
III. Elektronische Systeme	160
1. Internetbasierte Systeme	160
2. Hotline/Callcenter	161

IV. Fazit	162
C. Weitere Modalitäten	163
I. Einführung einer Meldeverpflichtung	163
II. Implementierung monetärer Anreize	165
III. Kombination mit digitalem „Selbst-Check“	166
D. Conclusio	166

6. Kapitel

Vertraulichkeitszusicherung und private Auskunftsansprüche	169
A. Einsichtsrecht in die Personalakte nach § 83 BetrVG	169
I. De lege lata	171
II. Einschaltung einer externen Stelle	171
III. Einschränkungsmöglichkeiten nach der WBRL	172
IV. Fazit	172
B. Datenschutzrechtliche Auskunft- und Informationspflichten	173
I. Auskunftsrechte bei unternehmensinternen Systemen	175
1. Unterrichtungspflicht	175
a) Art. 14 DSGVO	175
b) Einschränkungsmöglichkeiten de lege lata	176
2. Auskunftsanspruch	178
a) Art. 15 DSGVO	178
b) Einschränkungen de lege lata	179
3. Zwischenergebnis	180
II. Aspekte bei Einsatz eines unternehmensexternen Systems	180
1. Ombudsperson	181
2. Elektronische Hinweisgebersysteme	181
III. Einschränkungsmöglichkeiten nach der WBRL	182
C. Conclusio	184

7. Kapitel

Vertraulichkeitsversprechen und strafprozessuale Zugriffsrechte	185
A. Zugriffsrechte bei unternehmensinternen Hinweisgebersystemen	187
I. Interne Empfänger als Zeugen	187
II. Durchsuchungs- und Beschlagnahmemöglichkeiten	188
III. Mehr Schutz durch Beauftragung von Syndikus-Anwälten?	188

B. Zugriffsrechte bei Beauftragung einer anwaltlichen Ombudsperson	189
I. Zeugnisverweigerungsrecht	189
II. Entbindung von der Schweigepflicht	193
1. Verpflichtung des Unternehmens zur Entbindung von der Schweigepflicht? ..	193
2. Berechtigung zur Entbindung	193
3. Zwischenergebnis und Ausblick in die Zukunft	195
III. Durchsuchungs- und Beschlagnahmemöglichkeiten	196
1. Relevante Entscheidungen	196
a) HSH Nordbank-Verfahren	197
b) LG Bonn	198
c) LG Mannheim	199
d) LG Saarbrücken	199
e) LG Braunschweig	200
f) LG Bochum	200
g) LG Stuttgart	202
h) Die Beschlüsse des BVerfG in der Sache „Jones-Day“	202
2. Erörterung der Entscheidungen und der Rechtslage	204
a) Genereller Beschlagnahmeschutz anwaltlich erstellter Unterlagen	205
aa) Schutz vor Beschlagnahme gem. § 97 Abs. 1 Nr. 3 StPO	205
bb) Schutz vor Durchsuchungen und Beschlagnahme nach § 160a StPO ...	207
b) Änderungen durch Neuregelung der Verbandssanktionierung	210
c) Beschlagnahmeschutz bei einer Ombudsperson	211
aa) Mandatsähnliches Verhältnis zum Hinweisgeber	212
bb) Mandatsverhältnis zum Unternehmen	214
(1) Beschuldigtenstellung des Unternehmens	215
(2) Verteidigerstatus	216
d) Beschlagnahmeschutz aus Verfassungsrecht	218
aa) Grundrechtsbetroffenheit des Hinweisgebers	219
(1) Recht auf informationelle Selbstbestimmung	219
(2) Selbstbelastungsfreiheit	220
bb) Grundrechtsbetroffenheit des Unternehmens	222
(1) Geheimnisschutz	222
(2) Selbstbelastungsfreiheit	223
cc) Grundrechtsbetroffenheit der Ombudsperson	224
(1) Berufsfreiheit des Rechtsanwalts, Art. 12 GG	224
(2) Freiheit der Advokatur als unverzichtbarer Bestandteil des Rechts-	
staatsprinzips	226
e) Zwischenergebnis	229
3. Abhilfe durch Verzicht auf Dokumentation	229
4. Abhilfe durch Verschlüsselung	230

IV. Unterlagen im Gewahrsam des Unternehmens	232
V. Fazit	232
C. Zugriffsmöglichkeiten bei Hinweisgebersystemen von Drittanbietern	234
I. Whistleblowing-Hotline (Callcenter)	234
II. Digitale Hinweisgebersysteme (Mailbox)	234
1. Zugriff auf Daten beim Dienstanbieter	236
2. Zugriff auf Informationen von inländischen Servern	236
a) Speicherung von Metadaten	236
b) Verschlüsselte Daten	237
c) Sicherheitslücken	240
3. Zugriff auf Informationen von ausländischen Servern	242
4. Zugriff auf Informationen beim Hinweisempfänger	244
III. Fazit	245
D. Rechtslage nach der WBRL	246
I. Unmittelbare Auswirkungen auf die staatlichen Zugriffsrechte	246
1. Einfluss der Richtlinie auf die StPO	246
2. Ausweitung des Informationspools	248
3. Auswirkungen der obligatorischen Vertraulichkeitszusicherung	248
II. Mittelbare Auswirkungen auf die staatlichen Zugriffsrechte	249
1. Höherrangige Bemessung des Hinweisgeberschutzes	250
2. Selbstbelastungsfreiheit des Hinweisgebers	250
3. Selbstbelastungsfreiheit des Unternehmens	253
4. Allgemeines Rechtsstaatsprinzip	256
5. Aushöhlung des Zeugnisverweigerungsrechts bei einer Ombudsperson	259
III. Situation bei Neuregelung der Verbandssanktionierung	261
IV. Überlegungen zur Neuregelung des Vertraulichkeitsschutzes	262
1. Vorbild US-amerikanisches legal privilege	262
2. Vorschlag eines Beschlagnahmeverbots	265
3. Zusätzliche Schutzmodalitäten	267
V. Fazit	269
E. Conclusio	271
Schlussbetrachtung	273
Literaturverzeichnis	279
Stichwortverzeichnis	318