

Sonja Kreß

Criminal Compliance und Datenschutz im Konzern



Nomos

Inhaltsverzeichnis

Abkürzungsverzeichnis	17
Einleitung	23
A. Grundproblematik	23
B. Ziel der Arbeit	24
C. Gang der Arbeit	25
D. Definition der Grundbegriffe	26
I. (Criminal) Compliance	26
II. Konzern	29
Erstes Kapitel: Die »Compliance-Pflicht« – Umfang, Ziel und Inhalt	32
A. Die Compliance-Pflicht	32
I. Auslegung des deutschen Gesellschafts- und Ordnungswidrigkeitenrecht	32
1. Grundlagen aus dem Gesellschaftsrecht	32
2. Grundlagen aus dem Ordnungswidrigkeitenrecht	34
3. Gemeinsamer Inhalt der Sorgfalts- und Aufsichtspflicht	34
4. Zwischenfazit	41
II. Compliance-Pflicht aus sonstigem Recht	41
1. Ausdrückliche Compliance-Pflichten aus Spezialgesetzen	41
2. Pflicht aus dem Deutschen Corporate Governance Kodex (DCGK)	42
3. Pflichten aus ausländischem Recht	43
B. Konzernweite Compliance-Pflicht	44
C. Ziele der Compliance-Tätigkeit	51
I. Haftung nach § 130 I 1 OWiG	51
1. Adressatenkreis	51
2. Mögliche Taten i.S.d. betrieblichen Zuwiderhandlung	53
II. Haftung des Unternehmens nach § 30 I OWiG	54
III. Strafbarkeit wegen Unterlassen	55
IV. Haftung des Vorstands bzw. des Geschäftsführers gegenüber der Gesellschaft aus § 93 II 1 AktG	56
V. Rufschädigung	56
VI. Beeinflussung der Strafzumessung	57

D.	Inhalt der Compliance-Maßnahmen	58
I.	Präventive Maßnahmen	58
II.	Repressive Maßnahmen	59
E.	Gestaltungsmöglichkeiten der Compliance-Funktion im Konzern	59
I.	»Aufhängung« der Compliance-Organisation	59
II.	Umfang Compliance-Funktion	60
III.	Ausgestaltung der Compliance-Funktion im Konzern	61
Zweites Kapitel: Berührungspunkte zwischen Compliance und Datenschutz		64
Drittes Kapitel: Maßgebliches Recht		66
A.	Geschichte des Datenschutzrechts in Deutschland	66
B.	Anwendbarkeit BDSG vs. DSGVO	72
C.	Anwendbarkeit der Datenschutzgesetze	73
I.	Sachliche Anwendbarkeit	73
1.	Rechtslage nach dem BDSG	73
a)	Positive Anwendungsvoraussetzungen nach § 1 II Nr. 3 Hs. 1 BDSG	73
aa)	Definition personenbezogener Daten (pbD)	73
bb)	Relevanter Datenumgang	76
cc)	Unter Einsatz von Datenverarbeitungsanlagen	78
dd)	»In oder aus nicht-automatisierten Dateien«	79
ee)	Zwischenergebnis	80
b)	Subsidiarität nach § 1 III 1 BDSG	80
2.	Änderung aufgrund der DSGVO	81
II.	Örtliche Anwendbarkeit	83
1.	Rechtslage nach dem BDSG	84
a)	Datenumgang durch eine deutsche verantwortliche Stelle in Deutschland	84
b)	Datenumgang durch ausländische verantwortliche Stellen in Deutschland	84
aa)	Verantwortliche Stelle mit Sitz in der EU bzw. im EWR	84
bb)	Verantwortliche Stelle mit Sitz im Drittland	87
c)	Datenumgang durch deutsche verantwortliche Stellen im Ausland	88
aa)	In einem anderen Mitgliedstaat der EU bzw. des EWR	88
bb)	In einem Drittland	89

2. Änderungen aufgrund der DSGVO	89
Viertes Kapitel: Mögliche Rechtsfolgen einer Datenschutzverletzung	92
A. Rechtsfolgen nach dem Datenschutzrecht	93
I. Ordnungswidrigkeiten	93
1. Natürliche Person als tauglicher Täter?	94
2. Relevante Tatbestände des § 43 BDSG	95
a) § 43 I Nr. 2b BDSG	95
b) § 43 I Nr. 4 BDSG	96
c) § 43 I Nr. 8 BDSG	96
d) § 43 I Nr. 8a BDSG	97
e) § 43 II Nr. 1 BDSG	97
f) § 43 II Nr. 2 BDSG	97
g) § 43 II Nr. 5 Alt. 2 BDSG	98
II. Straftaten (§ 44 I BDSG)	101
III. Änderungen aufgrund der DSGVO	102
1. Ordnungswidrigkeiten	102
2. Straftaten	106
B. Geldbuße nach § 130 OWiG	107
C. Geldbuße gegen die juristische Person (§ 30 OWiG)	108
Fünftes Kapitel: Grenzen des Datenschutzes im Konzern	110
A. Datenschutzrechtlich relevante Vorgänge im internationalen Konzern	110
B. Notwendigkeit der Rechtfertigung einer Datenerhebung	112
I. Verfassungsrechtliche Grundlage des Datenschutzrechts	112
II. Inhalt und Bedeutung des Verbots mit Erlaubnisvorbehalt	114
C. Bestimmung der Verantwortlichkeit	115
I. Verantwortliche Stelle i.S.d. Datenschutzrechts	115
II. Kein Konzernprivileg	116
III. Joint Controllershship	119
IV. Qualifizierung des Datentransfers zwischen den Compliance-Stellen des Konzerns	122
1. Kriterien für das Vorliegen einer Auftragsdatenverarbeitung	123
2. Übertragbarkeit der Grundsätze der Auftragsdatenverarbeitung auf Compliance-Tätigkeit im Konzern	126
3. Zwischenergebnis	128

D.	Zulässigkeit der datenschutzrechtlich relevanten Vorgänge	128
I.	Vorgänge innerhalb eines Konzerns	128
1.	Keine Qualifikation der für Compliance relevanten pbD als sensibel	129
2.	Rechtfertigung durch Einwilligung des Betroffenen	129
a)	Anforderungen an eine Einwilligung	129
b)	Verhältnis zu anderen Ermächtigungsgrundlagen	133
c)	Zwischenergebnis	135
3.	Anwendbarkeit und Voraussetzungen der gesetzlichen Ermächtigungsgrundlagen gemäß §§ 28 und 32 BDSG i.R.d. Compliance-Tätigkeit eines Konzerns	136
a)	Erweiterung des Anwendungsbereichs des BDSG für private Unternehmen	137
b)	Die Ermächtigungsgrundlagen aus § 32 BDSG	139
aa)	Spezifische Anwendungsvoraussetzungen des § 32 I BDSG	140
bb)	Die Ermächtigungsgrundlage des § 32 I 2 BDSG	146
cc)	Die Ermächtigungsgrundlage des § 32 I 1 BDSG	157
c)	Die Ermächtigungsgrundlagen des § 28 BDSG	166
aa)	Spezifische Anwendungsvoraussetzung des § 28 I BDSG	166
bb)	Verhältnis § 28 I 1 Nr. 2 BDSG zu § 32 BDSG	167
cc)	Die Ermächtigungsgrundlage des § 28 I 1 Nr. 1 BDSG	170
dd)	Die Ermächtigungsgrundlage des § 28 I 1 Nr. 2 BDSG	171
d)	Fazit zur Situation der datenschutzrechtlichen Ermächtigungsgrundlagen im Compliance-Bereich	177
4.	Erörterung der datenschutzrechtlichen Rechtfertigung von Compliance-Vorgängen	178
a)	Zulässigkeit repressiver Compliance-Maßnahmen	178
aa)	Allgemeines zur Abwägung	180
bb)	Auswertung der Telekommunikation	183
cc)	Befragung	207
dd)	Durchsuchung	211
ee)	Fazit zur Zulässigkeit repressiver Compliance-Maßnahmen	212
b)	Zulässigkeit präventiver Compliance-Maßnahmen	214
aa)	Allgemeines zur Abwägung	215
bb)	Schulungen	217

cc)	Mitarbeiterkontrollen	218
dd)	Hinweisgebersysteme	227
ee)	Fazit zur Zulässigkeit präventiver Compliance-Maßnahmen	231
c)	Konzerninterne Übermittlungen zu Compliance-Zwecken	232
aa)	Übermittlungen von der Konzernmutter an eine Tochtergesellschaft	233
bb)	Übermittlungen von einer Tochtergesellschaft an die Konzernmutter	235
cc)	Fazit zur Zulässigkeit konzerninterner Übermittlungen zu Compliance-Zwecken	240
5.	Rechtfertigung durch Betriebsvereinbarung	241
6.	Fazit bzgl. der datenschutzrechtlichen Zulässigkeit der Compliance-Vorgänge innerhalb eines Konzerns	243
II.	Übermittlung pbD an Gerichte und Behörden	245
1.	Grundsatzproblem: Freiwillig versus Verpflichtung	246
2.	Mögliche Ermächtigungsgrundlagen für eine Übermittlung an staatliche Einrichtungen	246
a)	Einwilligung	246
b)	§ 32 I BDSG	247
c)	§ 28 I 1 Nr. 2 BDSG	248
d)	§ 28 II BDSG	249
aa)	§ 28 II Nr. 1 i.V.m. § 28 I 1 Nr. 2 BDSG	249
bb)	§ 28 II Nr. 2 BDSG	250
e)	Ergebnis bzgl. Übermittlung an öffentliche Stellen	254
III.	Datenweitergabe an Dritte	255
IV.	Änderungen aufgrund der DSGVO	257
1.	Einwilligung des Betroffenen	257
a)	Voraussetzungen im Einzelnen	258
aa)	Freiwilligkeit	258
bb)	Vorherige Information	260
cc)	Form	260
b)	Zwischenergebnis	261
2.	Gesetzliche Ermächtigungsgrundlagen	262
a)	Art. 6 I lit. b DSGVO	262
b)	Art. 6 I lit. c DSGVO	263
c)	Art. 6 I lit. d DSGVO	264
d)	Art. 6 I lit. e DSGVO	264
e)	Art. 6 I lit. fHs. 1 DSGVO	266
aa)	Anerkennung eines berechtigten Interesses gegenüber internen Ermittlungen?	267

bb) Konzernprivileg durch Erwägungsgründe?	268
f) Öffnungsklausel	271
g) Zweckänderung	275
aa) Vereinbarkeit der Zwecke	276
bb) Gesetzliche Rechtfertigung der Zweckänderung	277
cc) Zwischenergebnis	279
3. Änderung im Rahmen von Auftragsdatenverarbeitungen	280
4. Zwischenfazit	281
E. Besonderheiten betreffend Übermittlungen ins Ausland	282
I. Notwendigkeit einer »zwei-stufigen Prüfung« bei Auslandsberührung	282
II. Voraussetzungen der zweiten Prüfungsstufe	283
1. Auslandsübermittlung innerhalb des Konzernverbundes	283
a) Voraussetzungen für Übermittlungen in andere EU- oder EWR-Staaten	284
b) Voraussetzungen für Übermittlung in Drittländer	284
aa) Angemessenes Datenschutzniveau	285
bb) Vorliegen eines Ausnahmetatbestandes nach § 4c I 1 BDSG	295
cc) Genehmigung nach § 4c II 1 BDSG	301
c) Fazit zu den Erfordernissen der »zweiten Stufe« bei konzerninternen Datenübermittlungen	324
d) Sonderproblem: Transnationaler Transfer zwischen unselbständigen Unternehmensteilen	325
e) Sonderproblem: Datenimport	326
f) Sonderproblem: Rücktransport pbD in Drittstaat, wenn einziger Bezug zu Deutschland der Sitz des Datenbankbetreibers ist	327
2. Übermittlung an öffentliche Stellen im Ausland	330
a) Vorrang spezieller Gesetze und Vereinbarungen	330
b) Zulässigkeit der Übermittlung nach BDSG	331
aa) Übermittlungen innerhalb Europa bzw. innerhalb des EWR	332
bb) Übermittlung in Drittländer	334
c) Fazit und Handlungsempfehlung	336
3. Übermittlung an sonstige Dritte	337
III. Änderung der Zulässigkeit auf zweiter Stufe aufgrund der DSGVO	339
1. Allgemeines	339
2. Angemessenheitsentscheidung der EU-Kommission	339
3. Garantien nach der DSGVO	341
a) Individuelle Vertragsklauseln	341

b)	Standardvertragsklauseln	341
c)	Binding Corporate Rules	342
d)	Sonstige	343
4.	Ausnahmen	343
5.	Übermittlung an öffentliche Stellen	345
6.	Fazit zur Änderung der Anforderungen an den internationalen Datentransfer durch die DSGVO	346
F.	Nebenpflichten der Compliance	348
I.	Löschpflicht	348
1.	Nach § 35 BDSG	348
2.	Änderung aufgrund der DSGVO	351
II.	Benachrichtigungspflicht	353
1.	Zeitpunkt der Benachrichtigungspflicht	354
2.	Ausnahmen von der Benachrichtigungspflicht	354
3.	Änderung aufgrund der DSGVO	356
a)	Zeitpunkt der Benachrichtigung	356
b)	Ausnahmen von der Benachrichtigungspflicht	357
c)	Fazit	359
III.	Auskunftspflicht	359
1.	Inhalt der Pflicht nach § 34 BDSG	359
2.	Änderung aufgrund der DSGVO	360
IV.	Direkterhebungsgrundsatz	362
V.	Zusätzliche Voraussetzungen einer »konzerninternen Compliance-Datenbank«	363
1.	Anwendbarkeit der § 10 I bis IV BDSG bei »Verbundsdatenbanken«	364
2.	Notwendigkeit einer spezifischen Interessenabwägung	364
3.	Änderung aufgrund der DSGVO	366
VI.	Widerspruchsrecht nach Art. 21 I DSGVO	367
Sechstes Kapitel: Abschließende Zusammenfassung und Bewertung		368
A.	Bewertung der Voraussetzungen für eine Compliance-Abteilung	368
I.	Beantwortung der aufgestellten Thesen	368
1.	Das Datenschutzrecht schränkt die Arbeit einer Compliance-Abteilung in einem Konzern nicht ein.	368
a)	Die Compliance-Pflicht	368
b)	Anwendbarkeit des Datenschutzrechts	369
c)	Mögliche datenschutzrechtliche Ermächtigungsgrundlagen	371
aa)	Einwilligung	371
bb)	Gesetz	371

cc) Betriebsvereinbarung	372
2. Die Grenzen, die der Datenschutz einer Compliance-Abteilung aufgibt, sind in jedem Konzern identisch, unabhängig davon ob es sich um einen Konzern handelt, der nur deutschlandweit, EU-weit oder auch weltweit agiert.	373
3. Es können klare Vorgaben gegeben werden, wie die Compliance-Abteilung eines Konzerns zu agieren hat, um dem Datenschutz gerecht zu werden.	374
a) Interessenabwägung bzgl. Compliance-Maßnahmen	375
aa) Kategorisierung der untersuchten repressiven Maßnahmen	376
bb) Kategorisierung der untersuchten präventiven Maßnahmen	377
b) Interessenabwägung bzgl. eines konzerninternen Datentransfers zu Compliance-Zwecken	378
4. Ein Unternehmen bzw. ein Konzern hat im Falle eines Verstoßes gegen das Datenschutzrecht keine ernststen Folgen zu erwarten.	380
5. Aufgrund der DSGVO wird sich die Situation grundlegend ändern.	382
a) Erweiterter Geltungsbereich	382
b) Änderungen auf »erster Stufe«	383
c) Änderungen auf »zweiter Stufe«	384
d) Bußgeldrahmen	385
e) Fazit	386
II. Beeinflussung der Verhältnismäßigkeit über konzerninterne Vereinbarungen	386
III. Zusammenfassende Empfehlung für die Praxis	387
B. Bewertung der Gesetzesregelung aktuell und im Hinblick auf die DSGVO	389
I. Generalklausel als Ermächtigungsgrundlage	389
II. Konzernprivileg durch die Rechtsfolgen nach Art. 83 DSGVO	391
III. Zusammenfassendes Fazit zu den Datenschutzregelungen	394
 Literaturverzeichnis	 397