

# Compliance in Versicherungsunternehmen

Bürkle

4. Auflage 2026  
ISBN 978-3-406-82769-3  
C.H.BECK

schnell und portofrei erhältlich bei  
[beck-shop.de](https://beck-shop.de)

Die Online-Fachbuchhandlung [beck-shop.de](https://beck-shop.de) steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.

[beck-shop.de](https://beck-shop.de) hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird [beck-shop.de](https://beck-shop.de) für sein

umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Bürkle  
Compliance in Versicherungsunternehmen



**beck-shop.de**  
DIE FACHBUCHHANDLUNG



**beck-shop.de**  
DIE FACHBUCHHANDLUNG

# Rechtliche Anforderungen und praktische Umsetzung

Compliance in Versicherungsunternehmen

Herausgegeben von

**Dr. Jürgen Bürkle**

Bearbeitet von

Manuel Baroch Castellvi; Dr. Gunne W. Bähr, LL.M.; Dr. Jürgen Bürkle;  
Dr. Einiko Franz, LL. M. oec.; Martin Gehringer; Dr. Dr. Hermann Geiger, LL.M.;  
Dr. Helge Hartig; Dr. Axel Hausch; Benedikt Havers; Stefan Heinisch;  
Dr. Sebastian Heinrichs; Prof. Dr. Wessel Heukamp, LL.M.; Georg Kordges, LL.M.;  
Dr. Niclas Krohm; Dr. Carsten Kruchen, M.Jur.; Gunter Lescher; Dr. Björn Meuer;  
Sina Mundorf; Katharina Neumayer, LL.M.; Dr. Torsten Reich;  
Dr. Nina Schlierenkämper, LL.M.; Jochen Spengler; Prof. Dr. Fabian Stancke;  
Achim Stegmann; Dr. Martin Wolf, LL.M.

beck-shop.de  
DIE FACHBUCHHANDLUNG

  
C.H. BECK

Zitiervorschlag: Bürkle Compliance/Bearb. § ... Rn. ...

  
**beck-shop.de**  
DIE FACHBUCHHANDLUNG

**beck.de**

ISBN PRINT 978 3 406 82769 3

© 2026 Verlag C.H.Beck GmbH & Co. KG

Wilhelmstraße 9, 80801 München

info@beck.de

Satz, Druck und Bindung: Druckerei C.H.Beck Nördlingen

(Adresse wie Verlag)

Umschlag: Martina Busch, Grafikdesign, Homburg Saar

chbeck.de/nachhaltig

produktsicherheit.beck.de

Gedruckt auf säurefreiem, alterungsbeständigem Papier

(hergestellt aus chlorfrei gebleichtem Zellstoff)

Alle urheberrechtlichen Nutzungsrechte bleiben vorbehalten.

Der Verlag behält sich auch das Recht vor, Vervielfältigungen dieses Werkes  
zum Zwecke des Text and Data Mining vorzunehmen.

## Vorwort zur 4. Auflage

Seit der letzten Auflage dieses Handbuchs im Jahr 2020 hat sich die permanente Änderung des Rechtsumfelds für die Compliance in Versicherungsunternehmen in unveränderter Intensität, Geschwindigkeit und Tiefe fortgesetzt. Treiber dieser Entwicklung ist unverändert primär die europarechtliche Regulierung.

Diese Auflage unseres Handbuchs soll daher den Leserinnen und Lesern aktuelle Orientierung in dem immer komplexeren und dynamischeren europäischen und nationalen Rechtsumfeld bieten. Gleichzeitig wollen die Autorinnen und Autoren im Rahmen ihrer Anregungen zur Umsetzung in der Unternehmenspraxis vorhandene Spielräume aufzeigen und behördliche Äußerungen in den rechtlichen Kontext einordnen.

Diese Auflage aktualisiert den Inhalt der Voraufgabe und berücksichtigt dabei die einschlägige Gesetzgebung, Rechtsprechung und Literatur sowie die Verwaltungspraxis. Der Inhalt des Handbuchs wurde um drei praxisrelevante Themenfelder erweitert. Neu aufgenommen wurden die Bereiche Vergütung, Nachhaltigkeitsregulierung und IT-Regulierung.

Herausgeber, Autorinnen und Autoren danken Herrn Ulrich Pawlik vom Verlag C.H.Beck für die unverändert kompetente und engagierte Betreuung dieses Handbuchs.

*Stuttgart, im Februar 2026*

*Dr. Jürgen Bürkle*

  
**beck-shop.de**  
DIE FACHBUCHHANDLUNG



**beck-shop.de**  
DIE FACHBUCHHANDLUNG

## Bearbeitungsverzeichnis

<b>Manuel Baroch Castellvi</b> .....	Rechtsanwalt, DLA Piper UK LLP, Köln
<b>Dr. Gunne W. Bähr, LL.M.</b> .....	Rechtsanwalt, DLA Piper UK LLP, Köln
<b>Dr. Jürgen Bürkle</b> .....	Rechtsanwalt, BRP Renaud & Partner mbB, Stuttgart
<b>Dr. Einiko Franz, LL. M. oec.</b> .....	Partner, KPMG AG, Köln
<b>Martin Gehringer</b> .....	Wirtschaftsprüfer, EY GmbH & Co. KG, Eschborn
<b>Dr. Dr. Hermann Geiger, LL.M.</b> .....	Mitglied der Geschäftsleitung, Swiss Re, Zürich
<b>Dr. Helge Hartig</b> .....	Rechtsanwalt, ERGO Group AG, Düsseldorf
<b>Dr. Axel Hausch</b> .....	Rechtsanwalt, Stuttgart
<b>Benedikt Havers</b> .....	Hauptabteilungsleiter, SV Sparkassen Versicherung
<b>Stefan Heinisch</b> .....	Rechtsanwalt, Director, Hannover Rück SE
<b>Dr. Sebastian Heinrichs</b> .....	Rechtsanwalt, Hengeler Mueller, Frankfurt a. M.
<b>Prof. Dr. Wessel Heukamp, LL.M.</b> .....	Rechtsanwalt, Freshfields PartG mbB, München, Honorarprofessor, Ludwig-Maximilians-Universität München
<b>Georg Kordges, LL.M.</b> .....	Anwaltskanzlei Kordges, Essen
<b>Dr. Niclas Krohm</b> .....	Leitung Compliance, Datenschutz, Risikomanagement; Rechtsanwalt (Syndikusrechtsanwalt), Elisabeth Vinzenz Verband, Berlin
<b>Dr. Carsten Kruchen, M.Jur.</b> .....	Rechtsanwalt, Partner, Aderhold Rechtsanwaltsgesellschaft mbH, Düsseldorf
<b>Gunter Lescher</b> .....	Partner, Forensic Services, PricewaterhouseCoopers GmbH, Köln
<b>Dr. Björn Meuer</b> .....	Rechtsanwalt (Syndikusrechtsanwalt), stellvertretender Geldwäschebeauftragter, R+V Lebensversicherung AG, Wiesbaden
<b>Sina Mundorf</b> .....	Konzerndatenschutzbeauftragte und AI Compliance Officer, Rechtsanwältin (Syndikusrechtsanwältin), AXA Konzern AG, Köln
<b>Katharina Neumayer, LL.M.</b> .....	Rechtsanwältin, Group Legal & Compliance, Swiss Re, München
<b>Dr. Torsten Reich</b> .....	Chief Legal & Compliance Officer (CLO), Alteos GmbH, Berlin
<b>Dr. Nina Schlierenkämper, LL.M.</b> .....	Chief Compliance Officer, Zürich Beteiligungs-Aktiengesellschaft, Köln
<b>Jochen Spengler</b> .....	Wirtschaftsprüfer, EY GmbH & Co. KG, Eschborn

## Bearbeitungsverzeichnis

---

<b>Prof. Dr. Fabian Stancke</b> .....	Senior Advisor, Dentons Europe (Germany), Berlin, Professur für Wirtschaftsprivatrecht mit den Schwerpunkten Bank- und Versicherungsrecht, Fakultät Recht, Ostfalia Hochschule für angewandte Wissenschaften
<b>Achim Stegmann</b> .....	Leiter Ressort Recht, Geldwäschebeauftragter, R+V Lebensversicherung AG, Wiesbaden
<b>Dr. Martin Wolf, LL.M.</b> .....	Rechtsanwalt, Senior Expert Aufsichtsrecht, Generali Deutschland AG

  
**beck-shop.de**  
DIE FACHBUCHHANDLUNG

# Inhaltsverzeichnis

Vorwort zur 4. Auflage .....	V
Bearbeitungsverzeichnis .....	VII
Abkürzungsverzeichnis .....	XXXV
Verzeichnis der (abgekürzt) zitierten Literatur .....	LIX

## § 1. Besondere Bedeutung der Versicherungscompliance

A. Die besondere Bedeutung der Compliance in Versicherungsunternehmen ....	4
I. Rechtskonformität durch Corporate Compliance .....	4
II. Besonderheiten des Versicherungsprodukts .....	5
1. Rechtsprodukt .....	5
2. Vertrauensprodukt .....	6
B. Branchenspezifischer Rechtsrahmen .....	6
I. Vertragsrecht .....	8
1. Spezielles Vertragsrecht .....	8
2. Ausgelagertes Vertragsrecht .....	12
3. Internationales Vertragsrecht .....	16
II. Aufsichtsrecht .....	17
1. Zulassungs- und Tätigkeitsaufsicht .....	18
2. Aufsichtsrechtliche Vorgaben zur Unternehmensorganisation .....	19
3. Vorgaben für die Unternehmensorganisation .....	23
4. Behördliche Eingriffsmittel bei Rechtsverstößen .....	38
III. Modifizierte Vorgaben für Versicherungsunternehmen .....	40
IV. Selbstregulierung der Versicherungsunternehmen .....	43
C. Branchenspezifischer Nutzen der Compliance .....	44
I. Reputationsschutz .....	44
II. Werteorientierte Unternehmensführung .....	47
III. Vermeidung staatlicher Eingriffe .....	47
IV. Vermeidung staatlicher Regulierung .....	49
V. Schadens- und Haftungsprävention .....	49
VI. Aufsichtsrechtliche Kapitalanforderungen .....	51

## § 2. Branchenspezifische Rechtsgrundlagen und organisatorische Konsequenzen

A. Europäische Versicherungscompliance .....	57
I. Entwicklung der Versicherungscompliance .....	57
1. Regulierung .....	57
2. Aufsichtspraxis der BaFin .....	58
II. Regulierungsebenen .....	61
III. Rechtsquellen .....	62
1. Europäisches Recht .....	62
2. Nationales Recht .....	62
3. Rechtsprechung .....	63
4. Unternehmensinnenrecht .....	63

# Inhaltsverzeichnis

---

IV. Standards .....	64
1. Aufsichtsbehördliche Standards .....	64
2. Globale Standards .....	66
3. Branchenstandards .....	67
4. Betriebswirtschaftliche Standards .....	67
B. Compliance-Pflicht und Compliance-Verantwortung .....	68
I. Compliance-Pflicht der Versicherungsunternehmen .....	68
1. Unternehmensindividuelle Compliance .....	68
2. Konzern-Compliance .....	69
II. Compliance-Verantwortung des Vorstands .....	70
1. Gesellschaftsrechtliche Anforderungen .....	70
2. Aufsichtsrechtliche Anforderungen .....	73
III. Compliance-Verantwortung des Aufsichtsrats .....	79
1. Leitungsorgan und Schlüsselfunktionsinhaber .....	79
2. Geschäftsleiter-Compliance .....	80
3. Aufsichtsrats-Compliance .....	81
C. Aufsichtsrechtliche Regulierung der Compliance .....	83
I. Regulierungsziele des Aufsichtsrechts .....	83
II. Europarechtliche Vollharmonisierung .....	84
III. Europarechtliche Auslegung .....	85
IV. Prinzipienbasierte Regulierung .....	85
V. Verhältnismäßigkeit und Proportionalität .....	86
VI. Funktionsorientierte Regulierung .....	88
D. Aufsichtsrechtliche Regulierung der Compliance-Funktion .....	89
I. Relevante Regelungen .....	89
II. Die vier Teilfunktionen .....	91
III. Erweiterung der Teilfunktionen .....	92
IV. Stellenwert der Teilfunktionen .....	93
V. Tätigkeitsgebiet .....	94
VI. Operative Anforderungen .....	95
1. Überwachungsaufgabe .....	95
2. Beratungsaufgabe .....	103
3. Frühwarnaufgabe .....	105
4. Risikokontrollaufgabe .....	106
VII. Organisatorische Anforderungen .....	108
1. Wirksamkeit .....	108
2. Organisationsstruktur und Aufgabenwahrnehmung .....	109
3. Compliance-Berichte .....	114
4. Zusammenarbeit .....	117
5. Informationsversorgung .....	118
6. Compliance-Leitlinien .....	118
7. Compliance-Plan .....	119
8. Eignungsanforderungen .....	120
9. Outsourcing .....	126
10. Vergütung .....	126
VIII. Offenlegungs- und Anzeigepflichten .....	128
IX. Prüfung .....	129
1. Interne Prüfung .....	129
2. Externe Prüfung .....	130

**§ 3. Versicherungsgruppen/-konzerne**

A. Einführung .....	133
B. Konzern-Compliance als Ausfluss der aktienrechtlichen Konzernorganisationspflicht .....	137
C. Gruppen-Compliance als Ausfluss des Versicherungsaufsichtsrechts .....	144
I. Gruppen-Compliance und Tochter-GmbH .....	159
II. Gruppen-Compliance und Tochteraktiengesellschaften .....	159
D. Gruppen-Compliance im faktischen Konzern .....	161
I. Informationserteilung .....	161
II. Prüfungshandlungen durch die Gruppen-Compliance .....	165
III. Einheitliche Gruppen-Compliance-Standards/schriftliche Leitlinien ...	165
IV. Doppelmandate als Compliance-Instrument in der Gruppe? .....	169
1. Sicherung benötigter Informationen .....	169
2. Sanktionierung von Complianceverletzungen .....	174
V. Auswirkungen auf etwaige Minderheitsaktionäre .....	175
1. Auskunftsrechte .....	175
2. Keine Austritts- und Abfindungsrechte bei Funktionsausgliederungen	176
E. Compliance in der grenzüberschreitenden Versicherungsgruppe .....	176
F. Organhaftung .....	177

**§ 4. Rückversicherung**

A. Einleitung .....	182
I. Systematische Einordnung .....	182
II. Solvabilität II und Rückversicherung .....	185
III. Globale Entwicklungstendenzen .....	187
B. Regulatorische Compliance .....	190
I. Zulassungsaufsicht .....	191
1. Erlaubnispflicht für Inlandsunternehmen .....	191
2. EU-/EWR-ausländische Rückversicherungsunternehmen .....	194
3. Rückversicherungsunternehmen aus Drittstaaten .....	195
II. Laufende Aufsicht .....	198
1. Aufgaben und Ziel der Rückversicherungsaufsicht .....	198
2. Wesentliche Aspekte .....	199
III. Sanktionen .....	205
C. Transaktionsbezogene Compliance .....	206
I. Rückversicherungsverträge .....	206
1. Contract Certainty .....	206
2. Aufsichtliche Erwartungen an die Gestaltung und Governance von Rückversicherungsverträgen .....	207
3. Best Terms and Conditions Clauses .....	209
4. Datenschutz, IT-Governance und Vertraulichkeit .....	211
5. Außenwirtschaftsrecht .....	211
II. Finanzrückversicherung .....	212

# Inhaltsverzeichnis

---

III. Versicherungs-Zweckgesellschaften .....	215
IV. Bestandsübertragungen .....	217
V. Rückversicherungsvermittler .....	219
1. Insurance Distribution Directive .....	219
2. Contingent Commission Agreements .....	220
D. Ausblick .....	223

## § 5. Captives

A. Einleitung .....	227
B. Captive-Modelle .....	229
I. Erst- bzw. Rückversicherungs-Captives .....	229
II. Versicherbarkeit konzerneigener und -fremder Risiken .....	231
III. Weitere Lösungen für alternativen Risikotransfer .....	232
1. Rent a Captive .....	233
2. Protected Cell Company (PCC) .....	234
3. Incorporated Cell Company Carrying on Business of Insurance (ICC) .....	236
4. Virtuelle Captive (Virtual Captive) .....	236
C. Captive-Standorte .....	236
D. Aufbau einer Compliance-Struktur .....	237
I. Compliance-Management .....	237
II. Ausgestaltung der Compliance-Funktion .....	238
E. Aufsichtsrechtliche Compliance .....	239
I. Qualifikation der Captive als Versicherungsunternehmen .....	239
II. Captives unter Solvabilität II .....	240
1. Anwendbarkeit des Drei-Säulen-Konzepts von Solvabilität II .....	240
2. Besondere Regelungen für kleine Versicherungsunternehmen .....	241
3. Besondere Regelungen für firmeneigene (Rück-) Versicherungsunternehmen .....	242
4. Kritik an Überregulierung; Berücksichtigung des Proportionalitätsprinzips .....	243
5. Ausblick: Erleichterungen nach Solvabilität II-Review in Reichweite .....	246
III. Captives mit Sitz in Deutschland .....	249
1. Allgemeines .....	249
2. Aufsichtsrechtliche Vorgaben für Erstversicherungs-Captives .....	250
3. Aufsichtsrechtliche Vorgaben für Rückversicherungs-Captives .....	252
4. Outsourcing .....	253
IV. Captives mit Sitz innerhalb EU/EWR und Tätigkeit in Deutschland .....	255
1. Anforderungen des deutschen Aufsichtsrechts und anderer Tätigkeitsländer .....	255
2. Anforderungen des Aufsichtsrechts des Sitzstaates .....	256
V. Captives mit Sitz außerhalb EU/EWR und Tätigkeit in Deutschland .....	257
1. Anforderungen des deutschen Aufsichtsregimes .....	257
2. Aufsichtsrechtliche Vorgaben des Sitzstaates .....	258
F. Zivilrechtliche Compliance .....	261
I. Gesellschaftsrechtliche Compliance .....	261

II. Compliance der Versicherungsverhältnisse .....	261
1. Versicherungsvertragsrecht .....	261
2. Schiedsvereinbarungen .....	262
3. Beschränkungen der Versicherbarkeit und Pflichtversicherungen ...	263
G. Steuerrechtliche Compliance .....	266
I. Relevante Compliance-Ebenen und -Risiken .....	266
II. Überblick: Steuerrechtliche Compliance-Themen .....	267
III. Besteuerung der Captive .....	267
1. Domestic Captives .....	267
2. Offshore Captives .....	268
3. Compliance mit FATCA, CRS und anderen Steuertransparenzverpflichtungen .....	269
IV. Besteuerung der Captive-Anteilseigner .....	271
1. Domestic Captives .....	271
2. Offshore Captives .....	271
V. Besteuerung der versicherten Gesellschaften – Betriebsausgabenabzug ..	278
1. Unternehmen in Deutschland .....	278
2. Unternehmen im Ausland .....	280
VI. Versicherungsteuer-Compliance .....	281
VII. Umsatzsteuer-Compliance .....	284
VIII. Verdeckte Gewinnverlagerungen, Verrechnungspreise: Fremdvergleichskonforme Leistungen und Entgelte .....	285
IX. Compliance mit Mindestbesteuerungsvorschriften .....	287
H. Fronting .....	288
I. Funktion .....	288
II. Rechtliche Ausgestaltung .....	289
III. Sicherungsmöglichkeiten .....	289
I. Branchenspezifische Besonderheiten .....	291
<b>§ 6. Betriebliche Altersversorgung</b>	
A. Einleitung .....	294
B. EbAV-RL (RL (EU) 2016/2341) .....	295
I. Entstehungsgeschichte .....	295
1. Fortentwicklung der Pensionsfonds-RL (RL 2003/41/EG) .....	295
2. Diskussionen auf europäischer Ebene zur Holistic-Balance-Sheet und zum Common Framework .....	296
II. Zielsetzung und Struktur der EbAV-RL .....	297
1. Allgemeine Regelungen .....	297
2. Quantitative Regelungen .....	298
3. Qualitative Regelungen .....	298
4. Berichts- und Informationspflichten .....	299
C. Regulatorische Vorgaben für Einrichtungen der betrieblichen Altersversorgung	300
I. Umsetzung der EbAV-RL in das VAG .....	300
II. Neuregelung des VAG für EbAVs .....	300
1. Allgemeine Änderungen .....	300

2. Allgemeine Vorschriften zur Geschäftsorganisation und Proportionalitätsgrundsatz .....	301
3. Schlüsselfunktionen .....	301
4. Risikomanagement .....	301
5. Ausgliederung .....	302
III. MaGo für EbAV .....	302
1. Rundschreiben als bAV-spezifische Konkretisierung des Proportionalitätsprinzips .....	302
2. Verantwortung der Geschäftsleitung .....	303
3. Schlüsselfunktionen .....	303
4. Outsourcing und Ausgliederung von Schlüsselfunktionen .....	303
5. EbAV ohne eigene Mitarbeiter .....	303
6. Risikomanagement und eigene Risikobeurteilung .....	304
IV. DORA (Verordnung über die digitale operationale Resilienz im Finanzsektor) für EbAV .....	304
1. EbAVs als Finanzunternehmen iSv Art. 2 Abs. 1 DORA .....	304
2. Verhältnis zwischen DORA und §§ 232–240 VAG .....	305
3. Incident-Management .....	305
4. DORA und Auslagerungen .....	305
5. TLPT Penetrationstests .....	306
V. Neuregelung der Informationspflichten und VAG- Informationspflichtenverordnung (VAG-InfoV) .....	306
1. Allgemeine Anforderungen an die zu erteilenden Informationen .....	306
2. Bereitstellung der Information .....	306
3. Allgemeine Informationen zu einem Altersversorgungssystem .....	306
4. Informationspflichten vor dem Beitritt zu einem Altersversorgungssystem .....	307
5. Informationspflichten während der Anwartschaftsphase .....	307
6. Information der Versorgungsempfänger .....	308
7. Informationen auf Anfrage .....	308
D. Weitere compliancerelevante Besonderheiten der bAV .....	308
I. Versicherungsformen in der betrieblichen Altersversorgung .....	308
II. Berücksichtigung arbeits- und sozialversicherungsrechtlicher Vorgaben ..	309
III. Arbeitsrechtliche Vorgaben zur Leistungshöhe .....	310
IV. Informationspflichten des Versicherers gegenüber dem Arbeitgeber in der bAV .....	311
V. Versicherer als Informations-Erfüllungsgehilfe des Arbeitgebers .....	312
VI. Rechtsdienstleistungen und bAV-Beratung .....	312
1. Einleitung .....	312
2. Nebenleistung nach § 5 Abs. 1 RDG .....	313
3. Makler und Beratungsgesellschaften .....	313
4. Rechtsfolgen unzulässiger Rechtsberatung .....	313
VII. Versorgungsausgleich .....	314
VIII. Versicherer-Unterstützungskassen .....	314
IX. Rückdeckungsversicherungen .....	315

**§ 7. Internationale Versicherungsgeschäfte**

A. Einführung .....	318
B. Aufsichtsrechtliche Rahmenbedingungen .....	320
I. Die Regelungsbereiche der §§ 61 ff. VAG und §§ 67 ff. VAG .....	320
II. Unterscheidung zwischen Finanzaufsicht und „allgemeiner Rechtsaufsicht“ .....	320
III. Abgrenzungsfragen: Aufsichtsfreie Korrespondenzversicherung – Dienstleistungsverkehr – Niederlassungsgeschäft .....	322
1. Aufsichtsfreie Korrespondenzversicherung .....	322
2. Abgrenzung Dienstleistungsverkehr zur Niederlassung .....	324
C. Anwendbare Vorschriften des VAG und dort geregelte Handlungsbefugnisse der BaFin .....	326
I. Nach § 62 Abs. 1 S. 2 VAG entsprechend anzuwendende aufsichtsrechtliche Vorschriften .....	326
II. Handlungsbefugnisse der BaFin .....	327
D. Weitere anwendbare „Rechtsvorschriften des Allgemeininteresses“ .....	328
I. Der Begriff des „Allgemeininteresses“ .....	328
II. Schreiben der BaFin vom 16.3.2011 – Vorschriften des Allgemeininteresses in Deutschland .....	329
III. Das Urteil des Bundesverwaltungsgerichts vom 21.4.2021 .....	332
IV. Gesetze, die Rechtsvorschriften des Allgemeininteresses enthalten .....	332
1. Einführung .....	332
2. Versicherungsvertragsgesetz .....	333
3. Bürgerliches Gesetzbuch, insbes. die Vorschriften über die Allgemeinen Geschäftsbedingungen .....	334
4. Gesetz gegen den unlauteren Wettbewerb .....	334
5. Kartellrecht .....	335
6. Bundesdatenschutzgesetz .....	335
7. Digitale-Dienste-Gesetz .....	336
8. Geldwäschegesetz .....	336
9. Arbeitsrecht .....	336
10. Strafvorschriften .....	336
11. Gesellschaftsrechtliche Vorschriften .....	336
E. Aktuelle Entwicklungen im internationalen Versicherungsrecht .....	337
I. Folgen des Brexit .....	337
1. Konsequenzen für UK-Versicherungsunternehmen .....	338
2. Konsequenzen für EU/EWR-Versicherungsunternehmen .....	338
3. Bei Lloyd's vereinigte Einzelversicherer .....	338
II. Gruppenversicherungen im Lichte der TC Medical Air-Rechtsprechung .....	339
III. Neue Anforderungen im grenzüberschreitenden Versicherungsgeschäft .....	340
F. Ergebnisse und Folgerungen im Hinblick auf Corporate Compliance .....	341

**§ 8. Solvabilität, Kapitalanlage und Rechnungslegung**

A. Solvabilität .....	344
I. Grundgedanken und strukturelle Änderungen zur früheren Rechtslage .....	344

1. Grundstrukturen .....	344
2. Rechtsquellen und Verhältnisbestimmung .....	345
3. Solvency II-Review .....	346
II. Solvabilitätsübersicht .....	346
1. Grundlagen .....	346
2. Versicherungstechnische Rückstellungen .....	348
III. Bedeckung der Solvenzkapitalanforderungen durch Eigenmittel .....	350
1. Ermittlung der verfügbaren Eigenmittel .....	350
2. Qualitative Einordnung der Eigenmittel .....	351
3. Quantitative Vorgaben zur Eigenmittelbedeckung der Solvenzkapitalanforderungen .....	351
IV. Eingriffsbefugnisse der BaFin .....	353
V. Zusammenfassung .....	354
B. Kapitalanlage .....	354
I. Einführung und Kurzdarstellung der Rechtslage unter Solvency I .....	354
II. Systematik der Kapitalanlageregulierung unter Solvabilität II .....	355
1. Paradigmenwechsel hin zur Kapitalanlagefreiheit .....	355
2. Das Prudent Person Principle als leitender Anlagemaßstab .....	356
3. Eigenmittelunterlegung als Korrelat der Kapitalanlagefreiheit .....	360
III. Anforderungen an das Governance-System bezüglich Kapitalanlagen ...	361
1. Struktur der Geschäftsorganisationsgrundsätze im Solvabilität II- Regime .....	362
2. Im Besonderen: Risikomanagement im Bereich der Kapitalanlage ..	364
IV. Zusammenfassung .....	365
C. Rechnungslegung .....	366
I. Adressaten der Rechnungslegungsvorschriften .....	366
II. Systematik der Rechnungslegungsvorschriften .....	367
1. Einzelabschluss .....	367
2. Konzernabschluss .....	369
III. Internes Kontrollsystem für die Rechnungslegung .....	369
1. Einrichtungspflicht .....	370
2. Inhaltliche Ausformung des internen Kontrollsystems bzgl. Rechnungslegung .....	370

## § 9. Risikomanagementsystem und Internes Kontrollsystem

A. Rechtliche Rahmenbedingungen .....	372
I. EU-Rechtsrahmen .....	372
1. Solvabilität II-RL .....	372
2. Solva II-VO, EIOPA-Leitlinien und Erläuterungen .....	373
3. Weitere Regelungen .....	374
II. Nationale Regelungen .....	374
1. Versicherungsaufsichtsgesetz .....	374
2. Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen .....	375
3. Weitere Regelungen .....	375
B. Allgemeine Anforderungen an die Geschäftsorganisation .....	377
I. Überblick .....	377
II. Geschäftsleiterpflichten .....	377

III. Aufbau- und Ablauforganisation .....	378
1. Organisatorische Rahmenbedingungen .....	378
2. Aufbauorganisation .....	378
3. Ablauforganisation .....	380
4. Interne Leitlinien .....	381
5. Interne Überprüfung der Geschäftsorganisation .....	382
6. Schlüsselfunktionen .....	383
IV. Vergütung .....	385
V. Produktgovernance .....	386
VI. Proportionalitätsprinzip .....	387
C. Risikomanagementsystem .....	387
I. Grundlegende Anforderungen .....	387
1. Rechtliche Einordnung .....	387
2. Zuständigkeit .....	387
3. Aufgaben und Umfang .....	388
4. Risikokategorien .....	389
5. Proportionalität und Wesentlichkeit .....	390
6. Leitlinien zum Risikomanagement .....	391
II. Risikostrategie .....	391
III. Risikotragfähigkeit .....	392
1. Ermittlung der Risikotragfähigkeit .....	392
2. Risikodeckungspotenzial .....	393
3. Risikoprofil .....	393
4. Risikotragfähigkeitskonzept .....	394
5. Limitsystem .....	394
IV. Unabhängige Risikocontrollingfunktion .....	394
V. Risikokontrollprozess .....	395
1. Organisation .....	395
2. Risikoidentifikation .....	395
3. Risikoanalyse und -bewertung .....	396
4. Risikosteuerung .....	397
5. Risikoüberwachung .....	397
VI. ORSA .....	398
VII. Risikoberichterstattung .....	399
1. Interne Berichterstattung .....	399
2. Externe Berichterstattung .....	400
VIII. Weitere Elemente des Risikomanagementsystems .....	401
1. Liquiditätsplan .....	401
2. Kapitalanlagen .....	401
3. Vorgaben für das Aktiv-Passiv-Management .....	401
4. Externe Ratings .....	401
D. Internes Kontrollsystem .....	402
I. Überblick .....	402
II. Wirksamkeit des Internen Kontrollsystems .....	402
1. Kontrollen auf Prozessebene .....	403
2. Kontrollen auf Unternehmensebene .....	404
3. IT-Kontrollen .....	404
III. Berichterstattung .....	405
E. Compliance-Funktion .....	405

# Inhaltsverzeichnis

---

F. Interne Revision .....	406
I. Verpflichtung zur Einrichtung .....	406
II. Organisatorische Einbindung .....	406
III. Prüfung und Berichterstattung .....	407
IV. Prüfung des Risikomanagementsystems .....	408
G. Ausgliederung (Outsourcing) .....	409
H. Notfallmanagement .....	410
I. Dokumentationspflicht .....	413

## § 10. Nachhaltigkeit

A. Vorbemerkung .....	416
B. Die Entwicklung der „Nachhaltigkeit“ .....	417
I. Die „2030 Agenda for Sustainable Development“ und das Pariser Übereinkommen .....	417
II. EU-Aktionsplan für die Finanzierung nachhaltigen Wachstums .....	418
1. Anforderungen für nachhaltige kundenbezogene Geldanlagegeschäfte	420
2. Nachhaltigkeitsberichterstattung iRd jährlichen Geschäftsabschlusses	421
3. Sorgfaltspflichten in Lieferketten .....	423
III. Nationale Initiativen .....	428
IV. Bewertung der rechtlichen Maßnahmen und Ausblick .....	429
C. Der Begriff der „Nachhaltigkeit“ – „Nachhaltigkeitsregulatorik“, „Sustainable Finance“ und „Corporate Social Responsibility“ .....	430
I. Der Begriff der „Nachhaltigkeit“ .....	431
II. Nachhaltigkeit und „Sustainable Finance“ bzw. „Financial Sustainability“, „Green Finance“ .....	432
III. Nachhaltigkeit und Corporate Social Responsibility (CSR) .....	432
IV. „Nachhaltigkeitsregulatorik“ und „ESG-Compliance“ .....	433
1. „Nachhaltigkeitsregulatorik“ .....	433
2. „ESG-Compliance“ .....	434
D. Die besonderen Herausforderungen durch die Nachhaltigkeit .....	434
I. Die Komplexität der rechtlichen Vorgaben .....	435
1. Die drei Säulen der Nachhaltigkeit und mögliche Zielkonflikte .....	435
2. Komplexität der gesetzgeberischen Maßnahmen .....	435
3. Rechtsprechung .....	435
II. Aufsichtsrechtliche Anforderungen und Überwachung; Sanktionen .....	436
1. Delegierte Verordnungen der EU .....	436
2. Merkblatt der BaFin „zum Umgang mit Nachhaltigkeitsrisiken“ .....	437
III. Rechtsstreitigkeiten und Reputationsverlust als wirtschaftlicher Schaden	438
IV. Selbstverpflichtungen der Unternehmen .....	438
E. Auswirkungen der Nachhaltigkeit auf die Compliance-Funktion des Unternehmens .....	440
I. Die grundlegende Anforderung: Nachhaltigkeitskompetenz im Aufsichtsrat, in der Geschäftsleitung und bei den Überwachungsfunktionen .....	441

II. Grundsätzliche Überlegungen zur Organisation der Compliance-Funktion im Hinblick auf die Nachhaltigkeit .....	441
1. Die Aufgaben der Compliance-Funktion .....	441
2. Grundlegende Organisationsanforderungen und -prinzipien .....	442
III. Die Identifikation und Bewertung von (Rechts-)Risiken .....	443
IV. Die Rolle der Hauptversammlung .....	444
V. Die Rolle des Aufsichtsrats .....	445
1. Auswahl geeigneter Geschäftsleiter .....	445
2. Festlegung der Vergütung der Geschäftsleiter .....	445
3. Erweiterung der Überwachung der Geschäftsleitung im Hinblick auf nachhaltigkeitsbezogene Prozesse und Systeme, insbes. der Nachhaltigkeitsberichterstattung .....	446
4. Beratung des Vorstands und Forderung an die Vorstände, ökologische und soziale Ziele angemessen zu berücksichtigen; Erweiterung der Zustimmungsbefugnisse des Aufsichtsrats .....	447
VI. Die Rolle des Vorstands .....	448
1. Der Einfluss von Nachhaltigkeitsaspekten auf die Geschäftsorganisation und das Risikomanagement-System aus Sicht der Aufsichtsbehörden .....	448
2. Finanzielles Engagement des Unternehmens zur Förderung der Nachhaltigkeit .....	450
VII. Die Rollen des Inhabers der Compliance-Funktion und des Nachhaltigkeitsbeauftragten .....	451

**§ 11. Vorvertragliche Informationspflichten**

A. Historische Entwicklung der Informationspflichten .....	454
B. Allgemeiner gesetzlicher Rahmen für die Informationspflichten .....	456
C. Informationspflichten bei einzelnen Vertragstypen .....	459
I. Nichtlebensversicherung gem. Anhang I Solvabilität II-RL, außer substitutiver Krankenversicherung .....	459
1. Informationsblatt zu Versicherungsprodukten .....	459
2. Allgemeine Informationspflichten .....	460
3. Zeitpunkt der Informationserteilung .....	460
4. Spezifische Folgen bei Verstößen .....	461
II. Substitutive Krankenversicherung .....	461
III. Reine Risikolebensversicherungen einschließlich Berufsunfähigkeits-, Erwerbsunfähigkeits- und Arbeitsunfähigkeitsversicherung, wenn von einem Lebensversicherungsunternehmen angeboten .....	462
1. Informationsblatt zu Versicherungsprodukten .....	462
2. Allgemeine Informationen .....	463
3. Besondere Informationen .....	463
4. Zeitpunkt der Informationserteilung und spezifische Folgen bei Verstößen .....	464
IV. Altersvorsorge- und Basisrentenverträge .....	464
1. Allgemeines .....	464
2. Produktinformationsblatt .....	465
3. Allgemeine und besondere Informationen .....	466
4. Zeitpunkt der Informationserteilung .....	467
5. Spezifische Folgen bei Verstößen .....	467

V. Versicherungsanlageprodukte .....	468
1. Überblick .....	468
2. Basisinformationsblatt .....	469
3. Allgemeine Informationen .....	469
4. Besondere Informationen .....	469
5. Informationen über Vertrieb und Kosten .....	470
6. Zeitpunkt der Informationserteilung .....	471
7. Spezifische Folgen bei Verstößen .....	472
VI. Spezielle Informationspflichten bei Verbindung von Produkten .....	472
1. Allgemeines .....	472
2. Einzelne Informationspflichten .....	473
3. Spezifische Folgen bei Verstößen .....	474
VII. Informationspflichten bei PEPP .....	475

## § 12. Compliance im Versicherungsvertrieb

A. Einführung und Zielsetzung .....	478
B. Rechtliche Rahmenbedingungen Versicherungsvertrieb .....	479
I. Einführung: Versicherungsvermittler .....	479
II. Versicherungsvertreter .....	480
III. Versicherungsmakler .....	481
IV. Direktvertrieb .....	482
V. Angestellte Versicherungsvermittler .....	483
C. Verantwortlichkeit .....	484
I. Haftungs- und Reputationsrisiken .....	484
II. Compliance-Lösungen .....	485
1. Compliance-Klauseln .....	485
2. Richtlinien .....	487
D. Ausgestaltung eines Compliance-Programms .....	487
I. Bewertung des Compliance-Risikos .....	488
1. Vertriebswege .....	489
2. Produkte und Provisionen .....	490
3. Risikominimierende Maßnahmen .....	491
II. Compliance-Themen im Vertrieb .....	491
1. Datenschutz .....	491
2. Geldwäscheprävention .....	492
3. Korruptionsbekämpfung .....	493
4. Incentivierung .....	494
5. Strafrechtliches Handeln (Internal Fraud) .....	495
III. Sales Compliance .....	496
1. Beratung .....	497
2. Dokumentation .....	498
IV. Compliance-Plan .....	499
V. Schulungen und Förderung von Compliance-Verhalten .....	500
VI. Kommunikation/Tone from the Top .....	501
VII. Whistleblowing/Meldesysteme .....	502
VIII. Kontroll- und Überwachungsmöglichkeiten .....	503
1. Vermittlerauswahl .....	503
2. Geschäftsorganisation .....	507

3. AVAD .....	508
4. Beschwerden/IHK-Infopflicht (§ 51 VAG) .....	509
5. Meldung von Unregelmäßigkeiten an die Aufsichtsbehörde .....	509
IX. Sanktionen .....	511
E. Interner Verhaltenskodex/Code of Conduct .....	511
F. GDV-Verhaltensstandard für den Vertrieb .....	512
G. Ausblick .....	514
H. Schlussbetrachtung .....	515

**§ 13. Vergütungscompliance**

A. Einleitung .....	518
B. Rechtliche Vorgaben für die Gestaltung von Vergütungssystemen .....	519
I. Grundlagen .....	519
1. Vergütung als Regelungsgegenstand aufsichts- und aktienrechtlicher Normen .....	519
2. Die gesetzlichen Regelungen in der Übersicht .....	521
II. Vergütungsvorgaben für DVO-Unternehmen .....	525
1. Vorgaben für die Vergütung der Organe .....	525
2. Vergütungsvorgaben für Mitarbeiter .....	539
3. Vergütungsvorgaben für Beschäftigte von Dienstleistern .....	546
III. Vergütungsvorgaben für Nicht-DVO-Unternehmen .....	547
1. Arten von Nicht-DVO-Unternehmen .....	547
2. Vergütungsvorgaben für Organmitglieder .....	549
3. Vergütungsvorgaben für Mitarbeiter .....	552
4. Vergütungsvorgaben für Beschäftigte von Dienstleistern .....	554
5. Wertung .....	554
C. Vergütungscompliance .....	555
I. Vergütungspolitik .....	555
II. Compliance-Management-System Vergütung .....	556
1. Kultur .....	556
2. Ziele .....	556
3. Risiken .....	557
4. Programm .....	557
5. Organisation .....	559
6. Kommunikation .....	560
7. Überwachung und Verbesserung .....	562
8. Haftung und Eingriffsbefugnisse des Aufsichtsorgans .....	563
D. Vergütungscompliance in Versicherungsgruppen .....	563
I. Rechtliche Grundlagen .....	563
II. Gruppenspezifische Vergütungsvorgaben und ihre Umsetzung .....	564
1. Art und Inhalt der Vergütungsvorgaben in der Gruppe .....	564
2. Erstreckung auf weitere Gruppenunternehmen .....	565
3. Umsetzung des Vergütungssystems in der Gruppe .....	565

E. Eingriffsbefugnisse der Aufsicht .....	566
I. Voraussetzungen und Wirkungsweise .....	566
II. Beschränkung oder Streichung des Gesamtbetrags der variablen Vergütungen .....	567
III. Untersagung oder Beschränkung der Auszahlung variabler Vergütungsbestandteile .....	568
IV. Vertragliche Abbildung .....	569
V. Ausschluss für tarifvertragliche Leistungen .....	569

## § 14. Geldwäsche- und Terrorismusprävention

A. Einleitung .....	573
I. Wesentliche Rechtsgrundlagen .....	575
1. Strafrecht: Geldwäsche und Terrorismusfinanzierung .....	575
2. Geldwäschegesetz und Versicherungsaufsichtsgesetz .....	576
3. Auslegungs- und Anwendungshinweise (AuA) .....	577
4. EU-Geldwäsche-Verordnung (VO (EU) 2024/1624) .....	578
5. EBA-Leitlinien .....	578
II. Bewertung .....	579
B. Verpflichtete in der Versicherungswirtschaft .....	579
I. Versicherungsunternehmen .....	579
1. Lebensversicherer .....	579
2. Sachversicherer (Unfallversicherung mit Prämienrückgewähr) .....	580
3. Darlehensvergabe durch Versicherungsunternehmen .....	580
4. Pensionsfonds/Pensionskasse/Unterstützungskasse, Holdinggesellschaft .....	583
II. Versicherungsvermittler .....	583
III. Syndikusrechtsanwälte/Syndikussteuerberater .....	584
C. Risikomanagement/Organisationspflichten .....	585
I. Benanntes Mitglied der Unternehmensleitung .....	585
II. Geldwäschebeauftragter .....	587
1. Bestellung .....	587
2. Aufgaben .....	588
3. Ausstattung .....	589
4. Befugnisse .....	590
5. Der Geldwäschebeauftragte/Compliance Officer nach der VO (EU) 2024/1624 .....	590
III. Risikoanalyse (§ 5 GwG) .....	591
1. Aufbau .....	591
2. Risikoorientierte Sorgfaltspflichten .....	597
IV. Interne Sicherungsmaßnahmen .....	597
1. Interne Grundsätze, Verfahren und Kontrollen .....	598
2. Neue Produkte und Technologien .....	599
3. Gruppenweite Verfahren .....	599
4. Zuverlässigkeit und Unterrichtung der Beschäftigten .....	599
5. Überprüfung der Grundsätze und Verfahren .....	601
6. Hinweisgebersysteme .....	601
7. Sicherstellen der Auskunftsbereitschaft/Anfragen von Ermittlungsbehörden .....	602

D. Kundensorgfaltspflichten/Kundensorgfaltsmaßnahmen .....	602
I. Allgemeine Sorgfaltspflichten bei mittlerem Risiko .....	602
1. Umfang der allgemeinen Sorgfaltspflichten .....	602
2. Anlässe für die Erfüllung der allgemeinen Sorgfaltspflichten .....	618
3. Risikoadäquanz der Maßnahmen .....	620
4. Mitwirkungspflicht des Vertragspartners .....	620
5. Pflicht zur Nichtbegründung bzw. Beendigung der Geschäftsbeziehung/Nichtdurchführung der Transaktion .....	621
II. Vereinfachte Sorgfaltspflichten bei geringem Risiko .....	622
1. Risikofaktoren .....	622
2. Umfang der vereinfachten Sorgfaltspflichten .....	623
3. Insbes.: Zeitpunkt der Identifizierung .....	624
4. Auswirkungen der VO (EU) 2024/1624 .....	624
III. Verstärkte Sorgfaltspflichten bei erhöhtem Risiko .....	625
1. Risikofaktoren .....	625
2. Umfang verstärkter Sorgfaltspflichten .....	628
3. Zeitpunkt der Identifizierung .....	629
4. Auswirkungen der VO (EU) 2024/1624 .....	629
IV. Aufzeichnungs- und Aufbewahrungspflicht .....	631
V. Innenrevision und Wirtschaftsprüfer .....	632
E. Meldepflichten .....	632
I. Verdachtsmeldung (§ 43 GwG) .....	632
1. Verdachtsmeldepflicht .....	632
2. Erkennen von Verdachtsfällen .....	634
3. Form und Inhalt der Meldung/Meldeplattform goAML .....	639
4. Unverzüglichkeit der Verdachtsmeldung .....	639
5. FIU-Zentralstelle für Verdachtsmeldungen .....	641
6. Verbot der Informationsweitergabe .....	641
7. Stillhaltefrist .....	642
8. Auswirkungen der VO (EU) 2024/1624 .....	642
II. Meldepflicht an die Bundesbank .....	642
III. Unstimmigkeitsmeldung .....	642
F. Einschalten Dritter .....	643
I. Rückgriff auf Dritte .....	643
1. Rückgriff im Allgemeinen .....	643
2. Insbes.: Rückgriff auf existierende Identifizierungsdaten .....	644
II. Auslagerung von Kundensorgfaltspflichten .....	644
III. Auslagerung von internen Sicherungsmaßnahmen (Outsourcing) .....	645
IV. Partnerschaft für den Informationsaustausch .....	645
G. Gruppenweite Umsetzung .....	646
H. Aufsichtsbehörde und Bußgeldvorschriften .....	647
I. Aufsichtsbehörde .....	647
II. Bußgeldvorschriften .....	647
III. Bekanntmachungen von bestandskräftigen Maßnahmen und unanfechtbaren Bußgeldentscheidungen .....	648

## § 15. Kartellrecht

A. Die Bedeutung des Kartellrechts für die Versicherungswirtschaft .....	650
B. Die Bedeutung der Kartellrechts-Compliance in der Versicherungswirtschaft .	652
I. Legalitätsprinzip und Versicherungskartellrecht .....	652
II. Kartellrechtlicher Sanktionskanon und Compliance .....	653
C. Grundlagen des Kartellrechts .....	655
I. Überblick über das europäische und deutsche Kartellverbot .....	655
II. Die Freistellung vom Kartellverbot .....	656
III. Missbrauchsaufsicht .....	657
IV. Fusionskontrolle .....	658
D. Legal Management und Legal Judgement im Versicherungskartellrecht .....	659
I. Einführung eines Kartellrechts-Compliance-Programms .....	659
II. Maßnahmen .....	661
1. Absehen von Maßnahmen infolge einer rechtlichen Prüfung .....	661
2. Abhilfemaßnahmen .....	662
3. Klärung der Rechtslage mit Kartellbehörden .....	663
4. Kronzeugenantrag .....	663
E. Fallgruppen des Versicherungskartellrechts .....	664
I. Kartellrecht und Verbandsarbeit .....	664
II. Abstimmungen zu Prämien .....	665
III. Musterversicherungsbedingungen .....	666
IV. Mitversicherung .....	667
V. Marktinformationssysteme und Benchmarking .....	669
VI. Vorversichereranfrage .....	671
VII. Verzeichnisse über erhöhte Risiken .....	672
VIII. Schadenbedarfstatistiken, Sterbetafeln und Studien .....	673
IX. Sicherheitsvorkehrungen .....	676
X. Rahmenverträge mit Leistungserbringern .....	677
XI. Kooperationen im Vertrieb .....	679
1. Vertriebskooperationen .....	679
2. Provisionsabgabeverbot .....	680
3. Wettbewerbsrichtlinien .....	680
XII. Kartellrechtliche Herausforderungen in der Digital Economy .....	681

## § 16. Datenschutz

A. Einleitung .....	684
B. Stakeholder .....	685
I. Versicherungsunternehmen und ihre Verbände .....	685
II. Versicherungsnehmer und Dritte .....	686
III. Arbeitnehmer und Betriebsrat .....	686
IV. Datenschutzbehörden .....	686
V. Der Europäische Datenschutzausschuss .....	687
VI. Verbraucherschützer .....	688

C. Datenschutzrechtliche Grundlagen .....	688
I. Einleitung .....	688
II. Normen .....	689
1. Datenschutz-Grundverordnung .....	689
2. Bundesdatenschutzgesetz .....	690
3. Verhaltensregeln zum Datenschutz des GDV (Code of Conduct) ...	691
4. Versicherungsvertragsgesetz .....	692
5. ePrivacy .....	693
D. Datenschutz im Versicherungsunternehmen .....	693
I. Datenschutzmanagement und -organisation .....	693
1. Datenschutzmanagement .....	693
2. Datenschutzorganisation .....	696
II. Rechtsgrundlagen .....	698
1. Einleitung .....	698
2. Gesetzliche Erlaubnistatbestände .....	699
3. Einwilligung .....	703
III. Betroffenenrechte .....	704
1. Transparente Information, Kommunikation und Durchsetzungsmöglichkeiten .....	704
2. Recht auf Auskunft und Kopie der Daten .....	707
3. Recht auf Datenübertragbarkeit .....	707
4. Recht auf Berichtigung .....	708
5. Recht auf Löschung .....	708
6. Einschränkung der Verarbeitung .....	709
7. Mitteilungspflichten .....	709
8. Recht auf Widerspruch .....	709
9. Beschwerde .....	710
IV. Einschaltung von Dienstleistern und Outsourcing .....	710
1. Auftragsverarbeitung .....	711
2. Datenverarbeitung durch Dienstleister ohne Auftragsverarbeitung ...	711
3. Gemeinsam für die Verarbeitung Verantwortliche .....	712
4. Schutz von Privatgeheimnissen .....	713
V. Internationale Datentransfers .....	713
1. Angemessenheitsbeschluss .....	714
2. EU-Standardvertragsklauseln .....	714
3. Verbindliche interne Datenschutzvorschriften .....	714
4. Ausnahmen für bestimmte Fälle .....	714
VI. Automatisierte Einzelfallentscheidungen .....	715
1. Einfache personenbezogene Daten .....	715
2. Besondere Kategorien personenbezogener Daten .....	716
VII. Statistik .....	716

**§ 17. IT-Regulierung**

A. DORA .....	721
I. Schutzziele .....	721
II. Geltungsbereich und Ausnahmen .....	722
III. Regelungssystematik .....	723
IV. Delegierte Rechtsakte und Durchführungsrechtsakte .....	723
V. IKT-Governance .....	724
VI. Spezifische IKT-Risikofunktionen und Beauftragte .....	725

# Inhaltsverzeichnis

---

VII. Auslagerung von IKT-Kontrollfunktionen .....	726
VIII. IKT-Revision .....	726
IX. IKT-Risikomanagementrahmen .....	727
X. Strategie für die digitale operationale Resilienz (IKT-Risikostrategie) ...	727
XI. Dimensionen des IKT-Risikomanagementrahmens .....	728
XII. Interne Regelungen, insbes. Leitlinien, Strategien .....	729
1. Allgemeine Geschäftsfortführungsleitlinie .....	729
2. Informationssicherheitsleitlinie .....	730
3. IKT-Drittdienstleister-Leitlinie .....	731
4. Outsourcing-Leitlinie (Anpassung) .....	731
5. IKT-Kommunikationsstrategie .....	731
6. Regelmäßige Überprüfung und Aktualisierung .....	732
XIII. IKT-Richtlinien .....	732
1. Richtlinie für das Management von IKT-Assets .....	732
2. Richtlinien für das Management der Netzwerksicherheit .....	732
3. Richtlinien zur Zugangskontrolle .....	732
4. Richtlinien für die physische Sicherheit und die Sicherheit vor Umwelt Ereignissen .....	732
5. Richtlinie für Verschlüsselung und kryptografische Kontrollen .....	732
6. Richtlinien für das IKT-Änderungsmanagement .....	733
7. Richtlinien für Patches und Updates .....	733
8. Richtlinien für die Datensicherung .....	733
XIV. Dokumentationspflichten .....	733
XV. IKT-Dienstleistungen .....	733
1. Kritische/wichtige Funktionen .....	734
2. Meldepflichten bzgl. IKT-Dienstleistungen, die kritische/wichtige Funktionen unterstützen .....	734
XVI. IKT-Drittparteiensrisiko .....	735
1. IKT-Subdienstleister .....	735
2. IKT-Subdienstleisterkette .....	735
3. Kritische IKT-Drittdienstleister .....	736
4. Informationsregister .....	736
XVII. Mindestinhalte von Verträgen mit IKT-Drittdienstleistern .....	738
XVIII. Melde- und Berichtspflichten .....	739
1. Schwerwiegender IKT-bezogener Vorfall .....	739
2. Cyberbedrohung/Cyberangriff .....	739
3. Adressat, Inhalt und Form der Meldungen .....	740
XIX. Tests der digitalen operationalen Resilienz .....	741
XX. Pflichtschulungen, Schulungsprogramme .....	741
XXI. (Keine) Überwachungspflicht der DORA-Compliance von Versicherungsvermittlern .....	742
XXII. Sanktionen .....	742
1. Bußgelder .....	742
2. Kapitalaufschlag .....	743
3. Anprangerungspflicht .....	743
XXIII. Digitale Resilienz bei der Abwicklungsplanung (IRRD) .....	743
XXIV. DORA in der Abschlussprüfung .....	744
B. NIS-2-Richtlinie .....	744
I. BSIG .....	744
II. Konzerninterne IKT-Dienstleister .....	745

C. „KI“ in Versicherungsunternehmen .....	745
I. Definition von „KI“ .....	745
II. KI und Corporate Governance .....	745
III. Beschaffungsprozess von KI-Systemen .....	746
1. KI-System? .....	747
2. Risikoklassifizierung und Rollenverteilung .....	747
3. Folgeabschätzungen .....	747
4. IKT-Sicherheit und Resilienz .....	747
5. Arbeitsrecht .....	747
6. Vertragsgestaltung, Klauselbibliothek .....	748
IV. KI und Datenschutz .....	748
1. Privacy by Design, Trainingsdaten .....	748
2. Automatisierte Entscheidungen .....	748
3. Externe Dienstleister .....	749
V. KI-VO .....	749
1. KI-Risikoklassen .....	750
2. Schrittweises Inkrafttreten der KI-VO .....	750
3. Geltungsbereich/Adressaten .....	750
4. Verbotene Praktiken .....	751
5. Hochrisiko-KI-Systeme .....	754
6. KI-Systeme mit minimalem oder keinem Risiko .....	755
7. KI-Systeme mit allgemeinem Verwendungszweck .....	756
8. Betreiberpflichten .....	756
9. Einzelne Betreiberpflichten von Hochrisiko-KI-Systemen .....	757
10. Betreiber-Schwelle .....	760
11. Betreiber-Anbieter-Schwelle .....	761
12. Haftung .....	761
13. Haftung wegen Urheberrechtsverstößen .....	762
D. Europäische Daten- und Finanzstrategien .....	763
I. Verordnung über den freien Datenfluss .....	764
II. Digital Markets Act – DMA .....	764
III. Data Governance Act .....	765
IV. Data Act .....	765
1. Datennutzung .....	765
2. Portabilität und Interoperabilität .....	766
V. Digital Services Act .....	767
VI. Europäischer Gesundheitsdatenraum – EHDS .....	767
1. Gesundheitsdatennutzungsgesetz – GDNG .....	768
2. Bereitstellungspflicht zur Sekundärnutzung .....	768
VII. Financial Data Access – FiDA .....	769
1. Datenübermittlungspflicht .....	769
2. „Kundendaten“ .....	770

**§ 18. Fraud**

A. Einleitung .....	775
B. Begriffsbestimmung .....	775

# Inhaltsverzeichnis

---

C. Ursachen und Erscheinungsformen von Fraud .....	777
I. Ursachen .....	777
II. Erscheinungsformen .....	777
D. Relevanz des Themas für die Versicherungswirtschaft .....	778
I. Empirische Daten .....	779
II. Fraud-Risiken .....	781
III. Tätertypen .....	784
E. Rechtlicher Datenkranz .....	786
F. Anti-Fraud-Management als Bestandteil des unternehmensübergreifenden CMS .....	789
I. Elemente eines AFM gemäß IDW PS 980 nF (09.2022) .....	789
1. Kultur .....	789
2. Ziele .....	789
3. Organisation .....	790
4. Risiken .....	791
5. Programm .....	791
6. Kommunikation .....	792
7. Überwachung/Verbesserung .....	793
II. Aufdeckung von Fraud-Fällen .....	793
1. Hinweisgebersysteme .....	794
2. Forensische Datenanalysen .....	795
III. Aufklärung von Fraud-Fällen .....	795
1. Verdacht- und Fallmanagement .....	796
2. Rechtliche Besonderheiten .....	798
IV. Versicherungsschutz .....	799
1. D799 .....	799
2. Vertrauensschadenversicherung .....	799
3. Cyberversicherung .....	800
G. Ausblick .....	800

## § 19. Finanzsanktionen und Embargos

A. Allgemeiner Teil .....	806
I. Begriff der Sanktionen .....	806
II. Die Anwendbarkeit verschiedener Sanktionsregime .....	806
1. Die Anwendbarkeit von UN-Sanktionen .....	807
2. Die Anwendbarkeit von EU-Sanktionen .....	807
3. Die Anwendbarkeit britischer Sanktionen .....	814
4. Die Anwendbarkeit deutscher Sanktionen/Außenwirtschaftsrecht ...	814
5. Die Anwendbarkeit von US-Sanktionen .....	815
6. Die Anwendbarkeit der Sanktionsregeln weiterer Staaten .....	815
III. Auslegung einzelner Sanktionsnormen .....	816
IV. Blocking-Verordnungen/Statutes .....	816
V. Allgemeine Begriffe und Regeln/Definitionen .....	818
1. Das Einfrieren von Geldern .....	818
2. Wirtschaftliche Ressourcen .....	821
3. Ausnahmen vom Gebot, Gelder oder wirtschaftliche Ressourcen einzufrieren .....	822

4. Versicherung .....	822
5. Rückversicherung .....	822
6. Bereitstellung von Versicherung und Rückversicherung .....	822
7. Vermögenssperren/gelistete Personen .....	823
8. Investitionssperren .....	825
9. Embargos .....	825
10. Versicherungen und Rückversicherungen als „Finanzhilfen“ iSd EU-Sanktionsverordnungen .....	826
11. Erfüllungsverbote .....	826
12. (Rück-)Versicherung als strafbare Beihilfe .....	826
13. Die Ausbuchung von Forderungen .....	827
14. Die Verweigerung von Leistungen/guter Glaube .....	827
15. Meldepflichten .....	827
B. Besonderer Teil .....	827
I. Länderprogramme .....	828
1. Afghanistan .....	829
2. Belarus (Weißrussland) .....	829
3. Bosnien Herzegowina .....	830
4. Burundi .....	830
5. Guatemala .....	830
6. Guinea .....	831
7. Guinea-Bissau .....	831
8. Haiti .....	831
9. Irak .....	831
10. Iran .....	831
11. Jemen .....	834
12. Kongo (Demokratische Republik) .....	834
13. Krim .....	835
14. Kuba .....	835
15. Libanon .....	835
16. Libyen .....	835
17. Mali .....	836
18. Moldau .....	836
19. Myanmar (Birma) .....	836
20. Nicaragua .....	836
21. Niger .....	836
22. Nordkorea (Demokratische Volksrepublik Korea) .....	836
23. Russland .....	837
24. Simbabwe .....	844
25. Somalia .....	845
26. Sudan .....	845
27. Südsudan .....	845
28. Syrien .....	845
29. Tunesien .....	845
30. Türkei .....	846
31. Ukraine .....	846
32. Venezuela .....	846
33. Zentralafrikanische Republik .....	846
II. Personenprogramme/Terrorprogramm .....	847
1. Maßnahmen gegen das Al-Qaida-Netzwerk .....	847
2. Maßnahmen wegen der Ermordung Rafiq Hariris .....	847

# Inhaltsverzeichnis

---

3. Maßnahmen gegen bestimmte Personen angesichts der Lage in Afghanistan .....	847
4. Sonstige Terrorverdächtige .....	847
C. Vertragsgestaltung/Sanktionsklauseln .....	847
I. Klauseln unter ausdrücklicher Benennung bestimmter Sanktionsregime ..	848
II. Klauseln ohne ausdrückliche Benennung bestimmter Sanktionsregime ..	849
III. Mischformen .....	850
IV. Einzelfragen .....	850
1. Kündigungsfristen .....	850
2. Pro-rata-temporis-Zahlungen .....	850
3. Treuhandlösungen .....	851
4. Staatsangehörigkeit .....	851
5. Konzernklauseln .....	851
V. Spezielle Ausschlussklauseln .....	851
D. Praktische Umsetzung im Unternehmen .....	853
I. Einbindung verschiedener Einheiten des Unternehmens .....	854
II. Rechtsänderungen .....	854
III. Gliederung von Abteilungen/Einsatz von Mitarbeitern .....	855
IV. Prozesse .....	855
1. Erarbeitung eines Prüfmodells .....	855
2. Interne Richtlinien .....	857
3. Durchführung von Prüfungen durch Markt-/Schadenabteilungen ..	858
4. Die Identifizierung verbotener Güter und Dienstleistungen .....	859
5. Sperrmaßnahmen .....	860
6. Meldepflichten .....	861
V. Software-Screening-Lösungen .....	861
1. Auswahl .....	861
2. Einrichtung der Software .....	861
3. Unterhalt und Betrieb der Software .....	862
4. Fallbearbeitung .....	862
5. Informationsgewinnung .....	863
VI. Kommunikation .....	864
1. Schulungen .....	864
2. Intranet .....	864
3. Breaking News/Newsletter .....	864
VII. Dokumentation .....	865

## § 20. Steuern

A. Begrifflichkeiten und Rechtsgrundlagen .....	870
I. Pflicht zur Einrichtung und Unterhaltung eines effizienten Tax Compliance-Systems .....	870
II. Speziell steuerrechtliches Regelwerk .....	872
B. Ausgestaltung des Tax Compliance-Systems .....	873
I. Einbindung des Leiters der Steuerabteilung .....	873
II. Tax Compliance Management System gemäß IDW PS 980 nF (09.2022)	873
III. Module .....	875

C. Steuerrechtliche Risikofelder von Versicherungsunternehmen .....	876
I. Vollständigkeitsgebot, Wahrheitspflicht .....	876
1. Erklärungspflichten im Besteuerungsverfahren .....	877
2. Informationspflicht .....	877
3. Offenbarungspflicht .....	878
4. Einholung bzw. Nichteinholung von Rechtsrat .....	879
II. Berichtigung von Steuererklärungen (§ 153 AO) .....	882
1. Personen iSv §§ 34, 35 AO .....	882
2. Unrichtige und/oder unvollständige Erklärung .....	883
3. Nachträgliches Erkennen der Unrichtigkeit/Unvollständigkeit .....	883
4. Anzeige- und Berichtigungspflicht .....	884
III. Steuerstrafrecht, Verbandsgeldbuße .....	885
1. Steuerhinterziehung (§ 370 AO) .....	885
2. Leichtfertige Steuerverkürzung (§ 378 AO) .....	887
3. Selbstanzeige bei Versicherungsunternehmen .....	888
4. Verbandsgeldbuße und § 130 OWiG .....	892
5. Bestrebungen hin zum Unternehmensstrafrecht .....	894
IV. Haftung der Mitarbeiter .....	894
1. Haftung der Personen iSv §§ 34, 35 AO .....	894
2. Haftung der auf einer tieferen Hierarchieebene tätigen Mitarbeiter (§ 71 AO) .....	895
3. Haftung des Versicherungsunternehmens für Steuerschulden Dritter .....	896
V. Regelmäßige Prüfungen und deren Erleichterung bei Vorliegen eines wirksamen Tax Compliance-Systems .....	897
VI. Verbindliche Auskunft .....	897
VII. Ausgewählte Themen der Tax Compliance .....	899
1. (Geplante) Durchführung einer Compliance-Untersuchung .....	899
2. Delegation der Verantwortlichkeiten .....	900
D. Ausgewählte inhaltliche Schwerpunkte einer Tax Compliance .....	903
I. Ertragsteuerrechtliche Besonderheiten von Versicherungsunternehmen .....	903
1. Allgemeines zu § 21 KStG, § 8b Abs. 8, 9 KStG .....	903
2. Auswirkungen auf die Tax Compliance .....	905
II. Umsatzsteuerrechtliche Besonderheiten von Versicherungsunternehmen .....	906
III. Auswahl weiterer steuerrechtlich relevanter Bereiche .....	909
1. Versicherungsprodukte .....	909
2. Korruptionsdelikte .....	909
E. Internationale Entwicklungen .....	910
I. Entwicklungen auf OECD-Ebene .....	911
1. Leitsätze für multinationale Unternehmen .....	911
2. BEPS .....	911
II. Entwicklungen auf EU-Ebene .....	913
III. FATCA .....	914

## § 21. Outsourcing

A. Die aufsichtsrechtliche Bedeutung des Outsourcing .....	919
B. Rechtlicher Rahmen – Überblick .....	919

C. Allgemeine Anforderungen an Ausgliederungen gem. § 32 VAG, Art. 274	
Solvabilität II-VO .....	921
I. Anwendungsbereich .....	921
1. Adressatenkreis .....	921
2. Sachlicher Anwendungsbereich .....	922
II. Rechtsfolgen – Die allgemeinen Anforderungen des § 32 Abs. 2, 4 VAG und Art. 274 Abs. 1 Solvabilität II-VO .....	927
1. Proportionalitätsgrundsatz .....	928
2. Sicherstellung der ordnungsgemäßen Ausführung der ausgelagerten Tätigkeiten .....	928
3. Steuerungs- und Kontrollmöglichkeiten der Geschäftsleitung .....	941
4. Prüfungs- und Kontrollrechte der Aufsichtsbehörde .....	942
5. Ausgliederungsleitlinie – Outsourcing Policy .....	943
6. Subdelegation .....	945
D. Weitere Maßgaben für besondere Ausgliederungssachverhalte .....	946
I. Die Ausgliederung wichtiger Funktionen und Versicherungstätigkeiten ..	946
1. Abgrenzung der wichtigen Funktionen bzw. Versicherungstätigkeiten .....	946
2. Qualifizierte Anforderungen gem. § 32 Abs. 3 VAG, Art. 274 Abs. 2– 5 Solvabilität II-VO .....	948
II. Ausgliederungen von Schlüsselfunktionen .....	956
1. Ausgliederungsbeauftragter .....	957
2. Eignung der Mitarbeiter des Dienstleisters .....	959
3. Anzeige-/Berichtspflichten .....	959
III. Gruppeninterne Ausgliederungen .....	960
1. Risikoanalyse/-management .....	961
2. Due-Diligence, Qualifikationsanforderungen .....	961
3. Dienstleistungsvertrag .....	962
4. Steuerung und Kontrolle des Dienstleisters .....	962
IV. Outsourcing der internen Sicherungsmaßnahmen zur Geldwäsche- und Terrorismusprävention .....	963
V. Auslagerung der Steuerungs- und Kontrollpflichten des Versicherungsunternehmens .....	963
VI. Auslagerungen auf Mehrmandantendienstleister .....	964
VII. Ausgliederungen ins Ausland .....	965

## § 22. Aufsicht und Rechtsschutz

A. Überwachung durch BaFin und EIOPA .....	970
I. BaFin, EIOPA und das Europäische Aufsichtssystem .....	970
1. Entstehung und Regulierungsansatz .....	970
2. Hauptakteure und ihre Rollen bei Aufsicht und Regulierung .....	971
3. Zusammenarbeit von BaFin und EIOPA, Kooperation, Informationsaustausch .....	973
II. Aufsicht durch die BaFin .....	974
1. Aufsichtskonzept, Rechts- und Finanzaufsicht .....	974
2. Aufgaben .....	975
3. Befugnisse und Instrumente .....	977
4. (Weitere) Mittel der Aufsicht .....	982
5. Straf- und Bußgeldvorschriften .....	984
6. Bekanntmachungen .....	985