

Datenschutz in der Bankpraxis

von

Dr. Markus Deutsch, Dr. Andreas Fillmann, Paul Gürtler, Dr. Wulf Kamlah, Peter Suhren, Wolfgang Vahldiek, Dr. Thomas Winzer

1. Auflage

[Datenschutz in der Bankpraxis – Deutsch / Fillmann / Gürtler / et al.](#)

schnell und portofrei erhältlich bei [beck-shop.de](#) DIE FACHBUCHHANDLUNG

Thematische Gliederung:

[Datenschutz- und Melderecht](#)



Verlag C.H. Beck München 2012

Verlag C.H. Beck im Internet:

www.beck.de

ISBN 978 3 406 63924 1

Vahldiek (Hrsg.)
Datenschutz in der Bankpraxis

Datenschutz in der Bankpraxis

von
Wolfgang Vahldiek (Hrsg.)

mit Beiträgen von
Dr. Markus Deutsch
Dr. Andreas Fillmann
Paul Gürtler
Dr. Wulf Kamlah
Dr. Nadine Kramer
Peter Suhren
Dr. Thomas Winzer



Verlag C. H. Beck München 2012

www.beck.de

ISBN 978 3 406 63924 1

© 2012 Verlag C. H. Beck oHG
Wilhelmstraße 9, 80801 München
Druck und Bindung: Nomos Verlagsgesellschaft
In den Lissen 12, 76547 Sinzheim

Satz: ottomedien
Birkenweg 12, 64295 Darmstadt

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Vorwort

Der Geschäftsbetrieb von Banken ist im Hinblick auf den Datenschutz von besonderer Relevanz. Diese Erkenntnis ergibt sich schon allein aus der Tatsache, dass der Umgang mit personenbezogenen Daten gleichsam den Kern des bankgeschäftlichen Tätigwerdens darstellt. Jedes Konto, jede Kontogutschrift oder -belastung, jeder Zahlungsvorgang besteht im Verarbeiten und Verändern von digitalisierten Informationen, was mit Hilfe von Rechenzentren abgewickelt wird. Informationen über die Kunden sind Rohstoffe des Bankgewerbes.

Dies versteht auch die Politik sehr gut. Im Dienste der so empfundenen guten Sache – Steuergerechtigkeit, Kriminalitätsbekämpfung, etc. – wird auf die „Schätze“ auf den Servern der Banken nur allzu gern zugegriffen. Sei es, dass dieser Zugriff direkt erfolgt, wie zum Beispiel durch das Kontenabrufverfahren nach § 24c KWG, oder sei es, dass den Banken quasi-polizeiliche Hilfsfunktionen bei der Bekämpfung der Geldwäsche, der Terrorismusfinanzierung oder sonstiger Straftaten anvertraut – oder sollte man sagen: aufgebürdet? – werden. Direkte gesetzgeberische Aufforderungen, die Kundendaten für Zwecke zu nutzen oder nutzbar zu machen, die mit dem eigentlichen Bankvertragsverhältnis mit einem Kunden nichts zu tun haben, sind inzwischen häufig geworden.

Darüber hinausgehend ist die Geschäftstätigkeit der Banken in einem Höchstmaß aufsichtsrechtlich reguliert. Von Banken wird verlangt, dass sie ihre Datenbestände sorgfältig durchforsten und nutzen, und zwar im gesetzgeberisch verbindlich ausgestalteten eigenen Interesse, im Dienste ihres Risikomanagements. Der Begriff des Risikomanagements umfasst dabei nicht nur das Eingehen und Steuern von finanziellen Risiken im engeren Sinne, sondern ist sehr viel weitergehend. Im Grunde sind Banken heutzutage aufgefordert, vollständig und lückenlos sicher zu stellen, dass im Zusammenhang mit ihrer Geschäftstätigkeit keine Gesetzesverstöße stattfinden (Stichwort „Compliance“) und keine Umstände eintreten, die die öffentliche Meinung von einer Bank negativ beeinflussen könnten (Reputationsrisiko). Dieser Aufforderung seitens Gesetzgeber und Aufsichtsbehörden können Banken nur Folge leisten, wenn sie laufend ihren Datenbestand erweitern und effizient und automatisiert nach Auffälligkeiten suchen.

Vor diesem Hintergrund verwundert es wenig, dass mit der fortschreitenden Diskussion und Ausdifferenzierung des Datenschutzrechts in den vergangenen Jahren der diesbezügliche Wissens- und Beratungsbedarf gerade in Banken sehr stark angestiegen ist. Das vorliegende Werk soll einen Beitrag dazu leisten, den Praktikern gerade in diesem Bereich notwendige Hilfestellungen zu geben.

Die These, das BDSG sei ein schwer lesbares und schon gar nicht verständliches Gesetz, ist inzwischen Allgemeingut geworden. Dennoch sein hervorgehoben, dass in diesem Gesetz trotz aller Novellierungen bestimmte Grundgedanken gut erhalten geblieben sind, die es zu entdecken lohnt, da sie den Umgang mit dem Datenschutzrecht in der Praxis deutlich erleichtern.

Diese grundlegenden Ansätze des BDSG können zu einer Form von Strukturwissen zusammengefasst werden, das für die Beschäftigung mit datenschutzrechtlichen Fragen wie ein roter Faden Orientierung bieten kann und in vielen praktischen Fällen zu zutreffenden Lösungen hinleitet. Das vorliegende Werk soll einen Beitrag dazu leisten, diese Strukturen gerade mit Blick auf typische Fallgestaltungen im Bankbetrieb aufzuzeigen und handhabbar zu machen.

Idee und Konzept zu diesem Buch sind aus Anlass des Beginns einer Seminarreihe des Verbandes der Auslandsbanken entstanden. Mein besonderer Dank gilt den Autoren, die ihre langjährige Erfahrung in der Anwendung des BDSG in Beratung und Praxis speziell von Banken und Finanzdienstleistern in ihre Beiträge haben einfließen lassen. Ein weiterer besonderer Dank gebührt Christina Wolfer und Astrid Stanke vom Verlag C.H. Beck für die konstruktive und im besten Sinne routinierte Begleitung des Projekts.

Frankfurt, im Juni 2012

Wolfgang Vahldiek

Inhaltsübersicht

Vorwort	V
Inhaltsübersicht	VII
Inhaltsverzeichnis	XI
Literaturverzeichnis	XIX
Bearbeiterverzeichnis	XXV
§ 1. Der betriebliche Datenschutzbeauftragte – Aufgaben, Befugnisse, Organisation	1
I. Warum gibt es einen betrieblichen Datenschutzbeauftragten?	2
II. Pflicht zur Bestellung	3
III. Verpflichtete Stellen	4
IV. Zuständigkeitsbereich	6
V. Anforderungen an den betrieblichen Datenschutzbeauftragten	7
VI. Aufgaben des betrieblichen Datenschutzbeauftragten	9
VII. Befugnisse	13
VIII. Stellung im Unternehmen	13
IX. Auslagerung der Funktion des betrieblichen Datenschutzbeauftragten	15
X. Haftung	17
XI. Organisation von Datenschutzprozessen	18
§ 2. Datenerhebung, Datenverarbeitung und Datenübermittlung	21
I. Einfluss des Datenschutzes im Bankwesen	22
II. Grundlagen des Datenschutzrechts	23
III. Verbot mit Erlaubnisvorbehalt: Das „Ob“ der Datenverarbeitung	25
IV. Zweckbindungsgrundsatz	30
V. Direkterhebungsgrundsatz	32
VI. Datensparsamkeit und Datenvermeidung	32
VII. Verhältnismäßigkeitsgrundsatz	33
VIII. Praxisbeispiele aus dem Datenschutzrecht	34
IX. Das Bankgeheimnis	40
X. Vorschlag für ein datenschutzrechtliches Prüfungsschema im Bankwesen	42
§ 3. Der Schutz der Kundendaten	45
I. Einleitung	46
II. Problemfelder des Kundendatenschutzes	46
III. Auftragsdatenverarbeitung	61
IV. „Notification of breach“	67
V. Transparenz	70
VI. Bewertung und Ausblick	73

§ 4. Der Kreditentscheidungsprozess – Automatisierte Einzelentscheidung, Scoring und Auskunfteien	75
I. Einleitung	75
II. Automatisierte Einzelentscheidungen	75
III. Scoring	78
IV. Zusammenarbeit mit Auskunfteien	82
§ 5. Cloud Computing – Datenschutz in der Wolke	89
I. Was ist Cloud Computing?	89
II. Vertragsrechtliche Sicht	91
III. Welches Recht findet Anwendung?	91
IV. Datenschutzrechtliche Sicht	92
V. Aufsichtsrechtliche Sicht	96
VI. Zusammenfassung	97
§ 6. Schutz von Arbeitnehmerdaten in Banken	99
I. Rechtsgrundlagen des Arbeitnehmerdatenschutzes	100
II. Schutz der Beschäftigtendaten	103
III. Beteiligungsrechte des Betriebsrats	105
IV. Überwachung interner Verhaltensrichtlinien	112
V. Whistleblowing	114
VI. Aufdeckung von Straftaten	117
VII. Emailverkehr und sonstige Fernkommunikation	120
VIII. Offenlegung von Vergütungssystemen	126
IX. Die Auswirkungen der (geplanten) Datenschutznovelle	128
§ 7. Grenzüberschreitende Datenverarbeitung im Bankwesen	131
I. Einleitung	131
II. Wesentliche Regelungen und Definitionen (Rechtsvergleich)	133
III. Internationale Anwendbarkeit des BDSG	139
IV. Datenübermittlung im Konzern	141
§ 8. Datenübermittlung gemäß FATCA	159
I. Gegenstand der Regulierung	159
II. Wesentliche Definitionen	161
III. Grundsätzlicher Regelungsinhalt	163
IV. Würdigung gemäß nationaler Gesetze (BDSG)	164
§ 9. Datenschutz und Compliance	167
I. Grundlagen	168
II. Verhältnis des betrieblichen Datenschutzbeauftragten zum Geldwäsche- und Compliance-Beauftragten	176
III. Geldwäsche- und Terrorismusfinanzierungsbekämpfung	178
IV. Verhinderung strafbarer vermögensgefährdender Handlungen nach § 25c KWG	188

V. Staatliche Auskunftersuchen an ein Institut	193
VI. Datenschutz und Compliance in der Anlageberatung	199
VII. Grenzüberschreitender Datenverkehr	201
VIII. Verhältnis Aufsichtsrecht und Datenschutzrecht	204
IX. Zukünftige Entwicklungen	207
X. Zusammenfassung	209

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Inhaltsverzeichnis	XI
Literaturverzeichnis	XIX
Bearbeiterverzeichnis	XXV

§ 1. Der betriebliche Datenschutzbeauftragte – Aufgaben, Befugnisse, Organisation	1
I. Warum gibt es einen betrieblichen Datenschutzbeauftragten?	2
II. Pflicht zur Bestellung	3
1. Automatisierte und nicht automatisierte Datenverarbeitung	3
2. Berücksichtigung von Teilzeitbeschäftigten und Leiharbeitskräften	4
3. Ausnahmen	4
III. Verpflichtete Stellen	4
1. Internationale Anwendbarkeit des BDSG	4
2. Zweigstellen und Zweigniederlassungen ausländischer Institute	5
IV. Zuständigkeitsbereich	6
1. Verantwortliche Stelle	6
2. Verantwortliche Stelle im Konzern	6
3. Sachliche Zuständigkeit im Arbeitnehmerdatenschutz	6
V. Anforderungen an den betrieblichen Datenschutzbeauftragten	7
1. Zuverlässigkeit	7
a) Allgemeine Anforderungen	7
b) Interessenkonflikte	7
2. Fachkunde	8
VI. Aufgaben des betrieblichen Datenschutzbeauftragten	9
1. Zu beachtende Gesetze	9
2. Pflichtenumfang	9
a) Gesetzliche Pflichten des Datenschutzbeauftragten	10
b) Interne Beratung und Datenvermeidung	10
3. Verfahrensverzeichnis	10
4. Datengeheimnis	11
5. Vorabkontrolle	11
6. Repräsentative Funktionen/ Kontaktstelle	12
7. Krisenfälle	12
VII. Befugnisse	13
1. Einsichts- und Informationsrecht	13
2. Initiativ- und Einspruchsrecht	13
VIII. Stellung im Unternehmen	13
1. Unabhängigkeit	13
2. Weisungsfreiheit und Maßregelungsverbot	14

XI

3. Ausstattung mit personellen und sachlichen Ressourcen	14
4. Kündigungsschutz	14
5. Beendigung der Funktion des Datenschutzbeauftragten	15
IX. Auslagerung der Funktion des betrieblichen Datenschutzbeauftragten	15
1. Bestellung eines externen Datenschutzbeauftragten	15
2. Anforderungen an Auslagerungen nach § 25a Abs. 2 KWG	16
X. Haftung	17
1. Verantwortung im Außenverhältnis	17
2. Verantwortung im Innenverhältnis	17
3. Anspruchsgrundlagen	18
XI. Organisation von Datenschutzprozessen	18
1. Schwachstellenanalyse und Maßnahmenplan	18
2. Datenschutzkonzept	19
3. Datenschutzmanagementsystem	19
§ 2. Datenerhebung, Datenverarbeitung und Datenübermittlung	21
I. Einfluss des Datenschutzes im Bankwesen	22
1. Regelungssystematik (Überblick)	22
2. Beispiele	22
II. Grundlagen des Datenschutzrechts	23
1. Schutzzweck des Datenschutzrechts	23
2. Anwendungsbereich des Datenschutzrechts	24
3. Grundsätze des Datenschutzrechts	24
III. Verbot mit Erlaubnisvorbehalt: Das „Ob“ der Datenverarbeitung	25
1. Datenverarbeitung auf Grundlage einer Rechtsvorschrift	25
a) Rechtsgrundlagen ohne Interessenabwägung	25
b) Rechtsgrundlagen mit Interessenabwägung	27
2. Datenverarbeitung auf Grundlage einer Einwilligung	28
a) Freie Entscheidung des Betroffenen	28
b) Kenntnis der näheren Umstände	28
c) Form	29
3. Verhältnis Rechtsgrundlage und Einwilligung	29
IV. Zweckbindungsgrundsatz	30
1. Beispiele des Zweckbindungsgrundsatzes im Bankwesen	30
2. Unzulässigkeit der Vorratsdatenspeicherung	31
3. Zulässige Ausnahmen	31
V. Direkterhebungsgrundsatz	32
VI. Datensparsamkeit und Datenvermeidung	32
VII. Verhältnismäßigkeitsgrundsatz	33
VIII. Praxisbeispiele aus dem Datenschutzrecht	34
1. Fall: Videoüberwachung von Geschäftsräumen	34
2. Fall: Interne Ermittlungen: Der anonyme Schmähebrief	35
3. Fall: Aufzeichnung von Telefongesprächen	36
a) Rechtsgrundlage	36
b) Interessenabwägung (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG)	37
c) Einwilligung	39
IX. Das Bankgeheimnis	40

X.	Vorschlag für ein datenschutzrechtliches Prüfungsschema im Bankwesen	42
1.	Vorprüfung	42
2.	Prüfung des „Ob“ der Datenverarbeitung	42
a)	Rechtsgrundlage ohne Interessenabwägung	42
b)	Rechtsgrundlage mit Interessenabwägung	43
c)	Einwilligung	43
3.	Prüfung des „Wie“ der Datenverarbeitung – Datenschutzgrundsätze	43
§ 3.	Der Schutz der Kundendaten	45
I.	Einleitung	46
II.	Problemfelder des Kundendatenschutzes	46
1.	Der Vertragsschluss mit dem Kunden	46
a)	Daten für das Vertragsverhältnis	46
b)	Daten aus Anlass des Vertragsverhältnisses	48
2.	Daten bei der Durchführung des Vertrags	49
a)	Durchführung des Bankvertrags	49
b)	Nutzung der Daten für Zwecke des Kreditinstituts	50
3.	Werbung	50
a)	Bestandskunden	51
b)	Listendaten und Gruppenzugehörigkeit	51
c)	Hinzuspeicherung von Daten	52
d)	Abwägung der Interessen des Kreditinstituts und der Kundeninteressen	53
e)	Beispiel: Zahlungsstromanalyse	55
4.	Datenweitergabe im Konzern	59
5.	Werbung im Finanzdienstleistungskonzern	59
a)	Einwilligung	59
b)	Beipack- und Empfehlungswerbung	60
III.	Auftragsdatenverarbeitung	61
1.	Konzept der Auftragsdatenverarbeitung	62
2.	Auftragsdatenverarbeitung oder Funktionsübertragung?	62
3.	Die Anforderungen an die Auftragsdatenverarbeitung	63
a)	Auswahl des Auftragnehmers und Schriftform	64
b)	Der 10-Punkte-Katalog	65
4.	Weitere Regelungen	66
5.	Anpassungspflicht?	66
IV.	„Notification of breach“	67
1.	Die relevanten Daten	67
2.	Unbefugte Offenbarung	67
3.	Drohende schwerwiegende Beeinträchtigung	68
4.	Informationspflicht	68
5.	Umfang und Form der Information	69
6.	Verwendungsverbot	69
V.	Transparenz	70
1.	Unterrichtung bei Direkterhebung	70
2.	Hinweis auf Widerspruchsrecht bei Werbung	71
3.	Erhebung bei anderen als den Betroffenen	71

4. Negative automatisierte Einzelentscheidungen	71
5. Auskunftserteilung	72
a) Allgemeine Auskunft	72
b) Auskunftserteilung beim Scoring	72
VI. Bewertung und Ausblick	73
§ 4. Der Kreditentscheidungsprozess – Automatisierte Einzel- entscheidung, Scoring und Auskunfteien	75
I. Einleitung	75
II. Automatisierte Einzelentscheidungen	75
1. Ausschließlich automatisierte Verarbeitung	76
2. Erhebliche Beeinträchtigung	76
3. Automatisierte Einzelentscheidung	77
4. Zulässigkeit und Auskunftsanspruch	77
III. Scoring	78
1. Anwendungsbereich	79
2. Voraussetzungen	80
3. Transparenz (§ 34 Abs. 2 BDSG)	80
4. Transparenz bei Einschaltung Dritter	82
IV. Zusammenarbeit mit Auskunfteien	82
1. Anwendungsbereich des § 28a BDSG	83
2. Voraussetzungen (§ 28a Abs. 1 BDSG)	84
3. Voraussetzungen gemäß § 28a Abs. 2 BDSG („Positivdaten“)	85
4. Nachberichtspflichten (§ 28a Abs. 3 BDSG)	86
§ 5. Cloud Computing – Datenschutz in der Wolke	89
I. Was ist Cloud Computing?	89
1. Cloud Computing aus technischer Sicht	89
2. Cloud Computing aus unternehmerischer und wirtschaftlicher Sicht	90
II. Vertragsrechtliche Sicht	91
III. Welches Recht findet Anwendung?	91
IV. Datenschutzrechtliche Sicht	92
1. Relevanz für den Datenschutz	92
2. Anwendungsbereich des BDSG	92
3. Auftragsdatenverarbeitung oder Funktionsverlagerung	93
4. Cloud Computing mit Drittlandbezug	94
5. Organisation und Verfahren	95
V. Aufsichtsrechtliche Sicht	96
VI. Zusammenfassung	97
§ 6. Schutz von Arbeitnehmerdaten in Banken	99
I. Rechtsgrundlagen des Arbeitnehmerdatenschutzes	100
1. Europäische Ebene	100
a) Grundrechtscharta	100
b) Datenschutzrichtlinie 95/46/EG	100
c) Initiative für einheitliches europäisches Datenschutzrecht	101
2. Nationale Ebene	101

a) Verfassungsrecht	101
b) BDSG	101
c) Sonderregelung für Kreditinstitute	102
II. Schutz der Beschäftigtendaten	103
1. Betrieblicher Datenschutzbeauftragter	103
2. § 32 BDSG	103
3. Allgemeine Grundsätze	103
a) Kollidierende Interessen	103
b) Fragerecht des Arbeitgebers	104
c) Recht auf informationelle Selbstbestimmung	104
d) Einsichtsrecht in die Personalakte/Entfernungsanspruch	104
III. Beteiligungsrechte des Betriebsrats	105
1. Informationsrecht nach § 80 BetrVG	105
2. Weitere Beteiligungsrechte	106
a) Personalplanung	106
b) Personalfragebögen/Beurteilungsgrundsätze	106
3. Mitbestimmungsrechte	108
a) Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG	108
b) Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG	109
c) Erweiterung der datenschutzrechtlichen Eingriffsbefugnisse durch Betriebsvereinbarung	111
IV. Überwachung interner Verhaltensrichtlinien	112
1. Spezielle gesetzliche Regelungen	112
2. Maßstab des BDSG	112
a) Voraussetzungen	113
b) Beispiel: Kontenabgleich	113
V. Whistleblowing	114
1. Aktuelle Entscheidung des EGMR	114
2. Whistleblowingsysteme in Unternehmen	115
3. Sarbanes-Oxley-Act	115
4. Arbeitnehmerdatenschutz	116
VI. Aufdeckung von Straftaten	117
1. Einsatz einer Videokamera	117
a) Öffentlich zugängliche Räume	117
b) Nicht öffentlich zugängliche Räume	118
2. Detektiveinsatz	120
VII. Emailverkehr und sonstige Fernkommunikation	120
1. Dienstliche Nutzung	120
a) Voraussetzungen	120
b) Anwendbare Regelungen	121
2. Private Nutzung	123
a) Anwendbarkeit der Telekommunikationsgesetze	123
b) Fehlende Trennung der privaten und dienstlichen Nutzung	124
c) Pflichten nach dem TKG und TMG	124
VIII. Offenlegung von Vergütungssystemen	126
1. Gesetzliche Grundlage	126
2. Veröffentlichungspflichten nach der Instituts-Vergütungsverordnung	126
3. Vorrangigkeit des Datenschutzes	127

IX.	Die Auswirkungen der (geplanten) Datenschutznovelle	128
	1. Zulässige Fragen gegenüber dem Bewerber	128
	2. Aufdeckung von Straftaten	129
	3. Heimliche Überwachung	129
	4. Verdeckte Videoüberwachung	130
	5. Fernkommunikationsmittel	130
§ 7.	Grenzüberschreitende Datenverarbeitung im Bankwesen	131
	I. Einleitung	131
	II. Wesentliche Regelungen und Definitionen (Rechtsvergleich)	133
	1. Datenverarbeitung	133
	2. Verantwortliche Stelle	134
	3. Betroffener	135
	4. Personenbezogene Daten	135
	5. Rechtliche Zulässigkeit der Datenübermittlung	136
	a) Erste Prüfungsstufe: Einwilligung oder rechtliche Grundlage	136
	b) Zweite Prüfungsstufe: Angemessenes Datenschutzniveau	138
	6. Besondere Umstände der Datenübermittlung in einer Unternehmensgruppe	139
	III. Internationale Anwendbarkeit des BDSG	139
	IV. Datenübermittlung im Konzern	141
	1. Rechtliche Einordnung	141
	2. Analyse der Rolle der beteiligten Unternehmen	142
	3. Verantwortliche Stelle im Konzern	143
	a) Modalitäten der Datenübermittlung	144
	b) Abgrenzung der Funktionen	144
	4. Sicherstellung eines angemessenen Datenschutzniveaus	145
	a) EU-Standardvertragsklauseln	146
	b) Safe-Harbor-Abkommen	150
	c) Verbindliche Unternehmensregelungen im Konzern	153
	d) Individualvertrag	155
	e) Fazit und Ausblick	155
	5. § 4c BDSG – Ausnahmen vom Erfordernis eines angemessenen Datenschutzniveaus	157
	a) Einwilligung	157
	b) Erforderlichkeit zur Erfüllung einer Vertragsbeziehung	157
§ 8.	Datenübermittlung gemäß FATCA	159
	I. Gegenstand der Regulierung	159
	II. Wesentliche Definitionen	161
	III. Grundsätzlicher Regelungsinhalt	163
	IV. Würdigung gemäß nationaler Gesetze (BDSG)	164
§ 9.	Datenschutz und Compliance	167
	I. Grundlagen	168
	1. Allgemeine Anforderungen an Compliance	168

2. Spezielle Regelungen für die Organisation der Kreditinstitute	171
a) Kreditwesengesetz	171
b) Wertpapierhandelsgesetz	172
c) Geldwäschegesetz	173
3. Verhältnis der Compliance-Regelungen zum Datenschutz	173
4. Zusammenfassung	175
II. Verhältnis des betrieblichen Datenschutzbeauftragten zum Geldwäsche- und Compliance-Beauftragten	176
III. Geldwäsche- und Terrorismusfinanzierungsbekämpfung	178
1. Rechtsgrundlagen	178
2. Datenschutz und § 25c KWG	179
a) Angemessene Datenverarbeitungssysteme; § 25c Abs. 2 KWG	180
b) Institutsübergreifende Zusammenarbeit nach § 25c Abs. 3 S. 4 und 5 KWG	182
c) Institutsübergreifende Zusammenarbeit nach § 12 Abs. 1 Satz 2 GwG	183
d) Institutsübergreifende Zusammenarbeit nach § 12 Abs. 3 GwG	184
3. Sanktionslisten	185
4. Identifizierung und Kopien von Ausweispapieren	187
IV. Verhinderung strafbarer vermögensgefährdender Handlungen nach § 25c KWG	188
1. § 25c Abs. 2 Satz 2 KWG als Rechtsgrundlage für Betrugsbekämpfung	188
2. Warn- und Hinweissysteme	189
a) § 25c Abs. 3 Satz 4 und 5 KWG als Rechtsgrundlage für Warn- und Hinweisdateien der Kreditwirtschaft	189
b) Betrieb eines Warn- und Hinweissystems	191
c) Datenschutzerfordernissen an ein Warn- und Hinweissystem	191
V. Staatliche Auskunftersuchen an ein Institut	193
1. Ermittlungsbehörden	193
a) Staatsanwaltschaften	194
b) Polizei- und Ordnungsbehörden	194
c) Finanzbehörden	195
d) Datensicherheit	195
2. Checkliste Auskunftersuchen/Beschlagnahmen	197
a) Grundlagen	197
b) Formelle Legitimationsprüfung	197
c) Zulässigkeitsvoraussetzungen nach Fallgruppen im Strafverfahren	197
d) Beschlagnahme von Kontoguthaben	198
e) Einverständnis des Kunden	198
f) Dokumentation	199
g) Kostenerstattung	199
VI. Datenschutz und Compliance in der Anlageberatung	199
1. § 34d WpHG – Einsatz von Mitarbeitern in der Anlageberatung, als Vertriebsbeauftragte oder als Compliance-Beauftragte	199
2. WpHG-Mitarbeiteranzeigenverordnung (WpHGMaAnzV)	200
VII. Grenzüberschreitender Datenverkehr	201
1. Erste Stufe: Prüfung der Rechtsgrundlage	202
2. Zweite Stufe: Prüfung der Datenschutzadäquanz	203

VIII. Verhältnis Aufsichtsrecht und Datenschutzrecht	204
1. Datenschutzaufsicht	204
a) Befugnisse der Datenschutzaufsicht	204
b) Bußgeld- und Strafvorschriften im Datenschutz	205
2. Bankenaufsicht	206
3. Fazit	207
IX. Zukünftige Entwicklungen	207
X. Zusammenfassung	209