

Datenschutzsanktionenrecht

Klaas / Momsen / Wybitul

2023

ISBN 978-3-406-79459-9

C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung 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 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 für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Klaas/Momsen/Wybitul
Datenschutzsanktionenrecht

The logo for Beck's Shop features the text 'beck-shop.de' in a bold, lowercase, sans-serif font. Above the 'i' in 'shop' are three red circles of varying sizes, arranged in a slight arc. Below the main text, the phrase 'DIE FACHBUCHHANDLUNG' is written in a smaller, uppercase, sans-serif font.

beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG

Datenschutz- sanktionenrecht

Handbuch für die
Unternehmens- und Anwaltspraxis

Herausgegeben von

Dr. Arne Klaas

Rechtsanwalt in Berlin

Dr. Carsten Momsen

o. Professor an der Freien Universität Berlin

Tim Wybitul

Rechtsanwalt in Frankfurt

beck-shop.de

DIE FACHBUCHHANDLUNG

1. Auflage 2023



C.H. BECK

Zitiervorschlag:
Klaas/Momsen/Wybitul DatenschutzsanktionenR.-HdB/Bearbeiter § 1 Rn. 1


beck-shop.de
DIE FACHBUCHHANDLUNG

www.beck.de

ISBN 978 3 406 79459 9

© 2023 Verlag C.H.Beck oHG
Wilhelmstraße 9, 80801 München
Druck: Beltz Grafische Betriebe GmbH
Am Fliegerhorst 8, 99947 Bad Langensalza

Satz: 3w+p GmbH, Rimpar
Umschlaggestaltung: Druckerei C.H.Beck Nördlingen



chbeck.de/nachhaltig

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

Zum materiellen Datenschutzrecht wurde – und wird – viel geschrieben. Gerade seitdem die DS-GVO zum 25. Mai 2018 unmittelbar anwendbares Recht wurde, richtet sich sowohl das praktische als auch das wissenschaftliche „Spotlight“ auf dieses spannende Rechtsgebiet. Das Datenschutzrecht genießt diese Aufmerksamkeit zu Recht. Kein Wirtschaftszweig und kein Geschäftsfeld kann sich dem Anwendungsbereich der DSGVO und des BDSG entziehen. Die Frage nach den datenschutzrechtlichen Möglichkeiten und Grenzen ist daher von größter praktischer Bedeutung – und es ist nicht abzusehen, dass sich daran etwas in naher Zukunft ändern wird.

Das vorliegende Handbuch nimmt eine neue Perspektive ein. Die dem Datenschutzrecht zu teil werdende Aufmerksamkeit erklärt sich primär mit den Konsequenzen, die der unionsrechtliche Verwaltungs- und der nationale Gesetzgeber für den unrechtmäßigen Umgang mit personenbezogenen Daten vorgesehen haben. Denn nach einer kurzen „Eingewöhnungs- und Aufwärmphase“ haben die Datenschutzaufsichtsbehörden der Mitgliedsstaaten und eine Vielzahl von Ermittlungsverfahren eingeleitet und einige bereits mit dem Erlass von hohen Bußgeldbescheiden abgeschlossen. Die Bußgeldhöhe bewegt sich teils im Milliardenbereich. Die deutschen Datenschutzaufsichtsbehörden stehen ihren europäischen Kollegen nicht nach und sind selbst für einige der höheren Bußgelder verantwortlich.

Trotz seiner bereits erlangten praktischen Bedeutung ist das „Datenschutzsanktionenrecht“ kaum erforscht. Viele in der Praxis auftretende Rechtsfragen sind ungeklärt und teils noch nicht einmal identifiziert. Wesentlicher Grund: Das Datenschutzsanktionenrecht wird nur zum Teil durch das Unionsrecht geregelt. Einige Teilbereiche – wie zum Beispiel die Durchsetzung von Geldbußen oder das Schaffen von Straftatbeständen – musste dem Recht der nationalen Mitgliedsstaaten überlassen werden. Durch das Aufeinandertreffen von unionsrechtlichen Vorgaben und eigenständigen nationalrechtlichen Regelungen sind Auslegungsfragen und Kompetenzkonflikte vorprogrammiert.

Vor diesem Hintergrund haben die Herausgeber im Frühsommer 2021 das vorliegende Projekt ins Leben gerufen und ihren Fokus gezielt auf die Ahndung von Verstößen gegen das materielle Datenschutzrecht gerichtet. Herausgekommen ist eine umfassende Betrachtung aller praktischen Facetten des Geldbußenrechts aus Art. 83 DS-GVO, der Straftatbestände, die typischerweise bei unberechtigten Datenverarbeitungen verwirklicht werden sowie die damit im Zusammenhang stehenden prozessualen und taktischen Fragen. Ziel und Ansporn war es, dass dieser neue Blick auf das noch junge Datenschutzsanktionenrecht wissenschaftlich überzeugt und dem Rechtsanwender praktisch unmittelbar verwendbare Antworten an die Hand gibt. Hierzu wurde ein herausragendes Autorenteam gewonnen. Die Autoren sind ausgewiesene Experten auf dem Gebiet und haben bereits wichtige Vorarbeiten zu den sich stellenden Fragen geleistet. Um dem Leser eine ausgewogene Perspektive zu eröffnen, kommen im Handbuch alle Akteure der Sanktionspraxis zu Wort. Neben präventiv beratenden Anwälten, reaktiven Strafverteidigern und Wissenschaftlern kommt etwa mit Frau *Barbara Thiel* auch die Sicht der Landesbeauftragten für den Datenschutz Niedersachsen zur Sprache.

Die Herausgeber bedanken sich bei allen mitwirkenden Autoren für ihre wertvollen Einblicke in ihre Praxis. Ferner sind wir Frau *Susanne Loder* aufgrund ihrer hervorragenden organisatorischen Begleitung und ihrem aufmerksamen Lektorat zu besonderem Dank verpflichtet. Wir wünschen dem Handbuch eine gute Aufnahme. Für Anregungen und Kritik sind wir dankbar. Diese können Sie gerne an *Arne Klaas* klaas@kralaw.de richten.

Berlin und Frankfurt am Main im Juli 2023

Arne Klaas

Carsten Momsen

Tim Wybitul

beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	IX
Bearbeiterverzeichnis	XXV
Abkürzungsverzeichnis	XXVII
Verzeichnis der abgekürzt zitierten Literatur	XXXI

1. Teil Das Datenschutzsanktionenrecht

§ 1 Einleitung (<i>Klaas/Momsen/Wybitul</i>)	1
--	---

2. Teil Materielles Bußgeldrecht

§ 2 Grundlagen: Verhältnis von Unionsrecht und dem nationalen Bußgeldrecht (<i>Cornelius</i>)	7
§ 3 Materielles Bußgeldrecht (<i>Wybitul</i>)	51

3. Teil Die Verfolgung von bußgeldbewehrten Datenschutzverstößen

§ 4 Prozessuale Durchsetzung von Bußgeldern (<i>Thiel</i>)	67
§ 5 Anwaltliche Begleitung eines datenschutzrechtlichen Bußgeldverfahrens (<i>Basar</i>)	89
§ 6 Besondere Situationen: Umgang mit Data Breach/Cyber Security Incidents (<i>Brams</i>)	131

4. Teil Materielles Strafrecht

§ 7 Grundlagen: Verhältnis Europarecht und nationales Strafrecht (<i>Eisele</i>)	147
§ 8 Strafbare Datenschutzverstöße (§ 42 BDSG) (<i>Klaas</i>)	159
§ 9 Gefährdendes Verbreiten personenbezogener Daten (§ 201 StGB) (<i>Eisele</i>)	185
§ 10 Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) (<i>Lamsfuß</i>)	195
§ 11 Ausspähen von Daten (§ 202a StGB) (<i>Klaas</i>)	217
§ 12 Abfangen von Daten (§ 202b StGB) (<i>Klaas</i>)	239
§ 13 Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB) (<i>Klaas</i>)	251
§ 14 Datenhehlerei (§ 202d StGB) (<i>Hiéramente</i>)	265
§ 15 Verletzung von Privatgeheimnissen (§ 203 StGB) (<i>Cornelius/Spitz</i>)	289
§ 16 Verwertung fremder Geheimnisse (§ 204 StGB) (<i>Cornelius/Spitz</i>)	315
§ 17 Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB) (<i>Eisele/Bechtel</i>)	319
§ 18 Fälschung beweiserheblicher Daten (§ 269 StGB) (<i>Eisele/Bechtel</i>)	333
§ 19 Urkundenunterdrückung (§ 274 StGB) (<i>Eisele/Bechtel</i>)	347
§ 20 Datenveränderung (§ 303a StGB) (<i>Wengenroth</i>)	353
§ 21 Computersabotage (§ 303b StGB) (<i>Wengenroth</i>)	365
§ 22 Verletzung des Steuergeheimnisses (§ 355 StGB) (<i>Cornelius/Spitz</i>)	381
§ 23 Strafbare Verstöße gegen das TTDSG (§ 27 TTDSG) (<i>Cornelius/Spitz</i>)	385
§ 24 Verletzung von Geschäftsgeheimnissen (§ 23 GeschGehG) (<i>Cornelius/Spitz</i>)	397

5. Teil Die Verfolgung von Datenschutzstraftaten

§ 25 Anwendbarkeit deutschen Strafrechts – insbesondere bei grenzüberschreitenden, internetbasierten Datenschutzstraftaten (<i>Klaas</i>)	417
§ 26 Praktische Überlegungen und Hinweise zum Ablauf eines Strafverfahrens (<i>Hiéramente</i>)	439

6. Teil Gemeinsame Aspekte von Bußgeldern und Straftatbeständen

§ 27 Verhältnis von Bußgeldtatbeständen (Art. 83 DS-GVO) zu parallel verwirklichten Straftaten (<i>Klaas</i>)	449
§ 28 Auslegung (unwirksamer) datenschutzrechtlicher Einwilligungen in wirksame rechtfertigende Einwilligungen (<i>Klaas</i>)	457
§ 29 Einziehungsmaßnahmen infolge von Datenschutzverstößen (<i>Nadeborn/Lamsfuß</i>)	467
§ 30 Die Ermittlung von Datenschutzverstößen im digitalen Raum (<i>Brodowski</i>)	489
§ 31 Datenschutz-Compliance – Haftungsvermeidung in datenverarbeitenden Organisationen (<i>Jungkind/Petzinka</i>)	499
§ 32 Melde-, Mitwirkungs- und Rechenschaftspflichten im Spiegel von nemo tenetur (<i>Brodowski</i>)	519

7. Teil Datenschutzsanktionenrecht in den USA

§ 33 Überblick über das Datenschutzsanktionenrecht in den USA (<i>Klose/Momsen</i>)	527
--	-----

Sachverzeichnis	545
-----------------------	-----


beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Bearbeiterverzeichnis	XXV
Abkürzungsverzeichnis	XXVII
Verzeichnis der abgekürzt zitierten Literatur	XXXI

1. Teil Das Datenschutzsanktionenrecht

§ 1 Einleitung (<i>Klaas/Momsen/Wybitul</i>)	1
A. Entwicklung der Bußgeldpraxis in der Union und in Deutschland	2
B. Entwicklung der strafrechtlichen Verfolgung von Datenschutzverstößen in Deutschland	3
C. Datenschutzsanktionenrecht: Konflikt zwischen Unionsrecht und nationalem Recht	5
D. Wissenschaftliche Lösungen und praktisch verwendbare Antworten	5
E. Perspektivenwechsel: Behörden- und Verteidigungssicht im „Spiegel-Check“	6

2. Teil Materielles Bußgeldrecht

§ 2 Grundlagen: Verhältnis von Unionsrecht und dem nationalen Bußgeldrecht (<i>Cornelius</i>)	7
A. Überblick	10
B. Datenschutzrechtliche Bußgelder als Strafen im weiteren Sinne	10
C. Bestimmtheitsgrundsatz	12
D. Schuldprinzip	14
I. Ableitung aus der Unschuldsvermutung	14
II. Ableitung aus dem Gesetzlichkeitsprinzip, Art. 7 EMRK, Art. 49 Abs. 1 GRCh	16
III. Ableitung aus dem Verhältnismäßigkeitsgrundsatz, Art. 5 EUV, Art. 49 Abs. 3 GRCh	17
1. Gebot der persönlichen Verantwortlichkeit als Strafbarkeitsvoraussetzung	18
2. Verbot objektiver strafrechtlicher Verantwortlichkeit	20
IV. Ableitung aus der Menschenwürde, Art. 1 GRCh	21
V. Zusammenfassung	21
E. Materielle Ausgestaltung durch das Unionsrecht	22
I. Überblick	22
II. Anwendungsvorrang des Unionsrechts	23
III. Kartellrechtlicher Ausgangspunkt	24
1. Unionsrechtliche Praxis	25
2. Parallelen zur Respondeat Superior Doktrin	26
3. Parallelen zum deutschen Recht	26
4. Gleichlauf zwischen Normadressat und Ahndungssubjekt im Kartellordnungswidrigkeitenrecht	27
IV. Normadressat im Datenschutzrecht	28
1. Verantwortlicher für die Datenverarbeitung	28
2. Verhältnis zwischen „Verantwortlichem“ und „Unternehmen“	29
V. Inhaltsbestimmung eines unionsrechtlichen Schuldbegriffs	31
VI. Vorsatz und Fahrlässigkeit bei Sanktionen nach Art. 83 DS-GVO	33
1. Notwendigkeit eines zumindest fahrlässigen Verstoßes	33

2. Unionsrechtlicher Vorsatzbegriff	34
3. Unionsrechtlicher Fahrlässigkeitsbegriff	36
VII. Strafzumessungsschuld (bzw. Verhältnismäßigkeitsgrundsatz)	37
F. Verfahrensrechtliche Besonderheiten	37
I. Überblick	37
II. Rechenschaftspflicht und Unschuldsvermutung	38
III. Beweislast	39
IV. Beweismaß	40
1. Art. 6 Abs. 2 EMRK	41
2. Unionsrecht	41
V. Selbstbelastungsfreiheit	43
VI. Opportunitätsprinzip	43
VII. Beachtung des allgemeinen Verhältnismäßigkeitsgrundsatzes	44
G. Bedeutung von Rechtsunklarheiten	45
I. Generalklauselartige Formulierungen in der DS-GVO	46
II. Gebot der Normenklarheit	46
III. Schuldgrundsatz	46
IV. Verhältnis des Gebots der Normenklarheit zum Schuldprinzip	47
V. Schlussfolgerungen	48
§ 3 Materielles Bußgeldrecht (<i>Wybitul</i>)	51
A. Einleitung	52
B. Überblick über die Bußgeldtatbestände	52
C. Zurechnung bei Geldbußen nach Art. 83 DS-GVO	53
I. Einleitung	53
II. Das Zurechnungssystem des Art. 83 DS-GVO	53
1. Kein eigenes Zurechnungssystem	53
2. Kein Verweis auf ein vermeintliches Haftungssystem nach Art. 101, 102 AEUV	54
3. Kein Verweis auf ein Zurechnungssystem in ErwG 150 S. 3 DS-GVO	56
4. Verweis auf das Recht der Mitgliedstaaten	56
5. Nationale Regelungen in Deutschland	56
III. Zusammenfassung	58
D. Subjektive Vorwerfbarkeit	59
I. Einleitung	59
II. Subjektive Vorwerfbarkeit ist in der DS-GVO explizit angelegt	59
III. „Strict liability“ widerspricht der Systematik der DS-GVO	59
1. Unvereinbarkeit mit dem Verhältnismäßigkeitsprinzip	59
2. Unvereinbarkeit mit dem Schuldprinzip	60
3. Kein Erfordernis nach Effektivitätsgrundsatz	61
E. Besonderheiten bei Geldbußen wegen Verstößen gegen die Verarbeitungsgrundsätze	61
I. Bestimmtheitsgrundsatz	61
II. Konkurrenzverhältnis zwischen Bußgeldtatbeständen	62
F. Sanktionszumessung Bußgeldrahmen und Bußgeldberechnung	63
G. Ausblick	64
 3. Teil Die Verfolgung von bußgeldbewehrten Datenschutzverstößen	
§ 4 Prozessuale Durchsetzung von Bußgeldern (<i>Thiel</i>)	67
A. Anwendbarkeit deutschen OWiG-Rechts: Datenschutzspezifische Besonderheiten	67
I. Anwendbarkeit des allgemeinen Teils des OWiG	68
II. Anwendbarkeit der OWiG-Regelungen zum Bußgeldverfahren	69

B. Zuständigkeiten zur Verfolgung und Sanktionierung bußgeldrelevanter Verstöße	70
C. Ablauf eines bußgeldrechtlichen Verfahrens wegen Datenschutzverstößen ...	72
I. Einleitung durch die Behörde	72
II. Übergang ins gerichtliche Verfahren	74
D. Bußgeldberechnung und Sanktionszumessung	74
I. Darstellung des Sanktionsmodells des Europäischen Datenschutzausschusses	74
II. Kriterien der Zumessung und praktische Bedeutsamkeit	77
1. Kriterien zur Bestimmung des Ausgangsbetrages	77
2. Weitere Zumessungskriterien	78
3. Auffangkriterium: Andere erschwerende oder mildernde Umstände	79
E. Verwarnung kein Verfolgungshindernis für das Bußgeldverfahren	80
F. Besonderheiten bei der Bebußung von Unternehmen	81
G. Nebenfolgen	83
I. Einziehung von Gegenständen	83
II. Einziehung des Wertes von Taterträgen	83
H. Vermögensarrest zur Sicherung der Geldbuße	84
I. Verständigungen im Bußgeldverfahren	85
J. Vollstreckung von Bußgeldbescheiden	87
K. Verjährung von Datenschutzverstößen	87
§ 5 Anwaltliche Begleitung eines datenschutzrechtlichen Bußgeldverfahrens (Basar)	89
A. Einleitende Gedanken	90
B. Anzeichen für und Auslöser eines Bußgeldverfahrens	91
I. Öffentliche Berichte	91
II. Kontakt zur Datenschutzbehörde	92
III. Hinweise durch Betroffene	94
IV. Strafrechtliche Ermittlungsverfahren	94
V. Meldepflichten	95
C. Das (vorgelagerte) verwaltungsrechtliche Aufsichtsverfahren	96
I. Befugnisse der Datenschutzbehörden im Aufsichtsverfahren	96
II. Umgang mit Mitwirkungspflichten insbesondere im Auskunftsverfahren	97
1. Vorbereitung auf Maßnahmen der Datenschutzaufsicht	97
2. Rechte und Verhalten	98
III. Rechtsschutzmöglichkeiten über den Verwaltungsrechtsweg	103
1. Klagen gegen Anordnungen der Aufsicht	104
2. Vorbeugender Schutz gegen ein Bußgeld?	105
3. Taktische Erwägungen	107
D. Verteidigung im Bußgeldverfahren („Ermittlungsverfahren“)	108
I. Normenprogramm im Bußgeldverfahren	108
II. Rechte im Bußgeldverfahren	109
III. Rechtsschutz gegen die Einleitung des Bußgeldverfahrens	109
IV. Verteidigungsmöglichkeiten im Bußgeldverfahren vor der Behörde	110
V. Erlass des Bußgeldbescheids	114
1. Voraussetzungen für den Erlass	114
2. Bemessung des Bußgelds	116
E. Zwischenverfahren: Einspruch gegen den Bußgeldbescheid gem. § 67 Abs. 1 S. 1 OWiG	119
F. Verteidigung im Hauptverfahren	121
I. Prüfungsmaßstab	121

II. Möglichkeit der Einstellung	122
III. Ablauf der Hauptverhandlung	122
IV. Weitere Hinweise für die Praxis	124
G. Rechtsmittel: Beschwerde nach § 79 OWiG	125
H. Exkurs: Abwenden bzw. Einschränken öffentlichkeitwirksamer Pressemitteilungen durch Datenschutzbehörden	127
§ 6 Besondere Situationen: Umgang mit Data Breach/Cyber Security Incidents (Brams)	131
A. Einleitung	132
B. Überblick über Anforderungen nach der DS-GVO	132
I. Definition einer Datenschutzverletzung (Art. 4 Nr. 12 DS-GVO)	132
II. Vorgaben zum Umgang mit Datenschutzverletzungen nach der DS-GVO	133
1. Meldepflicht gegenüber Behörden (Art. 33 DS-GVO)	134
2. Informationspflicht gegenüber betroffenen Personen (Art. 34 DS-GVO)	134
3. Ausnahmen von Melde- und Informationspflichten	135
4. Dokumentationspflicht (Art. 33 Abs. 5 DS-GVO)	136
C. Überblick über mögliche Sanktionen bei Datenschutzverletzungen	137
I. Geldbußen (Art. 83 DS-GVO)	137
1. Überblick	137
2. Berechnung von Geldbußen bei Datenschutzverletzungen	137
II. Sonstige verwaltungsrechtliche Sanktionen (Art. 58 Abs. 2 DS-GVO)	138
III. Schadensersatz (Art. 82 DS-GVO)	138
IV. Mögliche Risiken für Unternehmen im Zusammenhang mit Massenverfahren	139
V. Weitere Risiken	139
D. Empfehlungen zum Umgang mit Datenschutzvorfällen	140
I. Vorbereitung auf mögliche Datenschutzvorfälle	140
1. Maßnahmen zur Datensicherheit	140
2. Kontrolle von Auftragsverarbeitern	141
3. Trainings und Awareness	142
4. Einführung von Reaktionsplänen	142
II. Reaktion auf mögliche Datenschutzvorfälle	142
1. Erste Maßnahmen	143
2. Erfüllung von möglichen Meldepflichten	143
3. Kooperation mit Aufsichtsbehörden?	143
4. Kommunikationsstrategie	143
5. Behebung möglicher Schwachstellen	144
6. Dokumentation	144
7. Vorbereitung auf die effektive Verteidigung gegen Schadensersatzforderungen und Geldbußen	144
8. Exkurs: Reaktion auf Ransomware-Attacken	144
E. Ausblick	145
4. Teil Materielles Strafrecht	
§ 7 Grundlagen: Verhältnis Europarecht und nationales Strafrecht (Eisele)	147
A. Europäisiertes Strafrecht	147
I. Begriffe aus dem Blickwinkel des Europäischen Rechts	147
II. Kernbereich der nationalen Souveränität	148
B. Das Prinzip der limitierten Einzelermächtigung und das Subsidiaritätsprinzip	148

C. Kompetenzgrundlagen im Bereich des Strafrechts	149
I. Kompetenzgrundlage des Art. 83 Abs. 1 AEUV	149
II. Kompetenzgrundlage des Art. 83 Abs. 2 AEUV	150
D. Inhaltliche Ausgestaltung von Richtlinien im strafrechtlichen Bereich	150
I. Regelungsmaterien	150
II. Inhaltliche Dichte der Regelungen	151
E. Bedeutung und Wirkung von Richtlinien im nationalen Recht	152
I. Richtlinienkonforme Auslegung	152
II. Wirkung von Richtlinien bei nicht rechtzeitiger und fehlerhafter Umsetzung	152
III. Speziell: Wirkung von EU-Recht auf nicht-harmonisiertes nationales Recht	153
F. DS-GVO und nationales Strafrecht	153
I. Systematik	153
II. Auslegung	154
III. Bestimmtheitsgrundsatz bei normativen Merkmalen und Blanketttatbeständen	155
1. Unionsrechtliche Regelungen	155
2. Nationales Datenschutzstrafrecht	156
IV. Anwendungsvorrang der DS-GVO	157
§ 8 Strafbare Datenschutzverstöße (§ 42 BDSG) (<i>Klaas</i>)	159
A. Vorbemerkung	160
B. Eingeschränkter Anwendungsbereich	161
I. Automatisierte Datenverarbeitung/Speichern in Dateisystemen	161
II. Haushaltsausnahme	161
C. Taugliche Täter	162
I. „Jedermanns-Delikt“: Argumente für die fehlende Einschränkung des Täterkreises	162
II. Sonderdelikt: Argumente für eine Beschränkung auf den datenschutzrechtlich Verantwortlichen	162
D. § 42 Abs. 1 StGB – Unberechtigte Weitergabe	164
I. Objektiver Tatbestand	164
1. Personenbezogene Daten	164
2. Große Zahl von Personen	164
3. Keine allgemeine Zugänglichkeit	165
4. Übermitteln (Nr. 1)	167
5. Auf andere Art und Weise zugänglich machen (Nr. 2)	167
6. „Dritter“	168
7. Fehlende Berechtigung	169
II. Subjektiver Tatbestand	171
1. Vorsatz	171
2. Gewerbsmäßigkeit	171
E. § 42 Abs. 2 BDSG – Unberechtigte Verarbeitung	172
I. Objektiver Tatbestand	172
1. Verarbeitung (Nr. 1)	172
2. Erschleichen durch unrichtige Angaben (Nr. 2)	173
3. Handeln gegen Entgelt	175
II. Subjektiver Tatbestand	176
1. Eventualvorsatz ausreichend	176
2. (Dritt-)Bereicherungsabsicht	176
3. Schädigungsabsicht	178
F. Rechtfertigung	179
G. Behandlung von Irrtümern	179

H. Absolutes Antragsdelikt	180
I. Versuch	181
J. Verjährung	181
K. Konkurrenzen	181
I. Mögliche Tateinheit mit § 42 Abs. 1, 2 BDSG	181
II. Abschließende Spezialregelungen und deren Grenzen	182
III. Verhältnis der Varianten zueinander	182
L. Strafzumessung	182
M. Prozessuales	183
§ 9 Gefährdendes Verbreiten personenbezogener Daten (§ 201 StGB) (<i>Eisele</i>)	185
A. Rechtspolitische Begründung	185
B. Geschütztes Rechtsgut	186
C. Strafanwendungsrecht	187
D. Objektiver Tatbestand	187
I. Personenbezogene Daten	187
II. Tathandlung des Verbreitens	188
1. Öffentliches Verbreiten	188
2. Verbreiten eines Inhalts	188
III. Art und Weise des Verbreitens	190
1. Eignung	190
2. Bestimmung	191
3. Bedeutung der Zustimmung	191
IV. In Bezug genommene Straftaten	191
E. Subjektiver Tatbestand	192
F. Tatbestandsausschluss	192
G. Rechtfertigung	193
H. Qualifikation	193
I. Konkurrenzen	193
§ 10 Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) (<i>Lamsfuß</i>)	195
A. Allgemeines	196
B. Objektiver Tatbestand	197
I. Tatobjekt: Das nichtöffentlich gesprochenes Wort	197
1. Gesprochenes Wort	197
2. Nichtöffentlich	198
II. Tathandlungen	202
1. Aufnehmen des nichtöffentlich gesprochenen Wortes (Abs. 1 Nr. 1)	202
2. Gebrauchen oder Zugänglichmachen einer Aufnahme (Abs. 1 Nr. 2)	203
3. Abhören des nichtöffentlichen Wortes mit einem Abhörgerät (Abs. 2 S. 1 Nr. 1)	205
4. Öffentliches Mitteilen (Abs. 2 S. 1 Nr. 2)	206
III. „Unbefugt“	207
1. Einwilligung	208
2. Gesetzliche Befugnisse	209
3. Allgemeine Rechtfertigungsgründe	209
C. Subjektiver Tatbestand	212
D. Rechtswidrigkeit	212
E. Qualifikation: Amtsträger (Abs. 3)	212
F. Versuch (Abs. 4)	213
G. Einziehung (Abs. 5)	213
H. Prozessuales	213
I. Strafantrag	213

II. Konkurrenzen	213
III. Verwertungsverbote	214
IV. Anspruch auf Vernichtung einer Aufnahme	216
§ 11 Ausspähen von Daten (§ 202a StGB) (Klaas)	217
A. Vorbemerkung	218
B. Rechtsgut und Beispiele für Rechtsguträger	218
C. Daten	220
D. Nicht für den Täter bestimmt	221
E. Gegen unberechtigten Zugang besonders gesichert	223
F. Verschaffen des Zugangs	225
G. Sich oder einem anderen	227
H. Überwindung der Zugangssicherung	227
I. Unbefugt	228
J. Subjektiver Tatbestand und Irrtum	231
K. Rechtswidrigkeit	231
I. Notstandslage	231
II. Notstandshandlung	232
1. Geeignetheit	232
2. Relativ mildestes Mittel	233
3. Abwägung der widerstreitenden Interessen	234
III. Subjektives Rechtfertigungselement	237
L. Relatives Antragsdelikt	237
M. Versuch	237
N. Verjährung	237
O. Konkurrenzen	238
§ 12 Abfangen von Daten (§ 202b StGB) (Klaas)	239
A. Vorbemerkung	239
B. Rechtsgut	240
C. Nicht für ihn bestimmte Daten	240
D. Zeitliche Einschränkung des Tatobjekts: Während des Übertragungsvorgangs	241
I. Aus einer nichtöffentlichen Datenübermittlung	241
II. Aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage	243
III. Einbezug von durch den Täter initiierte Datenübermittlungen/-abstrahlungen?	244
E. Verschaffen unter Anwendung von technischen Mitteln	245
F. Sich oder einem anderen	246
G. Unbefugt	246
H. Subjektiver Tatbestand und Irrtum	249
I. Rechtswidrigkeit	249
J. Konkurrenzen und Subsidiaritätsklausel	249
I. Allgemeine Konkurrenzen	249
II. Formelle Subsidiarität	249
K. Absolutes Antragsdelikt	249
L. Versuch	250
M. Verjährung	250
§ 13 Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB) (Klaas) ...	251
A. Vorbemerkung	251
B. Rechtsgut	252

C. Tatobjekt	252
I. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen	252
II. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist	253
D. Tathandlung	255
I. Herstellen	255
II. Sich oder einem anderen Verschaffen	255
III. Verkaufen	255
IV. Einem anderen Überlassen	257
V. Verbreiten	257
VI. Sonst zugänglich machen	257
VII. Intendierte Straflosigkeit des reinen „Besitzes“	257
E. Subjektiver Tatbestand	258
F. Rechtswidrigkeit	259
G. Tätige Reue	260
I. Entsprechende Anwendung von § 149 Abs. 2 StGB	260
II. Entsprechende Anwendung von § 149 Abs. 3 StGB	262
H. Officialdelikt	262
I. Versuch	263
J. Verjährung	263
K. Konkurrenzen	263
§ 14 Datenhehlerei (§ 202d StGB) (<i>Hiéramente</i>)	265
A. Vorbemerkung	265
B. Rechtsgut	267
C. Tatbestand	269
I. Objektiver Tatbestand	269
1. Tatobjekt	269
2. Tathandlung	276
II. Subjektiver Tatbestand	279
1. Vorsatz	279
2. Bereicherungs- oder Schädigungsabsicht	280
D. Absatz 3	281
I. Rechtsnatur der Regelung des Absatz 3	281
II. Sonderregelungen für Amtsträger und Beauftragte (Nr. 1)	282
III. Sonderregelungen bei journalistischer Tätigkeit (Nr. 2)	283
IV. Weitere Berufsgruppen	284
E. Rechtswidrigkeit und Schuld	287
F. Sonstiges	287
§ 15 Verletzung von Privatgeheimnissen (§ 203 StGB) (<i>Cornelius/Spitz</i>)	289
A. Überblick	290
I. Entstehungsgeschichte	290
II. Rechtsgut	291
B. Objektiver Tatbestand	292
I. Tatobjekt	292
1. Fremdes Geheimnis	292
2. Einzelangaben nach Abs. 2 S. 2	294
3. Anvertraut oder sonst bekanntgeworden	294
II. Täterkreis	295
1. Personengruppen des Abs. 1	295
2. Personengruppen des Abs. 2	296
3. Personengruppen des Abs. 4	297

III. Tathandlung	297
1. Kenntnissnahme oder Kenntnissnahmemöglichkeit	298
2. Offenbaren anonymisierter und pseudonymisierter Daten; Vergleich zur datenschutzrechtlichen Diskussion	299
IV. Tatbestandsausschluss nach Abs. 3	303
V. Tod des Geheimnisgeschützten nach Abs. 5	304
C. Subjektiver Tatbestand und Irrtum	305
D. Rechtswidrigkeit	305
I. Unbefugt	305
1. Das Merkmal „unbefugt“ in der strafrechtlichen Systematik	306
2. Das Merkmal „unbefugt“ und das Verhältnis zum Datenschutzrecht	306
3. Datenschutzrechtliche Spezialbereiche im Verhältnis zu § 203 StGB	308
II. Einwilligung	310
III. Mutmaßliche Einwilligung	312
IV. Sonstige gesetzliche Offenbarungspflichten und -befugnisse	312
E. Täterschaft und Teilnahme	312
F. Versuch und Vollendung	313
G. Qualifikation des Abs. 6	313
H. Rechtsfolgen, Verjährung, Strafantrag	314
§ 16 Verwertung fremder Geheimnisse (§ 204 StGB) (<i>Cornelius/Spitz</i>)	315
A. Überblick	315
B. Täterkreis	316
C. Tatbestand des Abs. 1	316
D. Verweisung auf § 203 Abs. 5 StGB in Abs. 2	317
E. Vollendung	317
F. Täterschaft und Teilnahme	317
G. Rechtsfolgen und Strafantrag	317
§ 17 Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB) (<i>Eisele/Bechtel</i>)	319
A. Allgemeines	320
B. Tatbestand	321
I. Objektiver Tatbestand	321
1. Täterkreis von Abs. 1 und Abs. 2	321
2. Mitteilung von dem Post- oder Fernmeldegeheimnis unterliegenden Tatsachen (Abs. 1)	324
3. Öffnen einer anvertrauten und verschlossenen Sendung bzw. Kenntnisverschaffung von deren Inhalt (Abs. 2 Nr. 1)	326
4. Unterdrücken anvertrauter Sendungen (Abs. 2 Nr. 2)	326
5. Erweiterung des Täterkreises (Abs. 3)	329
6. Amtsträger (Abs. 4)	329
II. Subjektiver Tatbestand	330
C. Rechtswidrigkeit	330
I. Rechtfertigung nach §§ 32, 34 StGB	330
II. (Mutmaßliche) Einwilligung	331
III. Gesetzliche Offenbarungsbefugnisse bzw. -pflichten	331
D. Konkurrenzen	331
§ 18 Fälschung beweisheblicher Daten (§ 269 StGB) (<i>Eisele/Bechtel</i>)	333
A. Allgemeines	333

B. Tatbestand	335
I. Objektiver Tatbestand	335
1. Der Datenbegriff des § 269 StGB	335
2. Tathandlungen	336
II. Subjektiver Tatbestand	344
C. Rechtswidrigkeit und Schuld	345
D. Strafschärfungen	345
E. Konkurrenzen	345
F. Prozessuales	346
§ 19 Urkundenunterdrückung (§ 274 StGB) (<i>Eisele/Bechtel</i>)	347
A. Allgemeines	347
B. Tatbestand	348
I. Objektiver Tatbestand	348
1. Daten	348
2. Tathandlungen	349
II. Subjektiver Tatbestand	351
C. Rechtswidrigkeit	352
§ 20 Datenveränderung (§ 303a StGB) (<i>Wengenroth</i>)	353
A. Allgemeines und Rechtsgut	353
B. Tatobjekt – Daten (§ 202a Abs. 2 StGB)	355
I. Daten	355
II. „Fremde“ Daten	355
III. Einschränkung im Bagatellbereich	356
C. Tathandlung – Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von Daten	357
I. Löschen	357
II. Unterdrücken	357
III. Unbrauchbarmachen	358
IV. Verändern	359
V. Unterlassen	359
D. Rechtswidrig	359
I. Bestimmung der Datenverfügungsbefugnis	360
II. Einschränkung bei digitalen Protestaktionen	362
III. Prozessuale Implikationen der Verfügungsbefugnis	362
E. Subjektiver Tatbestand	362
F. Rechtswidrigkeit – allgemeine Rechtfertigungsgründe	363
G. Versuch und Vollendung	363
H. Vorbereitung – § 303a Abs. 3 StGB	363
I. Konkurrenzen	364
J. Relatives Antragsdelikt	364
K. Verjährung	364
§ 21 Computersabotage (§ 303b StGB) (<i>Wengenroth</i>)	365
A. Allgemeines und Rechtsgut	366
B. Tatobjekt – Datenverarbeitung von wesentlicher Bedeutung	367
I. Datenverarbeitung	367
II. Wesentliche Bedeutung	368
III. Für „einen anderen“	369
C. Tathandlung	370
I. Tat nach § 303a StGB	370
II. Eingeben oder Übermitteln von Daten	370
1. Angriffsmittel – Daten	370
2. Eingeben	370

3. Übermitteln	371
4. Nachteilszufügungsabsicht	371
III. Einwirkungen auf Datenhardware	372
IV. Unterlassen	373
D. Taterfolg	373
I. Störung	373
II. Erheblichkeit	373
III. Kausalität	374
E. Qualifikation und Regelbeispiele (Abs. 2, Abs. 4)	374
I. Qualifikation (Abs. 2)	374
1. Adressaten	374
2. Fremd	375
3. Wesentliche Bedeutung	375
4. Störung der Datenverarbeitung	376
II. Regelbeispiele der Qualifikation (Abs. 4)	376
1. Herbeiführen eines Vermögensverlustes großen Ausmaßes	376
2. Gewerbsmäßiges Handeln oder als Mitglied einer Bande zur fortgesetzten Begehung von Computersabotage	376
3. Beeinträchtigung der Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder der Sicherheit der Bundesrepublik Deutschland	377
F. Subjektiver Tatbestand	377
G. Rechtswidrigkeit	377
H. Versuch und Vollendung	378
I. Vorbereitung (Abs. 5)	378
J. Konkurrenzen	378
K. Relatives Antragsdelikt	379
L. Verjährung	379
§ 22 Verletzung des Steuergeheimnisses (§ 355 StGB) (Cornelius/Spitz)	381
A. Überblick	381
B. Objektiver Tatbestand	382
I. Täterkreis	382
II. Tatobjekte	382
III. Tathandlung	383
C. Subjektiver Tatbestand und Irrtum	383
D. Rechtswidrigkeit	383
E. Rechtsfolgen, Strafantrag, Konkurrenzen	384
§ 23 Strafbare Verstöße gegen das TTDSG (§ 27 TTDSG) (Cornelius/Spitz)	385
A. Überblick	385
B. Blanketttatbestand	387
I. Vorliegen eines Blanketttatbestands	387
II. Gesetzlichkeitsprinzip und Bestimmtheitsgrundsatz	387
III. Dynamische Verweisung	388
IV. Irrtumsregelung	389
C. Objektiver Tatbestand	389
I. Abhören einer Nachricht (Abs. 1 Nr. 1)	389
1. Nachricht	389
2. Abhören	390
3. Nicht für den Empfänger bestimmt	391
4. Kenntnisnahme in vergleichbarer Weise	391
5. Funkanlage	391
II. Mitteilungsverbot (§ 27 Abs. 1 Nr. 2 TTDSG)	392
III. Herstellungs- und Bereitstellungsverbot (§ 27 Abs. 1 Nr. 3 TTDSG)	393

D. Subjektiver Tatbestand	394
E. Rechtswidrigkeit	394
F. Rechtsfolgen, Versuch und Verjährung	395
§ 24 Verletzung von Geschäftsgeheimnissen (§ 23 GeschGehG) (Cornelius/Spitz)	397
A. Entstehungsgeschichte und Normzweck	398
B. § 23 Abs. 1 GeschGehG: Strafbare Erlangung, Nutzung oder Offenlegung fremder Geschäftsgeheimnisse	400
I. Definition Geschäftsgeheimnis	400
1. Allgemeines	400
2. Geheim	401
3. Wirtschaftlicher Wert	402
4. Angemessene Geheimhaltungsmaßnahmen	402
5. Berechtigtes Interesse	402
II. Besondere subjektive Voraussetzungen	403
1. Förderung des eigenen oder fremden Wettbewerbs	403
2. Eigennutz	403
3. Zugunsten eines Dritten	404
4. Schädigungsabsicht	404
III. § 23 Abs. 1 Nr. 1 GeschGehG: Betriebsespionage	404
1. Objektiver Tatbestand	404
2. Subjektiver Tatbestand	405
IV. § 23 Abs. 1 Nr. 2 GeschGehG: Geheimnishehlerei bei eigener Vortat	405
1. Objektiver Tatbestand	405
2. Subjektiver Tatbestand	405
V. § 23 Abs. 1 Nr. 3 GeschGehG: Geheimnisverrat	406
1. Objektiver Tatbestand	406
2. Subjektiver Tatbestand	407
C. § 23 Abs. 2 GeschGehG: Geheimnishehlerei	407
I. Objektiver Tatbestand	408
II. Subjektiver Tatbestand	408
D. § 23 Abs. 3 GeschGehG: Vorlagenfreibeuterei	409
I. Objektiver Tatbestand	409
1. Tatobjekte: Geheime Vorlagen und technische Vorschriften	409
2. Anvertrautsein im geschäftlichen Verkehr	409
3. Tathandlung: Nutzen oder Offenlegen	410
II. Subjektiver Tatbestand	410
E. § 23 Abs. 4 GeschGehG: Qualifikationstatbestand	410
I. Gewerbsmäßiges Handeln (§ 23 Abs. 4 Nr. 1 GeschGehG)	411
II. Auslandsbezug (Nr. 2 und 3)	411
1. Täter weiß bei der Offenlegung, dass das Geschäftsgeheimnis im Ausland genutzt werden soll	411
2. Täter <i>nutzt</i> das Geschäftsgeheimnis im Ausland	412
F. § 23 Abs. 5 GeschGehG: Versuchsstrafbarkeit	412
G. § 23 Abs. 6 GeschGehG: Beihilfe durch Medienschaffende	413
H. Rechtswidrigkeit	413
I. § 23 Abs. 7 GeschGehG: Auslandstaten (§ 5 StGB) und Versuch der Beteiligung (§§ 30, 31 StGB)	414
I. Auslandstaten	414
II. Versuch der Beteiligung	414
J. Rechtsfolgen, Strafantrag und Verjährung	414

5. Teil Die Verfolgung von Datenschutzstraftaten

§ 25 Anwendbarkeit deutschen Strafrechts – insbesondere bei grenzüberschreitenden, internetbasierten Datenschutzstraftaten (*Klaas*) 417

 A. Praktische Relevanz des Strafanwendungsrechts 418

 B. Extraterritorialer Anwendungsbereich der DS-GVO vs. einschränkendes deutsches Strafanwendungsrecht 419

 C. Grundsätze der Anwendbarkeit des deutschen Strafrechts 419

 I. Geltung für Inlandstaaten 419

 1. Tatort der Haupttat 420

 2. Tatort der Teilnahme 420

 II. Geltung für Auslandstaaten 421

 1. Auslandstaaten mit besonderem Inlandsbezug, § 5 StGB 421

 2. Geltung für Auslandstaaten in anderen Fällen, § 7 StGB 424

 D. Besonderheiten bei internetbasierten Datenschutzverstößen 428

 I. Handlungsort 428

 II. Erfolgsort 429

 1. Erfolgsdelikte 430

 2. Kein Erfolgsort bei schlichten Tätigkeitsdelikten 430

 3. Gefährungsdelikte 430

 4. Stets: Gewährleistung eines „genuine links“ bei Internetsachverhalten 432

 III. Anbieter von Telemedien: Spezielles Strafanwendungsrecht aus § 3 TMG? 433

 1. Wer ist Anbieter eines Telemediums? 433

 2. Herkunftslandprinzip, § 3 Abs. 1 TMG 433

 3. Diensteanbieter mit Sitz im EU-Ausland 436

§ 26 Praktische Überlegungen und Hinweise zum Ablauf eines Strafverfahrens (*Hieramente*) 439

 A. Die Strafanzeige 439

 I. Wahl der Behörde 439

 II. Örtliche Zuständigkeit 440

 III. Form und Frist: Relevant bei Antragsdelikten 442

 IV. Zeitpunkt und Art der Anzeigenerstattung 443

 B. Das Ermittlungsverfahren 445

 I. Struktur des Ermittlungsverfahrens 445

 II. Rolle der Verletztenvertretung 446

 III. Rolle der Verteidigung 447

 C. Das Zwischenverfahren 448

 D. Die Hauptverhandlung 448

 E. Die Rechtsmittel 448

6. Teil Gemeinsame Aspekte von Bußgeldern und Straftatbeständen

§ 27 Verhältnis von Bußgeldtatbeständen (Art. 83 DS-GVO) zu parallel verwirklichten Straftaten (*Klaas*) 449

 A. § 21 OWiG: Konkurrenzverhältnis auf materieller Ebene 449

 I. Begrenzung der Reichweite von § 21 Abs. 1 S. 1 OWiG auf den individuellen Sanktionsadressaten 450

 II. Generelle Einschränkung der Anwendbarkeit von § 21 Abs. 1 S. 1 OWiG? 451

 B. Konkurrenzverhältnis auf prozessualer Ebene 451

 I. (Straf-)Klageverbrauch/Entgegenstehende Rechtskraft 451

 II. Auswirkung von Opportunitätseinstellungen 453

III. Keine Parallelität von Bußgeld- und Strafverfahren: „Anderweitige Rechtshängigkeit“	453
IV. Reichweite von „ne bis in idem“ im unionsrechtlichen Sinne	455
§ 28 Auslegung (unwirksamer) datenschutzrechtlicher Einwilligungen in wirksame rechtfertigende Einwilligungen (<i>Klaas</i>)	457
A. Die doppelte Bedeutung der Einwilligung	457
B. Geltung auch für Geldbußen gem. Art. 83 Abs. 5 lit. a) DS-GVO?	459
C. Grundlegende Anforderungen an die rechtfertigende Einwilligung	459
D. Mildere Anforderungen an eine rechtfertigende Einwilligung	460
I. Keine vorgeschriebene Form	460
II. Möglichkeit der konkludenten Einwilligung	461
1. Praktische Relevanz	461
2. Maßstab und praktische Anwendungsfelder	461
III. Welche Verstöße gegen datenschutzrechtliche Informationspflichten können über die rechtfertigende Einwilligung aufgefangen werden?	462
IV. „Gelockertes“ Kopplungsverbot	463
V. Einwilligungen durch Minderjährige „in Bezug auf Dienste der Informationsgesellschaft“	465
§ 29 Einziehungsmaßnahmen infolge von Datenschutzverstößen (<i>Nadeborn/Lamsfuß</i>)	467
A. Einleitung	468
B. Das Verhältnis zwischen DS-GVO und den nationalen Einziehungsregimen	469
I. Komplementäre Anwendung von DS-GVO und OWiG: Einziehung von Taterträgen nach OWiG	470
II. Komplementäre Anwendung von DS-GVO und StGB: Einziehung von Taterträgen nach StGB	471
III. Gemeinsamkeiten und Unterschiede der Einziehung nach StGB und OWiG	472
C. Einziehung bei Verstößen gegen die DS-GVO	473
I. Vermögensabschöpfung durch die Geldbuße	474
II. Einziehung des Wertes von Taterträgen nach § 29a OWiG	474
1. Einziehung trotz nicht vorwerfbarer Handlung (§ 29a Abs. 1 OWiG)	475
2. Einziehung bei tatunbeteiligten Dritten (§ 29a Abs. 2 OWiG)	476
3. Adressaten der Einziehung	477
4. Höhe des Einziehungsbetrages	478
5. Einziehung bei Erlöschen von Verletztenansprüchen	480
6. Verfahren, Rechtsbehelfe und Rechtsmittel	480
III. Keine Einziehung von Gegenständen bei Verstößen gegen die DS-GVO	482
D. Voraussetzungen der Einziehung nach StGB	482
I. Einziehung von Taterträgen nach §§ 73 ff. StGB	482
1. Rechtswidrige Tat	482
2. Adressat	482
3. Gegenstand der Einziehung	483
4. Sonderfall: Einziehung von Daten	483
5. Ausschluss der Einziehung des Tatertrages oder des Wertersatzes	484
II. Einziehung von Tatmitteln, Tatprodukten und Tatobjekten nach § 74 StGB	484
1. Anknüpfungstat	485
2. Adressat	485
3. Gegenstand der Einziehung	485

4. Sonderfall: Einziehung von Hardware	486
III. Verfahren, Rechtsbehelfe und Rechtsmittel	487
1. Gerichtliche Einziehungsentscheidung	487
2. Vorläufige Sicherung der Einziehung	488
§ 30 Die Ermittlung von Datenschutzverstößen im digitalen Raum (<i>Brodowski</i>)	489
A. „Beweistransfer“ aus aufsichtsrechtlichen Maßnahmen?	490
I. Auskunftsbefugnisse der (Straf-)Verfolgungsbehörden	490
II. Übermittlungsbefugnisse der Datenschutzbehörden und deren Begrenzungen	491
1. Übermittlung an Strafverfolgungsbehörden	491
2. Zweckändernde Folgenutzung durch dieselbe Verwaltungsbehörde	491
3. Zweckändernde Folgenutzung durch andere Verwaltungsbehörde	491
III. Umgehungsverbot	492
B. Allgemeine Befugnisse zur Erhebung digitaler Spuren	492
I. Zugriff auf öffentlich zugängliche Informationsquellen; Auskunftsersuchen und -verlangen	492
II. Herausgabeverlangen (§ 95 StPO)	493
III. Durchsuchung, Durchsicht und Beschlagnahme	494
C. Spezifische, „digitale“ Auskunftsbzw. Ermittlungsbefugnisse	494
I. Erhebung von Telekommunikations-Verkehrsdaten	495
1. Derzeit keine Vorratsdatenspeicherung	495
2. Anordnungsvoraussetzungen	495
3. Straftatbegehung mittels Telekommunikation; Straftat von erheblicher Bedeutung	495
4. Transnationale Verkehrsdatenerhebung	496
II. Erhebung von Nutzungsdaten bei Telemediendiensten	496
III. Erhebung von Bestandsdaten	497
IV. Verdeckte technische Überwachungsmaßnahmen	497
§ 31 Datenschutz-Compliance – Haftungsvermeidung in datenverarbeitenden Organisationen (<i>Jungkind/Petzinka</i>)	499
A. Einleitung	500
B. Haftungsvermeidung in Datenverarbeitungsvorgängen	500
I. Verarbeitung von Daten mit Rechtsgrundlage, Art. 6 DS-GVO	501
1. Compliance-Risiken	501
2. Gestaltung des CMS	503
II. Insbesondere: Weitergabe von Daten an Dritte, Art. 6 DS-GVO	505
1. Compliance-Risiken	505
2. Gestaltung des CMS	507
III. Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9 DS-GVO	508
1. Compliance-Risiken	508
2. Gestaltung des CMS	509
IV. Transparenz der Datenverarbeitung, Art. 5 Abs. 1 lit. a, Art. 12–15 DS-GVO	511
1. Compliance-Risiken	511
2. Gestaltung des CMS	513
V. Maßnahmen zum Schutz vor Angriffen oder Missbrauch, Art. 5 Abs. 1 lit. f und Art. 32 DS-GVO	515
1. Compliance-Risiken	515
2. Gestaltung des CMS	516
C. Fazit	518

§ 32	Melde-, Mitwirkungs- und Rechenschaftspflichten im Spiegel von nemo tenetur (<i>Brodowski</i>)	519
	A. Selbstbelastungsfreiheit im Straf- und Bußgeldverfahren	519
	I. Grundgesetzliche Gewährleistung	519
	II. Unionsrechtliche Gewährleistung	521
	1. Schutz natürlicher Personen	521
	2. Schutz juristischer Personen	522
	B. Konflikte zwischen Melde-, Benachrichtigungs-, Rechenschafts-, Mitwirkungs- und Vorlagepflichten und der Selbstbelastungsfreiheit	523
	I. Konflikte	523
	II. Sanktionen für Verstöße gegen Melde-, Benachrichtigungs-, Rechenschafts-, Mitwirkungs- und Vorlagepflichten im Lichte des Schweigerechts	523
	C. Verwendungsverbote (§§ 42 Abs. 4, 43 Abs. 4 BDSG)	525

7. Teil Datenschutzsanktionenrecht in den USA

§ 33	Überblick über das Datenschutzsanktionenrecht in den USA (<i>Klose/Momsen</i>) ...	527
	A. Grundzüge der Sanktionierungspraxis bei Datenschutzverstößen in den USA	528
	I. Gesetzlicher Rahmen	528
	1. Überblick über datenschutzrechtliche Vorgaben auf Bundesebene ...	528
	2. Abweichende Vorgaben der einzelnen Bundesstaaten	531
	II. Durchsetzung: Keine „zentrale Datenschutzaufsicht“	532
	III. Sanktionen	533
	1. Zivilrechtliche Sanktionen („civil penalties“ oder „civil actions“)	533
	2. Strafrechtliche Sanktionen	536
	3. Individuelle Ansprüche der Betroffenen	536
	4. Überblick über die Sanktionspraxis	537
	B. Verhältnis zur DS-GVO bei Betroffenheit „europäischer Daten“	537
	I. Hintergrund des CLOUD-Act	538
	II. Überblick über den wesentlichen Regelungsgehalt des CLOUD-Act	538
	III. Völkerrechtliche Grenzen einer extraterritorialen Zugriffsregelung	539
	IV. Verhältnis zu den Vorgaben der DS-GVO bei einer Datenübermittlung in die USA	539
	1. Anwendbarkeit der DS-GVO auf US-Unternehmen	540
	2. Voraussetzungen eines Datentransfers in die USA nach DS-GVO ...	540
	3. Ausblick auf die Sanktionspraxis im Anwendungsbereich von CLOUD-Act und DS-GVO	542
	Sachverzeichnis	545