

# Inhaltsverzeichnis

Der Autor sagt „Moin“ – wichtige Leitsätze zum Umgang mit und zu den Zielen des Praxishandbuchs (bitte vorab lesen) .....	V
Verzeichnis: Abbildungen, Diagramme, Tabellen .....	XXI
Abkürzungsverzeichnis .....	XXV
<b>1. Kapitel: Einstieg .....</b>	<b>1</b>
<b>2. Kapitel: Thesen &amp; Kontraste .....</b>	<b>3</b>
I. Übersicht .....	3
II. Literatur, Verbände, Behörden und Normgeber .....	3
1. Überblick .....	3
2. Meinungsbild 1: das VVT als bürokratische Bürde .....	3
3. Meinungsbild 2: das VVT ist nur ein (kleiner) Teil der Rechenschaftspflicht .....	4
4. Meinungsbild 3: Behörden und Gesetzgeber fordern Kontrollfähigkeit .....	5
a) Überblick .....	5
b) Aufsichtsbehörden in Deutschland .....	5
c) Aufsichtsbehörden und Gesetzgeber in weiteren EU-Mitgliedstaaten .....	6
5. Meinungsbild 4: das VVT ist integraler Bestandteil des Datenschutz-Managementsystems .....	6
a) Kirchliches Datenschutzrecht .....	6
b) Aufsichtsbehörde und EDPS .....	7
c) Praxisliteratur und Interessenvertretungen .....	7
III. Amtliche und nicht-amtlche Umfragen sowie Querschnittsprüfungen ..	8
1. Überblick .....	8
2. Spezifische Umfragen und Prüfungen .....	9
a) Umfrage 1: ASB Baden-Württemberg (2019) .....	9
b) Umfrage 2: LRH Niedersachsen (2019) .....	10
c) Umfrage 3: ASB Sachsen (2020) .....	10
d) Umfrage 4: McCann FitzGerald/mazars (2021/22) .....	11
e) Einzelprüfung 1: ASB Saarland (2018/19) .....	11
f) Einzelprüfung 2: ASB Niedersachsen (2018/19) .....	12
g) Einzelprüfung 3: ASB Thüringen (2018) .....	13
h) Einzelprüfungen 4, 5: KDSA Nord (2021) .....	14
i) Einzelprüfung 6: ASB Irland (2022) .....	14
j) Einzelprüfung 7: ASB Niedersachsen (2022) .....	15
k) Prüfbogen: Bulgarien (undatiert) .....	15
l) Sonstige Prüfdokumente der ASB .....	15

m) Weitere Umfragen .....	15
IV. Zwischenergebnisse .....	16
<b>3. Kapitel: Praktische Umsetzung durch vergleichende Betrachtung:</b>	
<b>Recht, Organisation, IT.....</b>	<b>18</b>
I. Übersicht .....	18
II. Recht.....	18
1. Übersicht.....	18
2. Norm- und Gesetzgebung sowie historische Entwicklungen .....	19
a) Internationales Recht.....	19
aa) Übersicht .....	19
bb) Beispiel 1: EMBL .....	19
(1) EMBL .....	19
(2) Binnenorganisation .....	19
(3) Fazit.....	20
cc) Beispiel 2: CERN .....	20
(1) CERN .....	20
(2) Binnenorganisation .....	20
(3) Fazit.....	21
b) EU-Sekundärrecht .....	21
aa) Übersicht .....	21
bb) Vergleich zwischen EU-DSVO, DSGVO, JI-RL .....	21
(1) Zweck .....	21
(2) Historische Vorläufer des Art. 30 Abs. 1 DSGVO	
seit 1977 .....	23
(a) Übersicht der einzelnen „Datenschutz-Epochen“.....	23
(b) Die erste Datenschutz-Epoche (1977–1990).....	27
(c) Die zweite Datenschutz-Epoche (1990–1995) .....	28
(d) Die dritte Datenschutz-Epoche (1995–2016) .....	30
(e) Die vierte Datenschutz-Epoche (ab 2016).....	31
(3) Anwendungsbereich .....	34
(a) Anwendungsbereich .....	34
(b) Ausnahmen zur Pflicht .....	36
(c) Rück-Ausnahmen, die zur Pflicht zurückführen .....	38
(d) Zwischenergebnis .....	40
(4) Pflichtangaben: Übersicht und Vergleich zwischen	
DSGVO, JI-RL, EU-DSVO.....	41
(5) Knotenpunkte innerhalb des Art. 30 Abs. 1 DSGVO .....	43
(6) Knotenpunkte zu Art. 30 DSGVO: Kontrolle, Bußgeld,	
Schadensersatz, Verhaltensregel.....	45
(7) Exkurs: Schadensersatzpflicht bei Verstoß gegen	
Organisationspflichten .....	45
(a) Diskussion auf nationalstaatlicher Ebene .....	45
(b) Entscheidungen des EuGH in den Rechtssachen	
C-300/21, C-60/22.....	47

(c) Einordnung im kirchlichen Datenschutzrecht .....	49
(8) Zwischenergebnis .....	50
c) Umgang mit Art. 30 DSGVO und Art. 24 JI-RL im nationalen Recht am Beispiel der föderalen und der staatskirchenrechtlichen Gesetzgebung in Deutschland .....	50
aa) Übersicht .....	50
bb) Bund- und Landesgesetzgebung in Deutschland .....	50
(1) Übersicht 1: Das allgemeine Datenschutzrecht .....	50
(2) Beobachtung 1.1: Befreiung der Landesrechnungshöfe von der Pflicht des Art. 30 DSGVO .....	50
(3) Beobachtung 1.2: Kopplung des VVT an ein „Freigabeverfahren“ (Risiko-Assessment) und ein „Change Management“ .....	52
(a) Übersicht .....	52
(b) Das „Freigabeverfahren“ .....	52
(c) Das „Change Management“ .....	54
(4) Beobachtung 1.3: Erweiterung der Pflichtangaben bei Umsetzung von Art. 24 JI-RL .....	56
(5) Übersicht 2: Zusammenschau mit dem übrigen Landesrecht .....	56
(6) Beobachtung 2.1: Erweiterung der Pflichtangaben bei Adaption von Art. 30 DSGVO .....	59
cc) Staatskirchenrecht in Deutschland .....	60
d) Gesetzgebung in weiteren EU-Mitgliedstaaten .....	61
aa) Übersicht .....	61
bb) Bereichsprivileg 1: Art. 85 Abs. 2 DSGVO .....	66
cc) Zwischenergebnis .....	68
dd) Bereichsprivileg 2: Art. 89 Abs. 1 DSGVO .....	69
ee) Zwischenergebnis .....	69
ff) Sonderfall: verarbeitungsspezifische Register .....	70
gg) Weitere Konstellationen im Fachrecht der EU-Mitgliedstaaten .....	70
e) Gesetzgebung in Staaten abseits der EU .....	71
f) Zusammenfassung .....	75
3. Rechtsprechung .....	76
a) Übersicht .....	76
b) Einzelne Gerichtsentscheidungen .....	76
aa) Deutschland .....	76
(1) Verwaltungsgerichtsbarkeit .....	76
(2) Vergabekammer .....	78
(3) Arbeitsgerichtsbarkeit .....	78
(4) Zivilgerichtsbarkeit .....	78
bb) Polen .....	79
cc) Belgien .....	79
c) Vertiefung: Verfahren vor dem EuGH .....	79

aa)	Übersicht .....	79
bb)	EuGH, C-579/21: Abgrenzung zwischen Art. 15 und Art. 30 DSGVO.....	80
cc)	EuGH, C-179/21: Kenntnis der Datenlieferanten und Datenempfänger „in der Kette“.....	83
dd)	EuGH, C-60/22: Formelle Rechtswidrigkeit durch fehlendes/mangelhaftes VVT? .....	83
	(1) Ausgangsverfahren .....	83
	(2) Einschub: Umgang mit dieser Frage unter Geltung der DS-RL .....	85
	(3) Entscheidung des EuGH .....	85
d)	Zwischenergebnis .....	86
4.	Aktivitäten der Aufsichtsbehörden .....	87
a)	Übersicht.....	87
b)	Empfehlungen .....	87
c)	Vollzug .....	88
aa)	Datenbasis und Informationsquellen.....	88
	(1) GDPRHub.eu (NOYB e. V.).....	88
	(2) OSS-Register (EDPB).....	93
	(3) Freie Recherche .....	94
bb)	Statistische und inhaltliche Auswertung der Entscheidungs- auswahl .....	95
	(1) Übersicht .....	95
	(2) Begleithinweis .....	95
	(3) Statistische Auswertung: Visualisierung .....	96
	(4) Inhaltsauswertung: Übersicht .....	98
	(5) Inhaltsauswertung: 1. Fallgruppe, direkte Interpretation von Art. 30 DSGVO.....	98
	(6) Inhaltsauswertung: 2. Fallgruppe, Querschnitts- entscheidungen .....	100
d)	Vollzug im Speziellen: Untersuchungen .....	101
aa)	Übersicht .....	101
bb)	Untersuchung 1: Prüfung von Krankenhäusern .....	102
cc)	Untersuchung 2: Prüfung von Energieversorgungs- unternehmen .....	102
dd)	Untersuchung 3: Prüfung von Arztpraxen .....	103
e)	Rückblick: Vollzug in der Zeit vor der DSGVO.....	103
f)	Zwischenergebnis .....	103
5.	Zwischenergebnis (Recht).....	104
III.	Organisation.....	104
1.	Übersicht.....	104
2.	Aufbau- und Ablauforganisation.....	105
a)	Vorfrage: „Verarbeitungstätigkeit“.....	105
aa)	Übersicht .....	105
	(1) Ausgangsfragen .....	105

(2) Operative Bedeutung .....	105
(3) Strategische Bedeutung .....	106
bb) Abgrenzung 1: „Verarbeitungstätigkeit“ und „Verarbeitung“ ..	106
(1) „Verarbeitung“ vs. „Verarbeitungstätigkeit“ nach der DSGVO .....	106
(2) „Verarbeitung“ nach dem Standard-Datenschutzmodell (SDM) .....	107
(a) Prüffähigkeit einer Verarbeitung .....	107
(b) Hierarchisches Begriffsverständnis .....	108
(c) Zwecksingularität oder Zweckpluralität einer Verarbeitung? .....	109
(3) Einordnung der Verarbeitungstätigkeit in einem 3-Ebenen-Modell (Makro, Meso, Mikro) .....	110
(4) Beispiele zur Erläuterung des 3-Ebenen-Modells .....	112
(a) Makro-Ebene .....	112
(b) Meso-Ebene .....	112
(c) Mikro-Ebene .....	112
(5) Darstellung und Zwischenfazit .....	113
cc) Abgrenzung 2: Granularität einer „Verarbeitungstätigkeit“ ..	113
(1) Übersicht .....	113
(2) Bisher diskutierte Merkmale zur Bestimmung einer „Verarbeitungstätigkeit“ .....	115
(a) Übersicht .....	115
(b) Diskurs: Einzelne Merkmalsgruppen und Merkmale ..	118
(3) Vertiefung: Zweckfestlegung einer Verarbeitung durch den Verantwortlichen .....	123
(a) Übersicht .....	123
(b) Grundlagen: Die Ansätze von Podlech (1990) und Hoffmann (1991) .....	124
(c) Vertiefung: „Zweckpräzision“, „Zweckhierarchien“ und „Datenschutzeignung“ .....	127
(d) Zwischenergebnis und Fortführung der Beispiele ..	132
(e) Weitere Ansätze zur „Zweckpräzision“ .....	133
(f) Fazit .....	134
(4) Vorschlag für eine Definition und für die Abgrenzung von „Verarbeitungstätigkeiten“ .....	134
(a) Definitionsvorschlag .....	134
(b) Primär entscheidende Faktoren: Zweck und Risikoneigung .....	134
(c) Korrektive: Kontext und Transparenz .....	135
(d) Bedingt taugliche Merkmale .....	136
(e) Untaugliche Merkmale .....	136
(5) Fallbeispiele in Anknüpfung an den Definitions- vorschlag .....	136
(a) Übersicht und „Bündelungsprozess“ .....	136

(b) Fall 1: Die Zusammenfassung zu einer VT kommt nicht in Betracht .....	138
(c) Fall 2: Die Zusammenfassung zu einer VT kommt bei einem Teil der Verarbeitungen in Betracht .....	138
(d) Fall 3: Die Zusammenfassung zu einer VT kommt bei allen Verarbeitungen in Betracht .....	139
(6) Zwischenergebnis .....	139
dd) Abgrenzung 3: „Verarbeitungstätigkeit“ und „Geschäftsprozess“.....	140
(1) Übersicht .....	140
(2) Prozessbegriff im Qualitätsmanagement .....	141
(3) Bewertung .....	142
(a) Bezugsobjekte im QMS und im VVT .....	142
(b) Prozesseigner im QMS und im VVT .....	142
(c) Einordnung von Organisationseinheiten, die keine VT verantworten .....	143
(d) Zwischenergebnis .....	144
(4) Fallbeispiel: Orientierung an standardisierten Prozessen am Beispiel von ITIL®.....	144
ee) Abgrenzung 4: „Verarbeitungstätigkeit“ und „Geschäftsgeheimnisse“ .....	145
ff) Zwischenergebnis.....	146
b) Auswertung: Praxisbeispiele aus öffentlichen Quellen.....	146
aa) Übersicht .....	146
bb) Quelle 1: Empirie zu den VVT von Organisationen der EU ..	146
(1) Einstieg: Methodik, Auswahl der EU (nahen) Organisationen .....	146
(2) Einsicht 1: ausgewählte Organisationen, Anzahl VVT-Einträge, Status der Veröffentlichung .....	147
(3) Einsicht 2: öffentliche VVT-Einträge nach Art. 31 EU-DSVO im Erhebungszeitraum .....	154
(4) Einsicht 3: quantitative Verteilung der VVT-Einträge ..	155
(5) Einsicht 4: Inhaltliche und prozessuale Auswertung der untersuchten EUI-Verzeichnisse .....	156
(a) Vorgehen .....	156
(b) Aufgabengruppierung (Strukturierung des VVT). .	156
(c) Zusatzangaben im VVT .....	158
(d) Ablaufprozess hinter dem VVT .....	160
(6) Zwischenergebnis .....	162
cc) Quelle 2: Verhaltensregeln (Code of Conduct, CoC).....	162
(1) Übersicht .....	162
(2) Beispiel 1: EGBA (2020) .....	163
(a) Übersicht .....	163
(b) Exkurs: „Verarbeitungsverzeichnis“ vs. „Data Map“ vs. „Verarbeitung“ nach SDM .....	164

(3) Beispiel 2: SCOPE Europe (2020) .....	165
(4) Beispiel 3: GDV (2018) .....	166
(5) Zwischenergebnis .....	166
dd) Quelle 3: Öffentliche Ausschreibungen .....	166
(1) Übersicht .....	166
(2) Fallbeispiel: NTMA (2022) .....	166
(3) Bewertung: die einzelnen Schnittstellen des VVT im DSMS .....	167
(4) Zwischenergebnis .....	168
ee) Quelle 4: Datenschutz-Aufsichtsbehörden und andere öffentliche Stellen .....	169
(1) Übersicht .....	169
(2) Fallgruppe 1: eigene VVT von Aufsichtsbehörden und anderen öffentlichen Stellen .....	169
(3) Fallgruppe 2: Vorlagen, Orientierungshilfen, Online-Tools .....	169
(a) Aufsichtsbehörden .....	169
(b) Andere öffentliche Stellen .....	170
(4) Fallgruppe 3: VVT von öffentlichen Stellen auf Antrag ..	170
(a) Übersicht .....	170
(b) Meinungsbild auf Bundes- und Landesebene .....	171
(5) Zwischenergebnis .....	172
ff) Quelle 5: Binding Corporate Rules (BCR) .....	172
(1) Übersicht .....	172
(2) Empfehlungen 01/2022 des EDPB zu BCR (Version 1.0, 2.0) .....	173
(3) Auswertung: Vorgaben zum VVT in veröffentlichten BCR-C .....	174
(4) Zwischenergebnis und Bewertung der ausgewählten BCR .....	178
gg) Zwischenergebnis .....	178
c) Ableitung von Standard-Anforderungen bzw. Entscheidungsbedarfe für die Aufbau- und Ablauforganisation ..	179
aa) Übersicht .....	179
bb) Aufbau- und Ablauforganisation .....	179
(1) Definition .....	179
(2) Übersicht der Standard-Anforderungen A1 bis A14 .....	180
(3) Zielsetzung und Beschreibung der Standard-Anforderungen A1 bis A14 .....	180
cc) Zwischenergebnis .....	184
d) Vertiefung von Einzelfragen im Rahmen der Aufbau- und Ablauforganisation .....	184
aa) Übersicht .....	184
bb) Einzelne Entscheidungsbedarfe .....	184

(1) Isoliertes oder integriertes VVT, Reifegrad, Kennzahlen (A1) .....	184
(a) Kontrollfragen .....	184
(b) Begleitende Hinweise mit Beispielen der Auswirkungen dieser ersten Entscheidung .....	185
(2) Verhältnisse in und Verlinkungen zu anderen Managementsystemen (A2) .....	186
(a) „Managementsystem“.....	186
(b) Verhältnis zwischen mehreren Management-systemen.....	186
(c) Beispiel 1: Informationssicherheits-Management-system (ISMS) .....	187
(d) Beispiel 2: Datenschutzmanagementsystem (DSMS) .....	189
(3) Notwendige Aktivitäten im VVT-Workflow (A3).....	191
(a) Übersicht .....	191
(b) Fallgruppe 1: Aktivitäten zur „Führung“ im weiteren Sinne .....	192
(c) Fallgruppe 2: Aktivitäten zur „Führung“ im engeren Sinne .....	195
(d) Zwischenfrage: Führung des VVT als Verarbeitungstätigkeit?.....	198
(4) Rollen und Zuständigkeiten im VVT-Workflow, insbesondere des Betriebsrats und des Datenschutzbeauftragten (A4).....	198
(a) Übersicht .....	198
(b) Rollen im Rahmen der „Führung“ des VVT .....	198
(c) Rolle 1: Rolle des Datenschutzbeauftragten .....	199
(d) Rolle 2: Rolle des VVT-Managers .....	202
(e) Rolle 3: Rolle des Betriebsrats .....	202
(5) Pflichtenverteilung im arbeitsteiligen Umfeld mit konzernexternen Entitäten (A5) .....	208
(a) Übersicht .....	208
(b) Beispiel 1: Zusammenwirken von gemeinsam Verantwortlichen .....	208
(c) Beispiel 2: Zusammenwirken von Verantwortlichen und Auftragsverarbeiter .....	209
(6) Kapazitäten, speziell Ressourcenbindung durch Change-Management (A6) .....	211
(7) Umgang mit verteilten Zuständigkeiten im Konzernverbund (A7) .....	212
(8) Umgang mit abweichenden VVT-Inhalten je Land/Region (A8) .....	214
(9) Amtssprache vs. Organisationssprache vs. Informationssprache, was gilt? (A9) .....	214

(10) Hilfsmittel zur prozessualen Darstellung des VVT-Workflows (A10) .....	216
(11) Versionen des VVT für externe Empfänger (A11) .....	217
(a) Übersicht .....	217
(b) Verständlichkeit, Übersichtlichkeit .....	217
(c) Zeitvorgabe zur Bereitstellung .....	218
(d) Weitere Anlässe zur Zugänglichmachung des VVT ..	218
(e) Sonstiges.....	219
(f) Exkurs: Detailtiefe und Dynamik der Beschreibung der TOM nach Art. 30 Abs. 1 lit. g DSGVO.....	219
(12) Festlegung der formalen Elemente eines VVT (A12) .....	221
(a) Übersicht .....	221
(b) Einzelne formale Elemente.....	221
(13) Festlegung von Zusatzangaben im VVT (A13) .....	223
(a) Übersicht .....	223
(b) Daumenregeln .....	223
(c) Einzelne Zusatzangaben .....	224
(14) Festlegung von Verknüpfungen der VT zu anderen Objekten (A14) .....	226
(a) Übersicht .....	226
(b) Einzelne Verknüpfungen.....	227
cc) Zwischenergebnis.....	229
e) Reifegrad und Kennzahlen.....	229
aa) Übersicht .....	229
bb) Qualitativer Ansatz: Reifegrad .....	229
(1) Übersicht.....	229
(2) Reifegradmodelle im Datenschutz .....	231
(3) Praxisbeispiele für das VVT .....	234
(a) Beispiel 1: bitkom.e. V. (Beta, 2022) .....	234
(b) Beispiel 2: CNIL (Entwurf, 2021) .....	238
(c) Vergleich beider Modell-Entwürfe.....	239
(4) Zwischenergebnis .....	243
cc) Quantitativer Ansatz: (Leistungs-)Kennzahlen .....	243
(1) Übersicht.....	243
(2) Leistungskennzahlen im DSMS .....	244
(3) Zwischenergebnis .....	247
(4) Leistungskennzahlen für die dem VVT zugeordneten Prozesse .....	247
3. Zwischenergebnis (Organisation).....	248
IV. IT .....	249
1. Übersicht: zulässige Formformate.....	249
2. Die „elektronische“ Form .....	249
3. Auswahl und Migration einer softwaregestützten Lösung .....	251
a) Marktangebot und Angebotsmarkt .....	251
b) Auswahlfaktoren .....	251

c) Mitbestimmung des Betriebsrats.....	251
4. Fallbeispiele: funktionale Anforderungen, softwaregestützte Implementierung .....	252
a) Übersicht.....	252
b) Fallbeispiel 1: NTMA (2022) (Fortsetzung).....	252
c) Fallbeispiel 2: EMBL-EBI: Data Protection Engine (DPE) .....	253
5. Umsetzung Standard-Anforderung 14: Verknüpfungen zum VVT ..	254
a) Übersicht.....	254
b) Identifizierung geeigneter Schnittstellen .....	254
aa) Übersicht.....	254
bb) Beispiele für Systemschnittstellen zum VVT: Vertrags-, Vendor- und Asset-Management.....	255
(1) Einstieg .....	255
(2) Fall 1: Change-Management.....	256
(a) Anforderung .....	256
(b) Asset-Lokation: Umgang mit dynamischen Datenübermittlungen (Art. 30 Abs. 1 lit. e DSGVO) .....	256
(c) Prozess: Umgang mit Änderungen der Rechtslage ..	258
(3) Fall 2: Vertragsgestaltung .....	260
(a) Anforderung .....	260
(b) Beispiele.....	260
(4) Fall 3: Risikobewertung.....	261
(a) Szenario 1: Positionierung von ASB zu einzelnen Produkten.....	261
(b) Szenario 2: Bekannt gewordene Schwachstellen von eingesetzten Assets.....	261
c) Zwischenergebnis .....	262
6. Gemeinsame Sprache: Ontologie & Taxonomie, Enterprise Architecture .....	262
a) Übersicht.....	262
b) Disziplin 1: Ontologie und Taxonomie.....	263
aa) Grundlagen .....	263
bb) Relevanz für das VVT .....	263
(1) Herleitung eines formalen Modells .....	263
(2) Etablierung einer Taxonomie .....	264
(a) Übersicht .....	264
(b) ISO 19944 .....	264
(c) „Privacy Taxonomy“ (Ethycा) .....	264
(d) „Data Privacy Vocabulary“ (W3C) .....	265
(3) Regional- und länderspezifische Besonderheiten.....	265
(4) Aktualisierung des Vokabulars .....	266
c) Disziplin 2: Enterprise Architecture Management .....	266
aa) Grundlagen .....	266
bb) Relevanz von EA für das DSMS, speziell das VVT .....	267
7. Zwischenergebnis (IT).....	268

<b>4. Kapitel: Gesamtergebnis . . . . .</b>	<b>269</b>
<b>5. Kapitel: Audit-Checkliste . . . . .</b>	<b>271</b>
I. Übersicht . . . . .	271
II. Audit-Checkliste . . . . .	272
<b>Quellenverzeichnis . . . . .</b>	<b>277</b>
I. Übersicht: Metriken und Statistiken des Quellenapparats . . . . .	277
II. Auszug Quellen 1: Facharbeiten, Literatur . . . . .	280
III. Auszug Quellen 2: Exekutive (in Teilen) . . . . .	287
IV. Auszug Quellen 3: Legislative (in Teilen) . . . . .	293
V. Auszug Quellen 4: Private Akteure, Selbstregulierung . . . . .	293
VI. Der Autor sagt „Weest bedankt!“ . . . . .	297
<b>Sachregister . . . . .</b>	<b>299</b>