

TIM TEMPLIN

Verhaltensregeln

Beiträge zum Verwaltungsrecht

Mohr Siebeck

Beiträge zum Verwaltungsrecht

herausgegeben von

Wolfgang Kahl, Jens-Peter Schneider
und Ferdinand Wollenschläger

38



Tim Templin

Verhaltensregeln

Theorie und Praxis regulierter Selbstregulierung im
europäischen Datenschutzrecht

Mohr Siebeck

Tim Templin, geboren 1996; Studium an der Albert-Ludwigs-Universität Freiburg, 2014–2019; Promotion an der Universität des Saarlandes (2019–2024).

ISBN 978-3-16-164044-5 / eISBN 978-3-16-164045-2

DOI 10.1628/978-3-16-164045-2

ISSN 2509-9272 / eISSN 2569-3859 (Beiträge zum Verwaltungsrecht)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über <https://dnb.dnb.de> abrufbar.

© 2025 Mohr Siebeck Tübingen. www.mohrsiebeck.com

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für die Verbreitung, Vervielfältigung, Übersetzung und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satz: Laupp & Göbel, Gomaringen

Gedruckt auf alterungsbeständigem Papier.

Mohr Siebeck GmbH & Co. KG, Wilhelmstraße 18, 72074 Tübingen, Deutschland
www.mohrsiebeck.com, info@mohrsiebeck.com

Printed in the Netherlands.

Meiner Familie

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2023/2024 von der Rechtswissenschaftlichen Fakultät der Universität des Saarlandes als Dissertation angenommen. Die hier vorliegende Fassung wurde für die Drucklegung mit Hinblick auf Literatur und Rechtsprechung aktualisiert. Sie befindet sich auf dem Stand von Februar 2024.

Mein besonderer Dank gebührt meinem Doktorvater Herrn Prof. Dr. Nikolaus Marsch, D.I.A.P. (ENA). Bereits während meiner Studienzeit in Freiburg weckte er mein wissenschaftliches Interesse am Datenschutzrecht und begleitet seitdem meinen juristischen Werdegang. Die Erstellung dieser Arbeit wäre mir ohne seine wohlgesetzten Ratschläge, seine ansteckende Begeisterung für die rechtswissenschaftliche Forschung sowie die Freiräume, die er mir für die Erstellung der Arbeit geschaffen hat, nicht möglich gewesen. Frau Prof. Dr. Annette Guckelberger danke ich für die Erstellung des Zweitgutachtens sowie ihre wertvollen Anmerkungen, die zur Qualität der Arbeit erheblich beigetragen haben.

Ich hatte das Privileg, an einem Lehrstuhl tätig zu sein, dessen Mitglieder stets eine freundschaftliche und unterstützende Atmosphäre zu schaffen vermochten, die meine Promotionszeit wissenschaftlich wie auch persönlich ungemein bereichert hat. Hierfür sei ihnen herzlich gedankt.

Nicht zuletzt sei auch meinen Eltern Andrea und Jörg Templin gedankt, deren Rückhalt und Unterstützung ich mir stets sicher sein konnte.

Inhaltsübersicht

Vorwort	VII
Inhaltsverzeichnis	XI
A. Einleitung: Objekt und Verlauf der Untersuchung	1
B. Verfahren und Rechtsfolgen des Art. 40 DS-GVO im Überblick	7
I. Verfahren	7
II. Prüfungsmaßstab und notwendiger Inhalt von Verhaltensregeln	17
III. Rechtsfolgen	21
IV. Auslegungsspielräume	26
C. Datenschutzrechtliche Verhaltensregeln nach Art. 40 DS-GVO in der Praxis	39
I. Die Verhaltensregeln der Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen (Österreich)	40
II. Die Verhaltensregeln für Internet Service Provider (Österreich)	42
III. Die Verhaltensregeln für Bilanzbuchhaltungsberufe (Österreich)	44
IV. Verhaltensregeln für die Verarbeitung von mit intelligenten Messsystemen erhobene personenbezogenen Daten (Österreich)	47
V. Der Verhaltenskodex für smartes Netzmanagement (Niederlande)	50
VI. Verhaltensregeln für die Ausübung des Gewerbes der Adressverlage und Direktmarketingunternehmen (Österreich)	53
VII. Verhaltensregeln für die Datenverarbeitung im Rahmen von Werbetätigkeiten (Spanien)	56
VIII. Verhaltensregeln für die Verarbeitung personenbezogener Daten im Bereich klinischer Studien und anderer klinischer Forschung und der Pharmakovigilanz (Spanien)	58
IX. Verhaltenskodex für die Verarbeitung von personenbezogenen Daten in den gemeinsamen Informationssystemen des Versicherungssektors (Spanien)	64
X. Die Verhaltensregeln für die Prüf- und Löschrufen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien (Deutschland)	69

XI. Verhaltensregeln zu technischen und organisatorischen Maßnahmen der Notarinnen und Notare im Hinblick auf elektronische Aufzeichnungen und Hilfsmittel (Deutschland)	74
XII. Data Pro Code (Niederlande)	75
XIII. Verhaltensregeln „Anforderungen an die Auftragsverarbeiter nach Art. 28 DS-GVO – Trusted Data Processor“ (Deutschland)	77
XIV. Transnationale Verhaltensregeln für Cloud-Anbieter	79
XV. Die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft als Sonderfall	85
XVI. Ergebnisse des Vergleichs der Verhaltensregeln	86
D. Regulierungsziele und -konzepte	103
I. Der Begriff der Regulierung	103
II. Regulierungsziele der DS-GVO	103
III. Regulierungskonzepte	105
IV. (Regulierte) Selbstregulierung in anderen Rechtsgebieten	141
E. Schlussfolgerungen	177
I. Schlussfolgerungen für die Auslegung des Art. 40 DS-GVO	178
II. Rechtspolitische Bewertung des Art. 40 f. DS-GVO	210
III. Erkenntnisse zum Konzept der Regulierten Selbstregulierung	215
F. Fazit und Ausblick	219
Literaturverzeichnis	223
Register	233

Inhaltsverzeichnis

Vorwort	VII
Inhaltsübersicht	IX
A. Einleitung: Objekt und Verlauf der Untersuchung	1
B. Verfahren und Rechtsfolgen des Art. 40 DS-GVO im Überblick	7
<i>I. Verfahren</i>	<i>7</i>
1. Vorlageberechtigte Stellen	7
2. Vorabverfahren und Konsultationen nach EG 99 DS-GVO	8
3. Zuständige Aufsichtsbehörde	9
4. Genehmigungsverfahren bei nationalen Verhaltensregeln	9
5. Genehmigungsverfahren bei transnationalen Verhaltensregeln	13
a) Stellungnahmeverfahren und Beschlussverfahren	14
b) Streitbeilegungsverfahren	15
6. Das Verfahren zum Erlass eines Durchführungsrechtsakts	16
<i>II. Prüfungsmaßstab und notwendiger Inhalt von Verhaltensregeln</i>	<i>17</i>
1. Beitrag zur ordnungsgemäßen Anwendung der DS-GVO	17
2. Einrichtung einer akkreditierten Überwachungsstelle	18
3. Zusätzliche Anforderungen an Verhaltensregeln i. S. d. Art. 40 Abs. 3 DS-GVO	20
<i>III. Rechtsfolgen</i>	<i>21</i>
1. Genehmigung nach Art. 40 Abs. 5 DS-GVO	21
a) Bindungswirkung gegenüber der Aufsichtsbehörde	21
b) Bindungswirkung gegenüber den Verantwortlichen und Auftragsverarbeitern sowie den Betroffenen	23
2. Stellungnahme des EDSA nach Art. 64 Abs. 1 DS-GVO	23
3. Verbindlicher Beschluss des EDSA nach Art. 65 Abs. 1 DS-GVO	24
4. Erklärung der allgemeinen Gültigkeit nach Art. 40 Abs. 9 DS-GVO	24
5. Offene Fragen	25
<i>IV. Auslegungsspielräume</i>	<i>26</i>

1. Rechtsfolgen der Genehmigung i. S. d. Art. 40 Abs. 5 DS-GVO	26
a) Die Bindungswirkung feststellender Verwaltungsakte	26
b) Der Wortlaut der DS-GVO	27
c) Die Vorgängerregelung des Art. 27 DS-RL und § 38a BDSG a. F./ Der Wille des Ordnungsgebers	28
aa) Die rechtliche Umsetzung in der DS-RL	28
bb) Die Wahrnehmung in der Praxis	29
cc) Die Neuerungen der DS-GVO	30
dd) Der Übergang zur DS-GVO	31
2. Rechtsfolgen der Allgemeingültigkeitserklärung nach Art. 40 Abs. 9 DS-GVO	31
a) Der Wortlaut der DS-GVO	32
b) Vorgängerregelung Art. 27 DS-RL, § 38a BDSG	32
c) Der Rechtscharakter von Durchführungsrechtsakten	33
3. Zwischenfazit: Der Wortlaut und die Entstehungsgeschichte taugen nur als Anhaltspunkt einer Auslegung des Art. 40 DS-GVO	37
 C. Datenschutzrechtliche Verhaltensregeln nach Art. 40 DS-GVO in der Praxis	39
 <i>I. Die Verhaltensregeln der Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen (Österreich)</i>	40
1. Betroffene Personen- und Datenkategorien	40
2. Die datenschutzrechtliche Rollenverteilung	40
3. Die Betroffenenrechte gem. Art. 12 ff. DS-GVO	41
4. Materielle Pflichten	41
5. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	42
6. Zusammenfassung	42
 <i>II. Die Verhaltensregeln für Internet Service Provider (Österreich)</i>	42
1. Die Bestimmung des Verantwortlichen i. S. d. Art. 4 Nr. 7 DS-GVO	43
2. Die Betroffenenrechte (Art. 12 ff. DS-GVO) und die Data-Breach- Notification (Art. 33 f. DS-GVO)	43
3. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	44
4. Zusammenfassung	44
 <i>III. Die Verhaltensregeln für Bilanzbuchhaltungsberufe (Österreich)</i>	44
1. Die datenschutzrechtliche Verantwortlichkeit	45
2. Die Rechtsgrundlage der Datenverarbeitung	45
3. Besondere Datenkategorien gem. Art. 9 DS-GVO	46

4. Materielle Pflichten	46
5. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	46
6. Zusammenfassung	47
<i>IV. Verhaltensregeln für die Verarbeitung von mit intelligenten Messsystemen erhobenen personenbezogenen Daten (Österreich)</i>	<i>47</i>
1. Informationspflichten bei der Einführung intelligenter Messsysteme . . .	48
2. Die datenschutzrechtliche Rollenverteilung	48
3. Gesetzliche Grundlagen der Datenverarbeitung i. S. d. Art. 6 DS-GVO und Umfang der Datenverarbeitung	48
4. Heranziehung von Auftragsverarbeitern nach Art. 28 DS-GVO	49
5. Vorgaben zur Sicherheit der Verarbeitung gem. Art. 32 DS-GVO und zur Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO	49
6. Die Betroffenenrechte gem. Art. 12 ff. DS-GVO	49
7. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	49
8. Zusammenfassung	50
<i>V. Der Verhaltenskodex für smartes Netzmanagement (Niederlande)</i>	<i>50</i>
1. Branchenspezifische Definitionen	51
2. Die Betroffenenrechte und Informationspflichten nach Art. 12 ff. DS-GVO	51
3. Der Verarbeitungszweck und die Rechtsgrundlage der Verarbeitung nach Art. 6 DS-GVO	51
4. Die Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und die Konsultation der Datenschutzaufsichtsbehörde gem. Art. 36 DS-GVO . .	51
5. Die Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	52
6. Zusammenfassung	52
<i>VI. Verhaltensregeln für die Ausübung des Gewerbes der Adressverlage und Direktmarketingunternehmen (Österreich)</i>	<i>53</i>
1. Definition branchenspezifischer Begriffe	53
2. Die datenschutzrechtliche Rollenverteilung	53
3. Die Pflichten bei der Datenerhebung und -verarbeitung	54
4. Die Datenverarbeitung als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DS-GVO	54
5. Vorgaben zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO	54
6. Die Betroffenenrechte	55
7. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	55
8. Zusammenfassung	55

<i>VII. Verhaltensregeln für die Datenverarbeitung im Rahmen von Werbetätigkeiten (Spanien)</i>	56
1. Die Pflichten bei der Datenerhebung und -verarbeitung	57
2. Die Rechtsgrundlage der Verarbeitung i. S. d. Art. 6 Abs. 1 DS-GVO	57
3. Die Betroffenenrechte	57
4. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	57
5. Zusammenfassung	58
<i>VIII. Verhaltensregeln für die Verarbeitung personenbezogener Daten im Bereich klinischer Studien und anderer klinischer Forschung und der Pharmakovigilanz (Spanien)</i>	58
1. Definition von Fachbegriffen	59
2. Grundsätze der Verarbeitung personenbezogener Daten i. S. d. Art. 5 DS-GVO	59
3. Die datenschutzrechtliche Rollenverteilung	60
4. Die Rechtsgrundlage der Verarbeitung und die Zweckänderung	60
5. Vorgaben zu den Art. 25, 30, 32, 35 und 36 DS-GVO	61
6. Vorgaben zur Auftragsverarbeitung i. S. d. Art. 4 Nr. 8, 28 DS-GVO	61
7. Vorgaben zu den Art. 33 und 34 DS-GVO	61
8. Vorgaben zur Pseudonymisierung	62
9. Nichtdatenschutzrechtliche Meldepflichten	62
10. Betroffenenrechte und Informationspflichten	62
11. Datenübertragung an Drittländer und internationale Organisationen	62
12. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	63
13. Sonstige Vorgaben	63
14. Zusammenfassung	64
<i>IX. Verhaltenskodex für die Verarbeitung von personenbezogenen Daten in den gemeinsamen Informationssystemen des Versicherungssektors (Spanien)</i>	64
1. Die datenschutzrechtliche Rollenverteilung	65
2. Grundsätze und Rechtsgrundlage der Verarbeitung gem. Art. 5 f. DS-GVO	66
3. Technisch-organisatorische Maßnahmen gem. Art. 25 Abs. 1 DS-GVO	66
4. Pflichten nach Art. 13, 30, 33, 34 und 37 ff. DS-GVO	67
5. Betroffenenrechte und Informationspflichten nach Art. 12 ff. DS-GVO	67
6. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	67
7. Kooperation mit Justizbehörden	68
8. Zusammenfassung	68
a) Der Verhaltenskodex als Unikum	68
b) Weitere Besonderheiten im Sanktionssystem	69

<i>X. Die Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien (Deutschland)</i>	69
1. Zielsetzung und Entstehungsgeschichte der Verhaltensregeln	70
2. Inhalt der Verhaltensregeln	71
3. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	72
4. Gerichtliche Rezeption der Verhaltensregeln	72
a) Entscheidungen mit Aussagen zur Rechtswirkung von Verhaltensregeln	72
b) Entscheidungen mit Aussagen bezüglich der Rechtmäßigkeit des Inhalts der Verhaltensregeln	73
5. Zusammenfassung	74
<i>XI. Verhaltensregeln zu technischen und organisatorischen Maßnahmen der Notarinnen und Notare im Hinblick auf elektronische Aufzeichnungen und Hilfsmittel (Deutschland)</i>	74
<i>XII. Data Pro Code (Niederlande)</i>	75
1. Vorgaben für die Auftragsverarbeitung nach Art. 28 DS-GVO	75
2. Grundsätze der Datenverarbeitung gem. Art. 5 DS-GVO	76
3. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	76
4. Zusammenfassung	76
<i>XIII. Verhaltensregeln „Anforderungen an die Auftragsverarbeiter nach Art. 28 DS-GVO – Trusted Data Processor“ (Deutschland)</i>	77
1. Vorgaben für die Auftragsverarbeitung nach Art. 28 DS-GVO	78
2. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und dem Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	78
3. Zusammenfassung	78
<i>XIV. Transnationale Verhaltensregeln für Cloud-Anbieter</i>	79
1. Anwendungsbereich	80
2. Datenschutzrechtliche Rollenverteilung	81
3. Vorgaben zum Verarbeitungsvertrag gem. Art. 28 Abs. 3 DS-GVO	81
4. Vorgaben zur Sicherheit der Verarbeitung gem. Art. 32 DS-GVO	81
5. Weitere materielle Vorgaben	82
6. „Controls“ als Mittel zur Umsetzung und Kontrolle	82
7. Compliance-Levels	83
8. Wahrnehmung in der Praxis	83
9. Vorgaben zur Stelle gem. Art. 41 Abs. 1 DS-GVO und der Überwachungsverfahren nach Art. 40 Abs. 4 DS-GVO	84
10. Zusammenfassung	84

<i>XV. Die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft als Sonderfall</i>	85
<i>XVI. Ergebnisse des Vergleichs der Verhaltensregeln</i>	86
1. Schwerpunkte der Konkretisierung	86
a) Umfassende und spezialisierte Verhaltensregeln	86
b) Die Funktion der Verhaltensregeln	86
c) Norm- und sektorspezifische Unterschiede der Konkretisierungsdichte	87
d) Meinungsdivergenzen zwischen Aufsichtsbehörden und vorlegenden Verbänden und Vereinigungen	89
2. Anreize	89
a) Verhaltensregeln als Compliance-Erleichterung und Beitrag zur Rechtssicherheit	89
b) Außendarstellung	90
aa) Abgrenzung zu den Zertifizierungen gem. Art. 42 DS-GVO	90
(1) Der Zweck als Ansatz zur Abgrenzung	91
(2) Unterschiedliche Akteure und Verfahren	92
(3) Ähnliche, aber nicht identische Anreize	93
bb) Verhaltensregeln als Wettbewerbsvorteil für Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DS-GVO	94
c) Negative Anreize	94
aa) Die Verfahrensdauer der Genehmigung der Verhaltensregeln und Akkreditierung der Überwachungsstelle	95
bb) Kosten der Erstellung und Genehmigung von Verhaltensregeln und Akkreditierung von Überwachungsstellen	96
cc) Kosten des Beitritts zu Verhaltensregeln	97
dd) Rechtliche Unsicherheiten	97
3. Nationale Besonderheiten	98
a) Österreich	98
b) Spanien	98
aa) Art. 65 Abs. 4 des spanischen Datenschutzgesetzes als Norm der Regulierten Selbstregulierung	99
bb) Zweifel an der Vereinbarkeit mit der DS-GVO	99
4. Die vorlegenden Vereinigungen und Verbände	100
5. Die Wahrnehmung der Verhaltensregeln	101
 D. Regulierungsziele und -konzepte	 103
<i>I. Der Begriff der Regulierung</i>	<i>103</i>
<i>II. Regulierungsziele der DS-GVO</i>	<i>103</i>
1. Binnenmarktharmonisierung	104
2. Schutz der Grundrechte und Grundfreiheiten	104
3. Zielsetzungen auf verschiedenen Ebenen	105

<i>III. Regulierungskonzepte</i>	105
1. Hoheitliche Regulierung	106
a) Hoheitliche Regulierung als Ausgangspunkt	106
b) Defizite der hoheitlichen Regulierung	107
aa) Der Wandel zur Informationsgesellschaft als Herausforderung	108
bb) Die wachsende Bedeutung des Steuerungswissens	108
cc) Der Einfluss der Globalisierung	109
dd) Wachsende Staatsaufgaben	110
ee) Vollzugsdefizite	110
ff) Staatsferne als Verfassungsvorgabe	111
c) Modernisierungsansätze	112
aa) Die Einbeziehung Privater	112
bb) Flexible Verfahren und erweiterte Exekutivkompetenzen	113
cc) Informelles Verwaltungshandeln	113
dd) Begrenzte Möglichkeiten zur Modernisierung	114
2. Selbstregulierung	114
a) Definitionsansätze	115
b) Die Organisationsform	115
c) Der angestrebte Zweck	116
d) Die Abgrenzung zur Regulierten Selbstregulierung	117
e) Erwartungen an die Selbstregulierung	118
f) Kritik an der Selbstregulierung	119
aa) Einbeziehung aller relevanten Akteure	120
(1) Trittbrettfahreffekte	120
(2) Selbstregulierung als Markteintrittsschranke	120
(3) Belange Dritter	121
bb) Mangelnde Berücksichtigung von Gemeinwohlinteressen und Informationsasymmetrie	121
cc) Eingeschränkte Sanktionsmöglichkeiten	122
g) Die Bedeutung von Anreizen	123
aa) Erscheinungsformen staatlich gesetzter Anreize	124
bb) Anreize im Rahmen der Selbstregulierung	125
h) Grenzen der Selbstregulierung	125
i) Die Steuerungsverantwortung als Ansatzpunkt	126
3. Regulierte Selbstregulierung	127
a) Begriffsdefinition und Konzept	128
aa) Die Rolle der Privaten	129
bb) Die rechtliche Steuerung als Merkmal der Regulierten Selbstregulierung	130
(1) Die Induzierung privater Beteiligung durch staatlich gesetzte Anreize	131
(a) Kosten und Risiken der Regulierten Selbstregulierung als negative Anreize	131

(b) Ausgestaltungsmöglichkeiten staatlich gesetzter Anreize . . .	132
(aa) Rein finanzielle Anreize	132
(bb) Der (teilweise) Verzicht auf staatliche Eingriffe als Anreiz	133
(2) Die Gewährleistungsverantwortung des Staates/ Verfahrens- und Zielvorgaben sowie die Auffangzuständigkeit des Staates . . .	133
(a) Inhaltliche Kontrolle	134
(b) Verfahrensvorgaben und Qualifikationserfordernisse	135
(c) Berichts- und Evaluationspflichten	136
b) Einordnung des Art. 40 DSGVO in das Konzept der Regulierten Selbstregulierung	137
aa) Die Rolle der Privaten	137
bb) Die rechtliche Steuerung der Verhaltensregeln	138
(1) Staatliche gesetzte Anreize im Zusammenhang mit Art. 40 DS-GVO	138
(a) Rechtssicherheit	138
(b) Allgemein gültige Verhaltensregeln als Grundlage für den Datentransfer in Drittländer	139
(2) Die Umsetzung der staatlichen Gewährleistungsverantwortung	139
(3) Eine erste Einordnung der rechtlichen Steuerung der Verhaltensregeln	140
IV. (Regulierte) Selbstregulierung in anderen Rechtsgebieten	141
1. Private Normsetzung zur Vermeidung einseitig hoheitlicher Normsetzung am Beispiel umweltrechtlicher Selbstverpflichtungen	143
a) Verfahren und Inhalt	143
b) Anreize	144
c) Die Perspektive des Staates	145
d) Umsetzung der Regulierungsziele	145
e) Vergleich	146
aa) Unterschiede und Gemeinsamkeiten normvermeidender und normkonkretisierender Regelwerke	146
bb) Unterschiedliche Bezugspunkte und Interventionspotentiale	147
cc) Möglicher Inhalt	148
dd) Zusammenfassung	148
2. Private Normsetzung zur Vorbereitung hoheitlicher Regulierung am Beispiel der Accounting-Standards-VO	149
a) Verfahren der Standardsetzung	149
b) Zweck und Inhalt der Rechnungslegungsstandards	150
c) Die Interessensituation der Privaten	150
d) Verfahren der Rezeption	151
e) Interessen des Verordnungsgebers	152

f) Umsetzung der Regulierungsziele	153
g) Vergleichbarkeit mit Art. 40 DS-GVO	153
aa) Die Regulierungsziele der Verordnungen	154
bb) Konzeptionelle Vergleichbarkeit mit Art. 40 DS-GVO	154
(1) Die IFRS als normvorbereitende Regelwerke – Fremdprogrammierungsanteile und die Rezeption als politische Entscheidung	154
(a) Die Rezeption der IFRS als (auch) politische Entscheidung – Vergleich zu Art. 40 Abs. 9 DS-GVO	156
(b) Unterschiede im Umfang der Fremdprogrammierung	156
(c) Möglichkeit einer konzeptionellen Vergleichbarkeit der IFRS und allgemein gültiger Verhaltensregeln nach Art. 40 Abs. 9 DS-GVO	157
(2) Vergleichbarkeit trotz teilweiser Kategorisierung der Rechnungslegungsstandards als „Expertenrecht“	157
(a) Aushandlungsprozesse im Rahmen der technischen Standardsetzung	158
(b) Konsequenzen für die Vergleichbarkeit der IAS-VO mit Art. 40 DS-GVO	159
(3) Private Regelwerke als Grundlage der Binnenmarktharmonisierung	159
(4) Die Binnenmarktharmonisierung als mögliches Telos des Art. 40 Abs. 9 DS-GVO	160
cc) Unterschiede im Verfahren und der demokratischen Legitimation	160
3. Normausfüllende, normergänzende und normakzessorische private Regelwerke	161
a) Rechtlich nicht rezipierte Verhaltensregeln am Beispiel des DVTM-Kodex	162
aa) Zielsetzung	162
bb) Die Erstellung des Kodex	162
cc) Ausgestaltung	163
dd) Anreize	163
ee) Die Umsetzung der Regulierungsziele	164
ff) Vergleichbarkeit mit Verhaltensregeln nach Art. 40 DS-GVO	165
(1) Keine rechtlich normierte Steuerung	165
(2) Vergleichbare Ziele der Privaten	165
(3) Fazit	165
b) Möglichkeiten zur Ausgestaltung rechtlich rezipierter Verhaltensregeln am Beispiel der Wettbewerbsregeln	166
aa) Der Zweck von Wettbewerbsregeln	166
bb) Die Zielsetzung der Privaten	167
cc) Regulierungsziele des Staats	168

dd) Ausgestaltung	169
(1) Die 6. GWB-Novelle	169
(2) Die Praxis nach der 6. GWB-Novelle:	170
(3) Die 7. GWB-Novelle	170
ee) Veränderte Anreizsituation durch die Gesetzesänderung	171
(1) Wegfall der Freistellungsmöglichkeit	171
(2) Rechtsprechungsänderung	172
ff) Praktische Auswirkung	172
gg) Vergleich mit Art. 40 DS-GVO	172
(1) Die Interessensituation der Privaten	172
(2) „Negative“ Anreize	173
(3) Rechtssicherheit als Anreiz	174
(4) Rückschlüsse für die Auslegung der Rechtsfolgen der Einhaltung von Verhaltensregeln	174
(5) Eine Beschränkung der Allgemeingültigkeitserklärung nach Art. 40 Abs. 9 DS-GVO	174
4. Zusammenfassung der Beobachtungen	175
E. Schlussfolgerungen	177
<i>I. Schlussfolgerungen für die Auslegung des Art. 40 DS-GVO</i>	178
1. Die Rechtsfolge der Einhaltung nach Art. 40 Abs. 5 DS-GVO genehmigter Verhaltensregeln	178
a) Bindungs- und Vermutungswirkung der Genehmigung für die Aufsichtsbehörde	178
aa) Bindungswirkung	178
bb) Vermutungswirkung	179
cc) Berücksichtigungspflicht und Einordnung als Verwaltungsakt mit Gültigkeitserklärung	180
b) Einordnung der Ansichten unter Einbezug der bisher genehmigten Verhaltensregeln	181
aa) Der Wortlaut der Verweisnormen vor dem Hintergrund der praktischen Umsetzung	181
(1) Das beschränkte Konkretisierungspotential der Verweisnormen	182
(2) Ablehnung einer umfassenden Nachweisfunktion der Verhaltensregeln	183
bb) Die Bedeutung der Verweisnormen	184
cc) Schwierigkeiten bei der verwaltungsverfahrensrechtlichen Einordnung der Genehmigung	185
c) Der Vertrauensschutz als Europäischer Rechtsgrundsatz	187
aa) Vertrauensschutz im Rahmen der Ausübung europäischen Rechts am Beispiel der Leitlinien und Empfehlungen der ESA	187

(1) Zurechenbare Vertrauenslage	188
(2) Schutzwürdiges Vertrauen	188
(3) Grenzen des Vertrauensschutzes	189
(4) Der Grundsatz des Vertrauensschutzes bei der Genehmigung transnationaler Verhaltensregeln	189
bb) Vorschlag zur Ermittlung und Abstufung der Bindungswirkung .	191
cc) Betrachtung der hier vertretenen Ansicht vor dem Hintergrund der Erkenntnisse zur regulierten Selbstregulierung	193
2. Schlussfolgerungen bezüglich der Rechtsfolge der Allgemeingültigkeitserklärung nach Art. 40 Abs. 9 DS-GVO	193
a) Die Ansichten zur Allgemeingültigkeitserklärung nach Art. 40 Abs. 9 DS-GVO	194
aa) Territoriale Erweiterung der Genehmigungswirkung	194
bb) Ablehnung der lediglich territorialen Erweiterung der Genehmigungswirkung	195
cc) Verbindlichkeit der Verhaltensregeln für nationale Gerichte	196
dd) Normative Verbindlichkeit auch für andere Unternehmen, deren Tätigkeiten in den Anwendungsbereich der Verhaltensregeln fallen.	196
b) Zum Wortlautargument und zur Rechtsnatur der Durchführungsrechtsakte	197
c) Einordnung der Ansichten vor dem Hintergrund der praktischen Umsetzung der Verhaltensregeln	197
aa) Inhalte und Differenzen in der Konkretisierungsdichte der Verhaltensregeln	197
bb) Die Konkretisierung im Kontext einer normativen Wirkung der Erklärung nach Art. 40 Abs. 9 DS-GVO	198
(1) Die Auswirkungen obligatorischer und fakultativer Vorgaben in den Verhaltensregeln	199
(2) Unterschiede in der normativen Wirkung als Folge der allgemeinen Gültigkeit obligatorischer und fakultativer Vorgaben in den Verhaltensregeln	199
(3) Schwierigkeiten mit obligatorischen technischen Vorgaben in Verhaltensregeln	200
cc) Die Konzeption der bisher genehmigten transnationalen Verhaltensregeln	200
dd) Überschneidungen im Anwendungsbereich	201
d) Das Telos der Erklärung der allgemeinen Gültigkeit nach Art. 40 Abs. 9 DS-GVO	202
aa) Die Binnenmarktharmonisierung als mögliches Telos der allgemeinen Gültigkeit nach Art. 40 Abs. 9 DS-GVO	202
bb) Die allgemeine Gültigkeit nach Art. 40 Abs. 9 DS-GVO als Anreiz?	203
e) Hier vertretene Auffassung: Wahlrecht der Kommission	204

aa) Die Beschränkung der normativen Wirkung durch eine einschränkende Ausgestaltung des Durchführungsrechtsakts seitens der Kommission	204
bb) Die Beschränkung des Gegenstands der Allgemeingültigkeitserklärung	206
cc) Die normative Wirkung der Allgemeingültigkeitserklärung nach Art. 40 Abs. 9 DS-GVO	206
dd) Aus der Natur des Durchführungsrechtsakts abgeleitete Voraussetzungen für die Allgemeingültigkeitserklärung	207
(1) Die Notwendigkeit einheitlicher Bedingungen für die Durchführung des Basisrechtsaktes	207
(2) Keine Ergänzung oder Änderung des Basisrechtsaktes	207
(3) Die Ziele des Basisrechtsaktes sowie die Zweckmäßigkeit und Erforderlichkeit	208
ee) Zusammenfassung	210
<i>II. Rechtspolitische Bewertung des Art. 40f. DS-GVO</i>	<i>210</i>
1. Rechtspolitische Bewertung am Maßstab des Konzepts der Regulierten Selbstregulierung	210
a) Verhaltensregeln als Möglichkeit zur „flexiblen Regulierung“	211
b) Die Entlastung der Aufsichtsbehörden	212
c) Die Anreizgestaltung	212
2. Rechtspolitische Bewertung am Maßstab der Regulierungsziele der DS-GVO	213
a) Schutz der Grundrechte und Grundfreiheiten	214
b) Binnenmarktharmonisierung	215
c) Zusammenfassung	215
<i>III. Erkenntnisse zum Konzept der Regulierten Selbstregulierung</i>	<i>215</i>
1. Unsicherheiten bei der Normauslegung	215
2. Die Verfahrensgestaltung	216
3. Rechtsgebietspezifische Grenzen der Regulierten Selbstregulierung	217
 F. Fazit und Ausblick	 219
 Literaturverzeichnis	 223
Register	233

A. Einleitung: Objekt und Verlauf der Untersuchung

Die von Unternehmensverbänden erstellten Verhaltensregeln fristeten seit ihrer erstmaligen Einführung in Art. 27 DS-RL¹ im Datenschutzrecht für lange Zeit ein Schattendasein. Obwohl sie Ausdruck des mittlerweile etablierten² Regulierungskonzepts der Regulierten Selbstregulierung sind, mit welchem vielerlei Erwartungen verbunden werden, kam ihnen in der Praxis wie auch in der Rechtswissenschaft kaum Aufmerksamkeit zu. Im neuen Gewand des Art. 40 DS-GVO stoßen die Verhaltensregeln nun erstmalig auf breites Interesse. Das Inkrafttreten der DS-GVO mit ihrem hohen Anteil an konkretisierungsbedürftigen Normen und den neu gesetzten Anreizen für genehmigte Verhaltensregeln scheint hier einen Wandel eingeleitet zu haben. Mindestens 16 Verhaltensregeln wurden seitdem durch die nationalen Datenschutzaufsichtsbehörden nach Art. 40 Abs. 5 DS-GVO genehmigt.³ Dennoch ist ihr Erfolg alles andere als gewiss. Noch gibt es nur wenige Fälle, in denen die Verhaltensregeln eine breite Abdeckung ihres Sektors erreichen konnten.⁴ Auch wurden noch keine Verhaltensregeln durch die Europäische Kommission mittels Durchführungsrechtsakt für allgemein gültig erklärt, wie es Art. 40 Abs. 9 DS-GVO ermöglicht. Unsicherheiten im Umgang mit den Verhaltensregeln bleiben bestehen. Dies gilt insbesondere für die Rechtsfolgen der Genehmigung und der Allgemeingültigkeitserklärung.

Ziel dieser Arbeit ist es daher zum einen, diesen Unsicherheiten durch den Vorschlag einer an der Rechtspraxis orientierten Auslegung zu begegnen. Zum anderen wird hierbei auf das Regulierungskonzept der Regulierten Selbstregulierung eingegangen, dessen Umsetzung in Art. 40 DS-GVO untersucht wird. Der praktische Vergleich mit Beispielen aus anderen Rechtsgebieten⁵ ist dabei in zweierlei Hinsicht Teil

¹ Die als Datenschutzrichtlinie (DS-RL) bezeichnete Richtlinie 95/46/EG, ABl. L 281 v. 23.11.1995, S. 31, trat am 13.12.1995 in Kraft und wurde am 25.05.2018 mit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO), Verordnung (EU) 2016/679, ABl. L 119, 4.05.2016, S. 1, ersetzt.

² Das Konzept der Regulierten Selbstregulierung wurde bereits im Jahr 1996 auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer unter dem Titel „Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung“ erörtert. Hierzu sei auf die Beiträge von *Schmidt-Preuß* und *Di Fabio* verwiesen, *M. Schmidt-Preuß*, VVDStRL 56 (1997), 160; *U. Di Fabio*, VVDStRL 57 (1997), 235.

³ Siehe C. für eine Darstellung einiger der bisher nach Art. 40 Abs. 5 DS-GVO genehmigten Verhaltensregeln.

⁴ Siehe C.XVI.5.

⁵ Siehe dazu D.IV.

des hier angestrebten Ziels. Zuvorderst dient er als Kontrastpunkt für die Untersuchung und Basis einer rechtspolitischen Bewertung des Art. 40 DS-GVO. Darüber hinaus lassen sich jedoch auch einige der im Rahmen der Untersuchung erlangten Erkenntnisse für zukünftige Umsetzungen des Konzepts nutzbar machen. Diese drei miteinander verknüpften Zwecke gewähren im Zusammenspiel Einblick in die Funktionsweise des Art. 40 DS-GVO im Speziellen und der Regulierten Selbstregulierung im Allgemeinen. Hierin liegt das übergreifende Ziel der Arbeit. Der von einem fokussierten Untersuchungsrahmen ausgehende Ansatz sowie die mittlerweile zunehmende Zahl der nach Art. 40 Abs. 5 DS-GVO genehmigten Verhaltensregeln ermöglichen es, die rechtstatsächlichen Umstände umfassender zu würdigen, als dies bereits vorherige Untersuchungen der Regulierten Selbstregulierung im Datenschutzrecht vermochten.⁶

Die Arbeit unterteilt sich dabei in vier Abschnitte. Ausgehend vom normativen Rahmen des Art. 40 DS-GVO werden die noch offenen Auslegungsfragen im ersten Abschnitt [B.] herausgearbeitet und unter Zuhilfenahme des juristischen Auslegungskanons betrachtet. Hierbei zeigt sich, dass weder der Wortlaut, die Systematik noch die Entstehungsgeschichte der DS-GVO die aufgeworfenen Fragen allein zu beantworten vermögen [B.IV.3.]. Ein Auslegungsvorschlag kann jedoch auf das Telos des Art. 40 DS-GVO gestützt werden. Hierzu ist es notwendig, zuvor die praktische Umsetzung und die konzeptionellen Grundlagen der Verhaltensregeln zu betrachten.

Der folgende zweite Abschnitt [C.] untersucht daher die zum jetzigen Zeitpunkt bereits genehmigten Verhaltensregeln. Hier zeigen sich verallgemeinerungsfähige Eigenschaften wie auch konzeptionelle Unterschiede und nationale Besonderheiten [C.XVI.]. Gemeinhin wird deutlich, dass die Verhaltensregeln mit Hinblick auf ihre Konkretisierungsleistung sehr divers ausgestaltet sind. Ein besonderes Augenmerk ist darüber hinaus auf die Beweggründe der Verbände und Unternehmen zu legen. Diese setzen Art. 40 DS-GVO durch die Vorlage von sowie die Unterwerfung unter Verhaltensregeln um und bestimmen somit maßgeblich über den Erfolg der Norm [C.XVI.2.].

Aus der isolierten Betrachtung der Umsetzung datenschutzrechtlicher Verhaltensregeln in der Praxis können bereits erste Schlüsse gezogen werden. Diese formen sich allerdings erst vor dem Hintergrund des abstrakten Wissens um die Regulierungsziele der DS-GVO [D.II.] sowie des in Art. 40 DS-GVO zum Tragen kommenden Regulierungskonzept der Regulierten Selbstregulierung [D.III.3.] zu einem abgerundeten Bild. Die Regulierte Selbstregulierung wird hierzu im dritten Abschnitt [D.] im

⁶ Zu verweisen ist hier insbesondere auf die Dissertationsschriften von *Verena Stürmer* (Regulierte Selbstregulierung im europäischen Datenschutzrecht, 2022), welche die Umsetzung dieses Regulierungskonzeptes in der DS-GVO unter besonderer Berücksichtigung des Accountability-Grundsatzes umfassend untersuchte, sowie von *Zoi Talidou* (Regulierte Selbstregulierung im Bereich des Datenschutzes, 2005), die (wohl erstmals) die Umsetzung in der nunmehr von der DS-GVO abgelösten DS-RL herausarbeitete.

weiteren Kontext der Regulierungskonzepte dargestellt. Durch den am Ende des Abschnitts vollzogenen Vergleich mit anderen Instrumenten der (Regulierten) Selbstregulierung [D.IV.] lassen sich zum einen die Ausgestaltungsentscheidungen des (Unions-)Gesetzgebers bei der Normierung des Art. 40 DS-GVO mit denen in anderen Rechtsgebieten abgleichen, um Erkenntnisse bezüglich des Telos der Norm zu gewinnen. Zum anderen lassen sich Rückschlüsse auf die übergreifende Funktionslogik der Konzepte ziehen, deren Nutzen sich auch in anderen Rechtsgebieten niederschlagen kann [D.IV.4.].

Im vierten Teil der Arbeit [E.] wird auf Grundlage dieser Erkenntnisse eine Auslegung des Art. 40 DS-GVO vorgeschlagen, die zwischen der Rechtsfolge der Einhaltung von genehmigten und von allgemein gültigen Verhaltensregeln unterscheidet [E.I.]. Hinsichtlich der genehmigten Verhaltensregeln sind vorwiegend nicht die nationalen Vorgaben zum Verwaltungsverfahren heranzuziehen, sondern vielmehr ist der Europäische Grundsatz des Vertrauensschutzes mit der inhaltlichen Diversität der Verhaltensregeln in der Praxis in Einklang zu bringen [E.I.1.c)].

Daraus folgt keine „Immunität“ der den Verhaltensregeln beigetretenen Unternehmen gegenüber aufsichtsbehördlichen Maßnahmen im Sinne eines umfassenden und abschließenden Nachweises der DS-GVO-Konformität. Dies wäre mit der Zielrichtung und Ausgestaltung der Verhaltensregeln in der Praxis nicht vereinbar, welche, trotz ihrer sektorspezifischen Konkretisierung, nicht den Anspruch haben (können), die datenschutzrechtlichen Pflichten der DS-GVO für die Vielzahl von Verarbeitungsvorgängen personenbezogener Daten durch die ihnen unterworfenen Unternehmen abschließend zu konkretisieren. Verhaltensregeln enthalten somit zwar regelmäßig wenige für den einzelnen Verarbeitungsvorgang spezifizierten Vorgaben, bieten aber – etwa indem sie geeignete technisch-organisatorische Maßnahmen im Rahmen des Art. 32 Abs. 1 DS-GVO aufzählen – eine durch die Aufsichtsbehörde genehmigte Konkretisierungsstufe zwischen der DS-GVO und dem jeweiligen Datenverarbeitungsvorgang [E.I.1.b)aa)].

Der Grundsatz des Vertrauensschutzes erfordert von Seiten der Aufsichtsbehörden eine einzelfallbezogene Prüfung, ob und wieweit sie bei Maßnahmen gegenüber den Verantwortlichen durch ihre vorherige Genehmigung der Verhaltensregeln an diese Konkretisierung gebunden sind. Eine solche Prüfung wird nur im Ausnahmefall dazu führen, dass der Aufsichtsbehörde Maßnahmen gegen datenschutzrechtlich Verantwortliche, die sich den Verhaltensregeln unterworfen haben, gänzlich verwehrt bleiben. Zur Ermittlung der Reichweite des von der Genehmigung der Verhaltensregeln ausgehenden Vertrauensschutzes wird ein sechsgliedriges Prüfungsschema vorgeschlagen [E.I.1.c)bb)].

Auch bezüglich der Rechtsfolge der als Durchführungsrechtsakt ausgestalteten Allgemeingültigkeitserklärung nach Art. 40 Abs. 9 DS-GVO wird ein differenzierter Ansatz verfolgt. Die Allgemeingültigkeit erschöpft sich dabei nicht in einer lediglich territorialen Erweiterung der Genehmigungsfolgen auf die europäischen Mitgliedstaaten, welche nach hier vertretener Ansicht bereits durch das nach Art. 40 Abs. 7

DS-GVO vor der Genehmigung transnationaler Verhaltensregeln durchzuführende Kohärenzverfahren herbeigeführt wird [E.I.1.c)aa)(4)]. Richtigerweise ist die Allgemeingültigkeitserklärung nach Art. 40 Abs. 9 DS-GVO als Mittel der Binnenmarktharmonisierung zu betrachten. Indem sie den Verhaltensregeln zu normativer Wirkung verhelfen kann, ermöglicht sie es der Europäischen Kommission, den Vollzug der DS-GVO in den Mitgliedstaaten anzugleichen und so gegebenenfalls auch Dritte, welche sich den Verhaltensregeln nicht selbst unterworfen haben, zur Einhaltung dieser zu verpflichten. Bei der Entscheidung über den Erlass und der Ausgestaltung des Durchführungsrechtsaktes hat die Kommission im Rahmen ihres Ermessensausübung zu beachten, dass die Vorgaben transnationaler Verhaltensregeln nicht in jedem Fall sinnvoll auf Dritte angewendet werden können. Faktoren wie die konzeptionelle Auslegung, die Konkretisierungsdichte oder Überschneidungen im Anwendungsbereich mehrerer Verhaltensregeln können einer Ausweitung auf Dritte mittels Allgemeingültigkeitserklärung entgegenstehen [E.I.2.c)].

Zur Ermittlung der Rechtsfolge der Allgemeingültigkeitserklärung nach Art. 40 Abs. 9 DS-GVO ist daher der Inhalt des Rechtsaktes selbst heranzuziehen und der Kommission ein Ermessen nicht nur bezüglich des Erlasses, sondern auch bei der Ausgestaltung des Durchführungsrechtsaktes einzuräumen, sodass sie die Erklärung auf einzelne Regelungen der Verhaltensregeln beschränken oder auch von einer Bindung Dritter absehen kann [E.I.2.e)]. Die Grenzen dieses Ermessens sind aus der Durchführungsbefugnis der Kommission herzuleiten und stehen einer Allgemeingültigkeitserklärung insbesondere dann entgegen, wenn die Verhaltensregeln inhaltlich über eine Konkretisierung der DS-GVO hinausgehen [E.I.2.e)dd)].

Weitergehend werden die Untersuchungsergebnisse sowohl mit den erhofften Vorteilen des Regulierungskonzeptes der Regulierten Selbstregulierung wie auch mit den Regulierungszielen der DS-GVO kontrastiert [E.II.]. Hierbei wird bezüglich der erhofften Vorteile deutlich, dass die Verhaltensregeln zwar eine – wenn auch durch die Verfahrenskomplexität beschränkte – Flexibilität der Konkretisierung ermöglichen, die angestrebte Entlastung der Aufsichtsbehörden jedoch zumindest nicht kurzfristig eintreten wird. Die laufenden Genehmigungsverfahren binden – auch aufgrund der erforderlichen Koordinierungsleistung – in erheblichem Umfang aufsichtsbehördliche Ressourcen. Mit einer entlastenden Wirkung ist erst zu rechnen, sobald sich die Verhaltensregeln und ihre Kontrollstellen nach Art. 41 Abs. 1 DS-GVO etabliert haben und die Aufsichtsbehörden sich von ihrer Funktion derart überzeugen konnten, dass sie die Intensität eigener Überwachungstätigkeiten in einem gewissen Umfang zurückfahren können.

Wie sich der Beitrag der Verhaltensregeln zur Umsetzung der Ziele der DS-GVO entwickelt, kann nur bedingt prognostiziert werden. Zu der Etablierung eines einheitlichen Schutzniveaus dürften die Verhaltensregeln, gleich ob rein national oder transnational, bereits jetzt beitragen [E.II.2.a)]. Ob Gleiches auch für die Förderung der Vollzugsharmonisierung durch transnationale Verhaltensregeln gilt, kann aufgrund der gegenwärtig wenigen genehmigten transnationalen Verhaltensregeln nicht

beurteilt werden. [E.II.2.b)]. Lehren für zukünftige Umsetzungen der Regulierten Selbstregulierung durch den (Unions-)Gesetzgeber ergeben sich insbesondere bei den Auswirkungen rechtlicher Unsicherheiten [E.III.1.] und komplexer Verfahrensgestaltung [E.III.2.] auf die für eine erfolgreiche Umsetzung essenzielle Anreizwirkung. Hier zeigt sich, dass ein höheres Maß an gesetzlicher Determinierung bezüglich der Voraussetzungen, Verfahren und Rechtsfolgen der Mechanismen der Regulierten Selbstregulierung den Umsetzungsaufwand für Private wie auch Aufsichtsbehörden deutlich verringert. Dass die Verfahren der Regulierten Selbstregulierung ein hohes Maß an Komplexität aufweisen, lässt sich dagegen nicht vollends verhindern. Die dem Konzept entspringende Notwendigkeit, alle betroffene Akteure miteinzubeziehen, steht dem entgegen. Möglichkeiten zum Abgleich, zur Bündelung und zur gemeinsamen Repräsentation von Interessen sollten jedoch nicht nur von den beteiligten Privaten, sondern auch von Aufsichtsbehörden hinsichtlich ihrer Rechtsansichten, frühzeitig genutzt werden. Zuletzt ist auch die Bedeutung rechtsgebietspezifischer Grenzen für die Umsetzungsmöglichkeiten des Regulierungskonzepts hervorzuheben [E.III.3.]. So ergeben sich etwa im Datenschutzrecht Einschränkungen bei der Entlastung der Aufsichtsbehörden, deren Zuständigkeit nicht durch einen Verweis auf Selbstkontrollenrichtungen zurückgestellt werden kann [C.XVI.3.b)bb)].

Ein abschließender Überblick über die Untersuchungsergebnisse, offen gebliebene Fragen sowie ein Ausblick auf zukünftige Forschungspotentiale finden sich im Fazit [F.]

B. Verfahren und Rechtsfolgen des Art. 40 DS-GVO im Überblick

Die in Art. 40f. DS-GVO normierten Verfahren [B.I.], Voraussetzungen [B.II.] und Rechtsfolgen [B.III.] sind gleichzeitig Ausgangspunkt und Gegenstand der vorliegenden Untersuchung. Sie sollen hier in ihren Grundzügen dargestellt werden.¹ Hingewiesen wird dabei auf die noch umstrittenen Auslegungsfragen.

I. Verfahren

Art. 40 DS-GVO unterscheidet zwischen den Verfahren der Genehmigung nationaler [B.I.4.] sowie transnationaler Verhaltensregeln [B.I.5.]. Transnationale Verhaltensregeln können darüber hinaus durch die Europäische Kommission nach Art. 40 Abs. 9 DS-GVO für allgemein gültig erklärt werden [B.I.6.]. Einheitlich ausgestaltet sind die Vorgaben bezüglich der vorlageberechtigten Stellen [B.I.1.], des Vorabverfahrens und der Konsultationen [B.I.2.] sowie über die zuständige Aufsichtsbehörde [B.I.3.].

1. Vorlageberechtigte Stellen

Dem Wortlaut des Art. 40 Abs. 2 DS-GVO nach dürfen nur solche Verbände und Vereinigungen Verhaltensregeln vorlegen, welche Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten. Der *EDSA*² leitet daraus ab, dass die Verbände und Vereinigungen ihre Vorlageberechtigung gegenüber der zuständigen Aufsichtsbehörde nachweisen müssen, indem sie darlegen, dass sie die Verarbeitungstätigkeit und die daraus entstehenden Bedürfnisse ihrer Mitglieder verstehen und ihre Ver-

¹ Im Detail lässt sich insbesondere der Verfahrensablauf den Leitlinien des *EDSA* entnehmen, *Europäischer Datenschutzausschuss*, 04.06.2019, Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679, Rn. 12f., online abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_de.pdf, zuletzt geprüft am 16.01.2024.

² Der Europäische Datenschutzausschuss (*EDSA*) setzt sich als unabhängiges Gremium aus den nationalen Datenschutzbehörden der Länder des Europäischen Wirtschaftsraums sowie dem Europäischen Datenschutzbeauftragten zusammen. Deutschland wird hier gem. § 17 BDSG durch den Bundesdatenschutzbeauftragten vertreten.

haltensregeln entsprechend ausarbeiten können.³ Maßgebliche Kriterien für diese Feststellung sind die absolute Anzahl der potenziell von den vorgelegten Verhaltensregeln betroffenen Mitglieder oder ihr prozentualer Anteil im betreffenden Sektor sowie die Erfahrung der vorlegenden Stelle in Bezug auf die vom jeweiligen Sektor abgedeckten Verarbeitungstätigkeiten.⁴ Konzerne oder einzelne Unternehmen sind nicht vorlageberechtigt, da dies kleine und mittlere Unternehmen von der Mitwirkung bei der Erstellung von Verhaltensregeln ausschließen könnte.⁵

2. Vorabverfahren und Konsultationen nach EG 99 DS-GVO

Da nachträgliche Änderungen der vorgelegten Verhaltensregeln im eigentlichen Genehmigungsverfahren entsprechend der Leitlinien des *EDSA* nicht mehr vorgesehen sind, muss die Abstimmung mit der zuständigen Aufsichtsbehörde bereits vor dem Beginn des eigentlichen Genehmigungsverfahrens erfolgen. In diesem Zeitraum ist demnach die entscheidende Abstimmungsarbeit mit den Behörden und den nach Erwägungsgrund 99 maßgeblichen Interessenträgern zu leisten. EG 99 besagt: „Bei der Ausarbeitung [...] solcher Verhaltensregeln sollten Verbände [...] die maßgeblichen Interessenträger, möglichst auch die betroffenen Personen, konsultieren und die Eingaben und Stellungnahmen, die sie dabei erhalten, berücksichtigen.“ Obwohl die Konsultationen nach EG 99 entsprechend der Formulierung „sollen“ nicht zwingend sind, so werden sie vom *EDSA* jedoch „dringend empfohlen“⁶ und ein Nachweis über Art und Umfang wird seitens der Aufsichtsbehörden als Zulässigkeitskriterium für eine inhaltliche Prüfung der Verhaltensregeln vorausgesetzt.⁷ Sollten Konsultationen nicht stattgefunden haben, so wird seitens der Aufsichtsbehörden verlangt, dass die Gründe hierfür dargelegt werden.⁸ In der Regel dürfte die vorlegende Stelle auch jenseits des Genehmigungsverfahrens ein eigenes Interesse an der Einbeziehung betroffener Interessenträger haben, da sie nur so eine breite Akzeptanz ihrer Verhaltensregeln erwarten kann.

³ *Europäischer Datenschutzausschuss*, 04.06.2019, Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679, Rn. 21 f. (online abrufbar, siehe Abschnitt B, Fn. 1).

⁴ *Europäischer Datenschutzausschuss*, 04.06.2019, Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679, Rn. 22 (online abrufbar, siehe Abschnitt B, Fn. 1).

⁵ *M. Vomhof*, in: Eßer/Kramer/Lewinski (Hrsg.), Auernhammer DS-GVO/BDSG, Art. 40 DS-GVO, Rn. 13; a. A. *M. Bergt/P. Pesch*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 40 DS-GVO, Rn. 13.

⁶ *Europäischer Datenschutzausschuss*, 04.06.2019, Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679, Rn. 28 (online abrufbar, siehe Abschnitt B, Fn. 1).

⁷ Die vollständigen Zulässigkeitsvoraussetzungen finden sich auf S. 12–15 der Leitlinien.

⁸ *Europäischer Datenschutzausschuss*, 04.06.2019, Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679, Rn. 28 (online abrufbar, siehe Abschnitt B, Fn. 1).

3. Zuständige Aufsichtsbehörde

Die Verhaltensregeln sind gem. Art. 40 Abs. 5 DS-GVO bei der nach Art. 55 DS-GVO zuständigen Aufsichtsbehörde vorzulegen. Zuständig ist demnach jene Aufsichtsbehörde, in deren örtlichen Zuständigkeitsbereich zumindest ein Teil der Datenverarbeitungen fallen, welche von den Verhaltensregeln umfasst werden. Bei der Vorlage transnationaler Verhaltensregeln wird es regelmäßig vorkommen, dass mehrere Aufsichtsbehörden zuständig sind. Der vorlegenden Stelle steht es in diesem Fall frei, unter den zuständigen Aufsichtsbehörden eine Auswahl zu treffen.⁹ Diese angerufene Aufsichtsbehörde¹⁰ informiert alle weiteren Aufsichtsbehörden über die Vorlage.

4. Genehmigungsverfahren bei nationalen Verhaltensregeln

In Deutschland ist aufgrund der föderalen Struktur der Datenschutzaufsicht zu beachten, dass alle Genehmigungsverfahren in der *Datenschutzkonferenz*¹¹ abgestimmt werden und vor der Genehmigung ein Umlaufverfahren stattfindet, in welchem alle föderalen Aufsichtsbehörden um Zustimmung gebeten werden.¹² Die Zuständigkeit innerhalb Deutschlands bestimmt sich nach dem Sitz des Inhabers der Verhaltensregeln.¹³

Mit Blick auf den missverständlichen Wortlaut des Art. 40 Abs. 5 S. 2 DS-GVO ist unklar, wie genau das Verfahren auf nationaler Ebene auszugestalten ist. Insbesondere das Verhältnis von Stellungnahme und Genehmigung ist umstritten. Im Wesentlichen lassen sich hier zwei verschiedene Interpretationsansätze nachvollziehen, die sich jeweils in drei Punkten unterscheiden. Erstens bei der Frage, ob die Stellungnahme und die Genehmigung einen einheitlichen Rechtsakt darstellen. Zweitens, sofern man von zwei verschiedenen Rechtsakten ausgeht, ob diese unterschiedlichen Prüfungsvoraussetzungen unterliegen und drittens, ob die in Art. 40 Abs. 5 S. 2 DS-GVO

⁹ Auf Art. 56 Abs. 1 DS-GVO wird nicht verwiesen, sodass das Prinzip der federführenden Aufsichtsbehörde hier nicht anwendbar ist. Der EDSA hat jedoch unverbindliche Kriterien für die Auswahl in Anhang 2 seiner Leitlinien veröffentlicht: *Europäischer Datenschutzausschuss*, 04.06.2019, Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679, Anhang 2 (online abrufbar, siehe Abschnitt B, Fn. 1).

¹⁰ Die Formulierung „angerufene Aufsichtsbehörde“ wird nachfolgend verwendet, um die Aufsichtsbehörde zu bezeichnen, bei welcher der Antrag auf Genehmigung der Verhaltensregeln gestellt wurde.

¹¹ Ehemals Düsseldorf Kreis.

¹² Hierbei ist davon auszugehen, dass im Düsseldorf Kreis etablierte – gesetzlich nicht vorgeschriebene – Abstimmungsverfahren auch in der Datenschutzkonferenz beibehalten wird. Erstmals wurde diese Abstimmung bei einem Art. 40 DS-GVO-Genehmigungsverfahren bzgl. der Verhaltensregeln der Wirtschaftsauskunfteien durchgeführt: *Düsseldorf Kreis*, 28.02./01.03.2018, Protokoll der Sitzung am 28. Februar/1. März 2018, S. 4f.

¹³ M. Vomhof, in: Eßer/Kramer/Lewinski (Hrsg.), Auernhammer DS-GVO/BDSG, Art. 40 DS-GVO, Rn. 37.

gewählte Formulierung der „ausreichend geeigneten Garantien“ den „geeigneten Garantien“ in Art. 40 Abs. 3 S. 1 DS-GVO entspricht.¹⁴

Der Wortlaut des Art. 40 DS-GVO wird verschieden ausgelegt. Zum Teil wird unter Berufung auf Art. 40 Abs. 5 DS-GVO, nach welchem „Die Aufsichtsbehörde [...] eine Stellungnahme darüber ab[gibt], ob der Entwurf [...] mit dieser Verordnung vereinbar ist und [...] diesen Entwurf [...], wenn sie der Auffassung ist, dass er ausreichende geeignete Garantien bietet [genehmigt].“, davon ausgegangen, dass es sich um ein zweistufiges Verfahren handelt, bei welchem sich Stellungnahme und Genehmigung auch in ihrem Prüfungsgehalt unterscheiden.¹⁵ Während sich die zeitlich vorgelagerte Stellungnahme auf die Vereinbarkeit mit der DS-GVO beziehen soll, könne eine Genehmigung nur erteilt werden, wenn „ausreichend geeignete Garantien“ vorliegen.¹⁶ Die Formulierung in Art. 46 Abs. 2 lit. e DS-GVO, welche nur von „genehmigten Verhaltensregeln gemäß Artikel 40“ spricht, unterstützt eine Differenzierung zwischen Stellungnahme (mit Hinblick auf die Vereinbarkeit mit der DS-GVO) und Genehmigung (sofern ausreichende geeignete Garantien im Sinne des Art. 46 DS-GVO vorliegen). Das Verfahren würde daher grundsätzlich mit einer Stellungnahme enden und eine Genehmigung wäre nur notwendig, wenn die vorliegenden Stellen mit ihren Verhaltensregeln darauf abzielen, geeignete Garantien für die Datenübermittlung in Drittländer im Sinne des Art. 46 DS-GVO zu schaffen.¹⁷

Dies deckt sich jedoch nicht mit dem Wortlaut des Art. 40 Abs. 7 DS-GVO, welcher bei transnationalen Verhaltensregeln vor der Genehmigung – jedoch nicht vor der Stellungnahme – eine Vorlage an den *EDSA* voraussetzt, dessen Prüfung sich sowohl auf die Vereinbarkeit mit der DS-GVO als auch auf das Vorliegen geeigneter Garantien beziehen kann. Wenn der *EDSA* nur vor der Genehmigung angerufen werden muss, jedoch nicht vor der Stellungnahme, dann bestünde, für den Fall, dass die vorliegende Stelle keine Garantien im Rahmen des Datentransfers in Drittstaaten vorgesehen hat, kein Grund für eine Überprüfung der Verhaltensregeln auf ihre Ver-

¹⁴ Um die verschiedenen Auffassungen in ihren Details zu erfassen, empfiehlt sich ein Blick in die zitierte Literatur. Die vorliegende Darstellung wurde zwecks Übersichtlichkeit auf die wesentlichen Punkte verkürzt.

¹⁵ *M. Vomhof*, in: Eßer/Kramer/Lewinski (Hrsg.), Auernhammer DS-GVO/BDSG, Art. 40 DS-GVO, Rn. 43 ff.; *A. Roßnagel*, in: Simitis/Hornung/Spiecker (Hrsg.), NK Datenschutzrecht 2019, Art. 40 DS-GVO, Rn. 61; ähnlich auch *Schweinoch*, wobei dieser bei beiden Verfahrensschritten denselben Prüfungsmaßstab anlegt, *M. Schweinoch*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 40 DS-GVO, Rn. 42.

¹⁶ So *Roßnagel*, der auf die Widersprüchlichkeit der Formulierung ausdrücklich hinweist: *A. Roßnagel*, in: Simitis/Hornung/Spiecker (Hrsg.), NK Datenschutzrecht 2019, Art. 40 DS-GVO, Rn. 61 ff.

¹⁷ Eine Genehmigung allein reicht hierfür, entgegen dem Wortlaut des Art. 46 Abs. 2 lit. e DS-GVO, jedoch nicht aus. Art. 40 Abs. 3 DS-GVO verlangt vielmehr auch nach einer allgemeinen Gültigkeit der Verhaltensregeln, welche durch die Kommission erteilt werden kann und nur für transnationale Verhaltensregeln möglich ist, vgl. Art. 40 Abs. 8 DS-GVO. So auch *Europäischer Datenschutzausschuss*, 07.07.2021, Guidelines 04/2021 on codes of conduct as tools for transfers, Rn. 21, online abrufbar unter: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_de, zuletzt geprüft am 16.01.2024.

Register

- Accounting-Standards *siehe* Rechnungslegungsstandards
- Akkreditierte Überwachungsstellen 18 ff., 83
- Kosten 96 f.
 - Verfahrensdauer 95 f.
- Allgemeingültigkeit 24 ff., 31–37, 160, 174 f., 193–210
- Beschränkung 206
 - Datentransfer in Drittländer 139
 - Erklärung 24 ff.
 - Telos 160
 - Voraussetzungen 207 ff.
 - Rechtsfolge 31–37, 174 f., 193–210
- Anreize 89–98, 123 f., 131 ff., 140 f., 144 f.
- Außendarstellung 90
 - Bedeutung 30, 123 f.
 - finanzielle 132 f.
 - im Rahmen der Selbstregulierung 125
 - Kosten 96 f., 131, 144, 150
 - negative Anreize 94, 131, 173
 - Rechtssicherheit 89, 171–174
 - staatlich gesetzte Anreize 124, 131 ff., 138, 212 f.
 - Wettbewerbsvorteil 94
- Aufsichtsbehörde 9, 21 ff.
- Entlastung 212
 - Zuständigkeit 9
- Auftragsverarbeitung 61, 75–84
- Bindungswirkung *siehe* Genehmigung
- Binnenmarktharmonisierung *siehe* Regulierungsziele
- Cloud-Dienste 79–84
- Codes of Conduct *siehe* Verhaltensregeln
- Datenschutzkonferenz 9
- Datenschutzrichtlinie 28 f., 32 f.
- Delegierte Rechtsakte 33
- Durchführungsrechtsakte 16, 33–37, 204–210
- DVTM-Kodex 162–165
- Entstehungsgeschichte *siehe* Genehmigung
- Erklärung der allgemeinen Gültigkeit *siehe* Allgemeingültigkeit
- Europäische Kommission 16, 204
- Europäischer Datenschutzausschuss 14 f., 23 f.
- Stellungnahme 14, 23
 - Streitbeilegungsverfahren 15
 - Verbindlicher Beschluss 14, 24
- Europäischer Gerichtshof 34–37, 72
- Expertenrecht 157
- Feststellender Verwaltungsakte *siehe* Verwaltungsakt
- Freistellungsmöglichkeit 171
- Genehmigung 21 ff., 26–31
- Bindungswirkung 26–31, 178 f.
 - Entstehungsgeschichte 11 f.
 - Kosten der Genehmigung 96 f.
 - Rechtsfolgen 26–31, 278
 - Verfahren bei nationalen Verhaltensregeln 9
 - Verfahren bei transnationalen Verhaltensregeln 13
 - Verfahrensdauer 95 f.
 - Vermutungswirkung 179 f.
 - Vorlageberechtigte Stellen 7
- Gewährleistungsverantwortung 133–140
- Grundrechte *siehe* Regulierungsziele
- Hoheitliche Regulierung *siehe* Regulierungskonzepte

- Informationspflichten 48, 51, 62, 67
 Informelles Verwaltungshandeln 113 f.
- Konkretisierung 86
 – Konkretisierungsdichte 87 f.
 – Konkretisierungspotentiale 182 f., 197 f.
 – Schwerpunkte 86–89
- Negative Anreize *siehe* Anreize
- Private Normsetzung 143–161
- Rechnungslegungsstandards 149–160
 Rechtssicherheit *siehe* Anreize
 Regulierte Selbstregulierung *siehe*
 Regulierungskonzepte
 Regulierungskonzepte 105–140
 – Abgrenzung 117 f.
 – hoheitliche Regulierung 106–114
 – Kritik an der Selbstregulierung
 119–123
 – Regulierte Selbstregulierung 127–140,
 193, 215–218
 – Selbstregulierung 114–126
 Regulierungsziele 103 ff.
 – Binnenmarktharmonisierung 104
 – Schutz der Grundrechte und Grund-
 freiheiten 104 f.
 – Umsetzung 145 f., 153, 164, 213 ff.
- Rezeption 151 f.
- Selbstregulierung *siehe* Regulierungs-
 konzepte
 Staatsaufgaben 110, 125 ff.
 Staatsferne 111 f.
 Steuerungswissen 108 f.
 Streitbeilegungsverfahren *siehe*
 Europäischer Datenschutzausschuss
- Trittbrettfahrereffekte 120
- Überwachungsstelle *siehe* Akkreditierte
 Überwachungsstelle
 Umweltrechtliche Selbstverpflichtungen
 143–148
 Unternehmensverbände 100 f.
- Verfahrensdauer *siehe* Akkreditierte
 Überwachungsstelle; Genehmigung
 Verhaltensregeln
 – Funktion 86 f.
 – nationale Besonderheiten 98 ff.
 – transnationale 79–84
 – Wahrnehmung 101
 Vermutungswirkung *siehe* Genehmigung
 Vertrauensschutz 187–191
 Verwaltungsakt 21 f., 178–181
 – feststellender Verwaltungsakt 21 f., 26 f.,
 178 f.
 – Verwaltungsakt mit Gültigkeits-
 erklärung 180 f.
- Verweisnormen
 – Bedeutung 184 f.
 – Konkretisierungspotential 182 ff.
 – Wortlaut 181 f.
- Vollzugsdefizite 110 f.
- Vorlageberechtigte Stellen *siehe*
 Genehmigung
- Wettbewerbsregeln 166–175
 Wortlaut der DS-GVO 27 f., 32
- Zertifizierung
 – Abgrenzung von Verhaltensregeln 90–94
 – Anreize 93 f.
 – Verfahren 92 f.
- Zuständigkeit *siehe* Aufsichtsbehörde