Schriften zum Internationalen und Europäischen Strafrecht

33

Nathalie Lauer

Informationshilfe im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Nomos

Schriften zum Internationalen und
Europäischen Strafrecht

Herausgegeben von

Professor Dr. Martin Heger, Humboldt-Universität zu Berlin
Professor Dr. Florian Jeßberger, Universität Hamburg
Professor Dr. Frank Neubacher, M.A., Universität zu Köln
Professor Dr. Helmut Satzger, LMU München
Professor Dr. Gerhard Werle, Humboldt-Universität zu Berlin

Band 33

Nathalie Lauer

Informationshilfe im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Berlin, Humbold-Univ., Diss., 2017

ISBN 978-3-8487-4620-0 (Print)
ISBN 978-3-8452-8852-9 (ePDF)

1. Auflage 2018
© Nomos Verlagsgesellschaft, Baden-Baden 2018. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2017 von der Juristischen Fakultät der Humboldt-Universität zu Berlin als Dissertation angenommen. Sie ist auf dem Stand von November 2015 und enthält bereits einen Ausblick auf die nach Abschluss der Arbeit beschlossene EU-Datenschutzreform. Wie im Ausblick gezeigt wird, kann diese Reform nur ein Schritt auf dem Weg der Europäischen Union, die erforderliche Balance zwischen der Erleichterung und Effektivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen einerseits und dem Grundrecht auf Datenschutz andererseits herzustellen, sein.

Diese Arbeit wäre ohne meinen viel zu früh verstorbenen Doktorvater, Herrn Professor Dr. Joachim Vogel, nicht entstanden. An seinem Lehrstuhl in Tübingen habe ich als Studentin die Freude am wissenschaftlichen Arbeiten und insbesondere am Europäischen Strafrecht entdeckt. Nach Joachim Vogels tragischem Tod hat Herr Professor Dr. Martin Heger ohne zu Zögern die Betreuung dieser Arbeit übernommen. Er hat mir den erforderlichen akademischen Freiraum bei der Fertigstellung der Arbeit eingeräumt und mich zu jeder Zeit in allen fachlichen und organisatorischen Belangen unterstützt. Ich bin ihm zutiefst dankbar. Ich danke auch Herrn Professor Dr. Tobias Reinbacher für die zügige Erstellung des Zweitgutachtens. Den Herausgebern der Schriftenreihe zum Internationalen und Europäischen Strafrecht möchte ich für die Aufnahme dieser Arbeit in die Schriftenreihe danken.

In den Jahren, in denen diese Arbeit entstanden ist, haben mich meine Familie, Freunde und Kollegen begleitet, denen ich von Herzen für Ihre Anregungen, sowie die kleinen und großen Gesten persönlichen und fachlichen Beistands danken möchte. Stellvertretend für all diese lieben Menschen seien hier Dr. Dominik Brodowski, LL.M. (UPenn), Karen Häußer, Dr. Ali B. Norouzi und Isabelle Yusuf genannt. Last but not least danke ich meinem Ehemann Dr. Mischa Lauer für seine bedingungslose Unterstützung und den Glauben an mich in allen Lebenslagen.

Luxemburg, im Januar 2018 *Nathalie Lauer*

Inhaltsverzeichnis

Einleitung 19

Erster Teil: Anforderungen an das System der Informationshilfe in der Europäischen Union 27

A. Erforderlichkeit eines effektiven Instruments betreffend die Übermittlung und den Austausch von Informationen 27

B. Das Gebot der Kohärenz 33

I. Innere Kohärenz 34

1. Insbesondere polizeiliche und justizielle Zusammenarbeit in Strafsachen – Kapitel 4 und 5 AEUV 34

2. Sonstige Politikbereiche der Europäischen Union 37

II. Äußere Kohärenz 38

III. Vertikale Kohärenz 40

IV. Zusammenfassung 40

C. Internationale Grund- und Menschenrechte, insbesondere das Recht auf Datenschutz 40

I. EU-Grundrechte 42

1. Art. 6 EUV i.V.m. Art. 8 GRC 43

a) Geltung von Art. 8 GRC im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen 43

aa) Enger Anwendungsbereich von Art. 8 GRC 43

bb) Eingeschränkter Anwendungsbereich von Art. 8 GRC je nach Zeitpunkt des Inkrafttretens der jeweiligen Maßnahme 44

cc) Weiter Anwendungsbereich von Art. 8 GRC 45

dd) Zwischenergebnis 48

b) Sachlicher und persönlicher Anwendungsbereich 48

c) Regelungsgehalt von Art. 8 GRC 50

aa) Vorfrage: Verhältnis zu Art. 16 AEUV 51

bb) Verhältnis zu Art. 8 EMRK 53

cc) Ausgangspunkt: Recht auf Schutz personenbezogener Daten, Art. 8 Abs. 1 GRC 56

dd) Beteiligung des Betroffenen 56
(1) Auskunft und Information 56
(2) Berichtigung unrichtiger personenbezogener Daten 58
(3) Sonstige positive Rechte 59
ee) Kontrolle 60
ff) Rechtfertigungsbedürftigkeit von Eingriffen und Beeinträchtigungen 64
gg) Rechtfertigung von Eingriffen und Beeinträchtigungen 66
(1) Gesetzesvorbehalt 67
(2) Zweckbindung 68
(3) Treu und Glauben 70
(4) Schranken-Schranken, Art. 52 Abs. 1 Satz 1 und Satz 2 GRC 71
(a) Verhältnismäßigkeitsgrundsatz 71
(b) Wesensgehaltsgarantie 75
d) Sekundärrecht im Bereich des Grundrechts auf Datenschutz 76
aa) Zum Verhältnis zwischen EG-Datenschutzrichtlinie und Art. 8 GRC 76
bb) Garantien der EG-Datenschutzrichtlinie 78
cc) Sonstige Regelungen 81
2. Art. 16 AEUV 81
3. Art. 6 EUV i.V.m. Art. 7 GRC 82
4. Art. 6 EUV i.V.m. Art. 47 GRC 84
II. Die Europäische Menschenrechtskonvention 85
1. Insbesondere Art. 8 EMRK 87
2. Art. 13 EMRK 92
III. Sonstiges internationales Recht, insbesondere Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten 94
IV. Zusammenfassung 98

D. Sonstige Anforderungen, insbesondere technischer und organisatorischer Art 100

Zweiter Teil: Die Instrumente für einen Informationsaustausch im Rahmen der polizeilichen und der justiziellen Zusammenarbeit in Strafsachen 102

A. Die einzelnen Instrumente 102
I. Der Rahmenbeschluss schwedische Initiative 102
1. Gesetzgebungsverfahren 102
2. Anwendungsbereich 103
a) Situation und handelnde Behörden 103
aa) Strafrechtliche Ermittlungen und polizeiliche Erkenntnisgewinnungsverfahren 103
bb) Strafverfolgungsbehörden 104
b) Erfasste Informationen 106
3. Regelungsgehalt 111
a) Grundsatz des gleichberechtigten Zugangs zu Informationen 111
b) Fristen für die Zurverfügungstellung der ersuchten Information 113
c) Grenzen des gleichberechtigten Zugangs – Verweigerungsgründe 116
d) Spontane Informationsübermittlung 123
e) Verwendung der übermittelten Informationen 124
f) Sonstige Informationspflichten 128
II. Prümer Vertrag und Prümer Beschluss 129
1. Gesetzgebungsverfahren 129
2. Anwendungsbereich 133
a) Erfasste Informationen 133
aa) Überblick 133
bb) Begriffsbestimmungen 134
(1) DNA-Profile 134
(2) Daktyloskopische Daten 135
(3) Offene Spuren 136
(4) Daten aus den Fahrzeugregistern 136
b) Sachlicher Anwendungsbereich des Prümer Beschlusses 136
c) Fazit 142

3. Regelungsgehalt 142
a) DNA-Profile 142
aa) Errichtung und Führung von DNA-Datenbanken 142
bb) Automatisierter DNA-Profil-Abruf im Einzelfall 144
cc) Automatisierter DNA-Profil-Abgleich 146
dd) Gewinnung von DNA-Profilen 147
b) Daktyloskopische Daten 148
c) Zu den Fundstellendatensätzen gehörende personenbezogene Daten 150
d) Daten aus Fahrzeugregistern 151
e) Straftatverhinderung und Gefahrenabwehr bei Großveranstaltungen mit grenzüberschreitender Dimension 152
f) Verhinderung terroristischer Straftaten 154
III. Die Richtlinie über die Europäische Ermittlungsanordnung 156
1. Gesetzgebungsverfahren 156
2. Anwendungsbereich 158
a) Sachlicher Anwendungsbereich 158
b) Gegenstand der Europäischen Ermittlungsanordnung 159
3. Regelungsgehalt 159
a) Anordnende Behörde 159
b) Voraussetzung für den Erlass einer Ermittlungsanordnung 161
c) Form und Verfahren der Übermittlung 162
d) Anerkennung der Europäischen Ermittlungsanordnung 164
e) Versagungsgründe – Grenzen der gegenseitigen Anerkennung 167
f) Aufschubgründe 175
g) Verfahren der Vollstreckung der Ermittlungsanordnung und Übermittlung 175
IV. Sonstige Instrumente 177
V. Der Entwurf Rahmenbeschluss Verfügbarkeit 179
1. Vorbemerkungen 179
2. Anwendungsbereich 180

3. Regelungsgehalt 181
a) Grundsatz der freien Verfügbarkeit 181
b) Grenzen 182
c) Sonstiges/Besonderes 183

B. Vergleich und Zusammenspiel der einzelnen Instrumente 184
I. Anwendungsbereich und Verhältnis zu anderen Rechtsakten 184
1. Vergleich Anwendungsbereich 184
2. Verhältnis zueinander und zu anderen Rechtsakten 188
a) Regelungen des Rahmenbeschlusses schwedische Initiative 188
b) Regelungen des Prümer Beschlusses 189
c) Regelungen der Richtlinie über die Europäische Ermittlungsanordnung 191
d) Offene Anwendungsfragen 192
e) Ergebnis 197
II. Gemeinsamkeiten und Unterschiede der Umsetzung der untersuchten Grundsätze 197

Dritter Teil: Informationshilfegegenrechte und Datenschutz 206

A. Europäische Grund- und Menschenrechte 207

B. Europäisches Sekundärrecht 209
I. Spezielle Regelungen 209
1. Der Rahmenbeschluss schwedische Initiative 209
a) Regelungen mit datenschutzrechtlichem Gehalt 209
aa) Art. 8 RBSI 210
(1) Art. 8 Abs. 1 RBSI – Anwendbarkeit der für den Kommunikationsweg geltenden Datenschutzbestimmungen 210
(2) Art. 8 Abs. 2 Satz 1 und 2 RBSI – Anwendbarkeit nationaler und völkerrechtlicher Datenschutzbestimmungen 212
(a) Verweis auf nationales Recht 212
(b) Verweis auf die Datenschutzkonvention und das Zusatzprotokoll zur Datenschutzkonvention 212

(c) Verweis auf die Empfehlung R (87) 15 des Ministerkomitees des Europarats 217
(3) Art. 8 Abs. 3 und 4 RBSI – autonome Regelungen zum Datenschutz 218
(a) Ein Grundsatz transnationaler Zweckbindung 218
(b) Ausnahmen vom Grundsatz der Zweckbindung 220
(c) Verwendungsbedingungen 223
bb) Art. 9 RBSI – Vertraulichkeit der Datenverarbeitung 224
cc) Art. 10 RBSI – Verweigerungsgründe 224
b) Bewertung 225
aa) Prinzip 225
bb) Verhältnismäßigkeitsgrundsatz 226
cc) Zweckbindung 227
dd) Fehlen eigenständiger Regelungen zu Auskunft, Information, Umgang mit besonders sensiblen Daten, Rechtschutz 229
(1) Auskunft und Information 229
(2) Berichtigungs-, Löschungsansprüche, Höchstspeicherfristen 230
(3) Kontrolle, Rechtsschutz 232
c) Ergebnis 235
2. Der Prümer Vertrag und der Prümer Beschluss 236
a) Die vorgesehenen Regelungen 236
aa) Mindeststandard – Art. 25 PB 237
bb) Art. 14 Abs. 2 Satz 1 PB – Zweckbindung und Löschungspflichten von personenbezogenen Daten, die im Zusammenhang mit Großveranstaltungen übermittelt werden 239
cc) Übermittlung zur Verhinderung terroristischer Straftaten 240
dd) Art. 26 PB – Zweckbindung 240
ee) Art. 28 – Richtigkeit, Löschungs- bzw. Sperrungspflichten 243
(1) Richtigkeit der Daten 243
(2) Sonstige Löschungspflichten 245

(3) Ausnahmsweise Sperrung statt Löschung im Interesse des Betroffenen 246
ff) Informationsansprüche 247
gg) Beschränkter Personenkreis – besondere Ermächtigung für automatisierte Abruf- und Abgleichverfahren 249
hh) Protokollierungs- und Dokumentationspflichten, Datenschutzbehörden 249
ii) Rechtsschutz 252
b) Bewertung 256
aa) Die Übermittlung von DNA-Profilen, daktyloskopischen Daten und KfZ-Halterdaten – Voraussetzungen und Reichweite 256
(1) Abgestufter Zugriff 256
(2) Abgestufte Übermittlungszwecke 257
(3) Keine Relevanzschwelle für den automatisierten Abruf und Abgleich von DNA-Profilen 259
(4) Gewinnung und Untersuchung molekulargenetischen Materials und Übermittlung von DNA-Profilen nach Art. 7 PB 261
bb) Mindestdatenschutzniveau 266
cc) Zweckbindung 271
dd) Datenqualität 273
ee) Beteiligungsrechte 274
ff) Protokollierung und Dokumentation, Kontrolle und Rechtschutz 277
c) Ergebnis 281
3. Der Entwurf Rahmenbeschluss Verfügbarkeit 282
a) Vorgesehene Regelungen 283
b) Bewertung 284
4. Die Richtlinie über die Europäische Ermittlungsanordnung 286
II. Der Rahmenbeschluss Datenschutz 287
1. Das Rechtssetzungsverfahren 287

2. Die vorgesehenen Regelungen 290
a) Anwendungsbereich 290
aa) Keine Anwendbarkeit des Rahmenbeschlusses Datenschutz auf rein nationale Datenverarbeitungen 291
(1) Vorgaben des Primärrechts – Rechtsgrundlage 293
(2) Ziele des Sekundärrechts, insbesondere des Rahmenbeschlusses Datenschutz 296
(3) Weitere Erwägungen 297
bb) Verhältnis zu anderen Instrumenten 299
b) Voraussetzungen für eine rechtmäßige Datenverarbeitung 301
aa) Achsen des Datenschutzes: Rechtmäßigkeit, Verhältnismäßigkeit und Zweckbindung (Art. 3 RBDS) 301
(1) Rechtmäßigkeit der Verarbeitung 301
(2) Verhältnismäßigkeitsgrundsatz 302
(3) Zweckbindung 303
bb) Berichtigung, Löschungsfristen und -verpflichtungen, Sperrung 308
cc) Besondere Arten von personenbezogenen Daten 314
dd) Automatisierte Einzelentscheidungen 316
ee) Besondere innerstaatliche Verarbeitungsbeschränkungen 318
ff) Beteiligung von Drittstaaten, internationalen Einrichtungen und nicht-öffentlichen Stellen in den Mitgliedstaaten 320
(1) Besonderheiten in Drittstaatskonstellationen 320
(a) Weiterleitung personenbezogener Daten an einen Drittstaat 321
(b) Grenzüberschreitende Weiterleitung von Informationen, die aus einem Drittstaat stammen 328

(c) Übermittlung von aus einem EU-Mitgliedstaat stammenden personenbezogenen Daten durch einen Drittstaat an einen anderen EU-Mitgliedstaat 329
(2) Beteiligung nicht-öffentlicher Stellen 332
gg) Vertraulichkeit der Verarbeitung 335
hh) Sicherheit der Verarbeitung 335
c) Beteiligung der betroffenen Person 336
aa) Pflicht zur Information (Art. 16 RBDS), Recht auf Auskunft (Art. 17 RBDS) 337
(1) Information 337
(2) Auskunftsanspruch 339
(a) Rechtsnatur und Umfang des Auskunftsanspruchs 339
(b) Antragserfordernis, Modalitäten 340
(c) Ausnahmen und Einschränkungen 340
bb) Berichtigungs-, Löschungs- und Sperrungsanspruch (Art. 18 RBDS) 342
cc) Schadensersatz 343
dd) Rechtsschutz 344
d) Umsetzung und Durchsetzung des Rahmenbeschlusses 345
aa) Protokollierung und Dokumentation 347
bb) Nationale Kontrollstellen 349
cc) Sanktionen 351
3. Bewertung 352
a) Allgemeines – Anwendungsbereich, Regelungstechnik 352
b) Grundsätze – Rechtmäßigkeit, Zweckbindung, Verhältnismäßigkeit 354
c) Berichtigung, Löschungsfristen und -pflichten, Sperrung 357
d) Besonders sensible Daten 359
e) Automatisierte Einzelentscheidungen 361
f) Innerstaatliche Verarbeitungsbeschränkungen 362

g) Drittstaaten, internationale Einrichtungen, nicht-öffentliche Stellen 363
aa) Drittstaaten und internationale Einrichtungen 363
(1) Angemessenes Datenschutzniveau im Drittstaat 363
(2) Insbesondere keine Zweckbindung 367
(3) Eingeschränkter Anwendungsbereich 367
(4) Informationen aus Drittstaaten 368
bb) Nicht-öffentliche Stellen 369
(1) Regelungsweite 369
(2) Regelungsgehalt 370
h) Beteiligung des Betroffenen 372
aa) Information des Betroffenen 372
bb) Auskunft an den Betroffenen 374
cc) Berichtigung, Löschung, Sperrung und Kennzeichnung 376
dd) Durchsetzung der Rechte des Betroffenen, insbesondere im Hinblick auf die Grenzüberschreitung 378
i) Effektive Umsetzung, insbesondere Kontrolle und Sanktionen 383
4. Ergebnis 385

Vierter Teil: Abschließende Bewertung und Ausblick 388

A. Das System der Informationshilfe unter dem Rahmenbeschluss schwedische Initiative und dem Prümer Beschluss 388
I. Tatsächliche Verbesserung der polizeilichen und justiziellen Informationshilfe? 388
II. Ein kohärentes System der Informationshilfe? 394
III. Der Beitrag des Datenschutzes zur effizienten Informationshilfe 395

B. Bewertung des Datenschutzes 397
I. Vereinbarkeit der untersuchten Informationshilfegrundlagen mit Art. 8 GRC 397
1. Art. 3, 4, 9 und 12 PB 397
2. Art. 7 PB 402
3. Art. 14 und 16 PB 404
4. Art. 3, 5 RBSI 407

5. Art. 7 RBSI 410
II. Der Rahmenbeschluss Datenschutz – eine einheitliche Regelung zur Gewährleistung eines hohen Datenschutzniveaus im Rahmen der polizeilichen und justiziellen Zusammenarbeit? 413
III. Zersplitterung und unterschiedliche Schutzniveaus in einem Raum der Freiheit, der Sicherheit und des Rechts 416
IV. Unterschiedliche Schutzniveaus – fehlende Kohärenz zum Datenschutz im Binnenmarkt? 418

C. Eine kohärente Strategie der Europäischen Union für einen internationalen Datenschutz? 423

D. Ausblick 430

Literaturverzeichnis 439

Einleitung

Die Europäische Union verfolgt das Ziel der Schaffung und Erhaltung eines Raumes der Freiheit, der Sicherheit und des Rechts (Art. 3 Abs. 2 EUV, Art. 67 Abs. 1 AEUV). Eine effektive grenzüberschreitende polizeiliche und justizielle Zusammenarbeit ist gefordert, um die Sicherheit und das Recht, aber auch die Freiheit im europäischen Raum der Freiheit, der Sicherheit und des Rechts entsprechend der Zielsetzung in den Verträgen zu gewährleisten. Im Mittelpunkt des medialen Interesses steht dabei regelmäßig die anhaltende Bedrohung in Europa durch den internationalen Terrorismus. Dieser stellt mit einer gegenüber den Anschlägen zu Beginn dieses Jahrhunderts in New York, Madrid und London veränderten Strategie, wie sie etwa in den Anschlägen vom 7. Januar 2015 in Paris zum Ausdruck kam, die zuständigen Behörden und den europäischen Gesetzgeber vor neue Herausforderungen.

Neben der Bekämpfung des (internationalen) Terrorismus ist auch die Bekämpfung sonstiger grenzüberschreitender Kriminalität[1] eine andauernde Aufgabe im Raum der Freiheit, der Sicherheit und des Rechts.

Ein modernes Informationsmanagement ist ein zentraler Baustein für die Erfüllung dieser Aufgaben. Jegliches polizeiliches Handeln beruht auf der Verfügbarkeit von Informationen, Eingriffe in Rechte der Bürger setzen in der Regel die Verfügbarkeit personenbezogener Daten voraus.[2] Vergleichbares gilt für Maßnahmen der Strafverfolgungsbehörden.

---

1 Insbesondere der internationale Drogenhandel, die organisierte Kriminalität und die Verhinderung illegaler Migration dienten und dienen neben der Bekämpfung des Terrorismus als Legitimationsfiguren einer immer tiefer werdenden Integration der polizeilichen und justiziellen Zusammenarbeit, *Aden/Busch*, in: Roggan/Kutscha (Hrsg.), Handbuch der inneren Sicherheit, S. 514; *Mutschler*, Der Prümer Vertrag, S. 47; vgl. auch *Nelles*, ZStW 109 (1997), 727 (731).

2 *Kugelmann*, in: Böse (Hrsg.), Europäisches Strafrecht mit polizeilicher Zusammenarbeit (EnzEuR Bd. 9), § 17 Rdnr. 11.

Ein möglichst ungehinderter Austausch von Daten[3] und Informationen[4] zwischen den zuständigen Behörden verschiedener Mitgliedstaaten kann daher essentiell dazu beitragen, ein hohes Maß an Sicherheit zu gewährleisten.[5] Dementsprechend umfasst die polizeiliche Zusammenarbeit ausdrücklich das „Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen" (Art. 87 Abs. 2 AEUV). Für die Zusammenarbeit der Justizbehörden in Strafsachen ist der Informationsaustausch Teil der Zusammenarbeit i.S.d. Art. 82 Abs. 1 lit. d AEUV.[6]

Auf den ersten Blick ist ein solcher Austausch leicht zu realisieren. Erstens sind Daten und Informationen faktisch besonders leicht und schnell übertragbar. Außerdem beeinträchtigt eine Übertragung an eine Behörde in einem anderen EU-Mitgliedstaat nicht die andauernde Verfügbarkeit der entsprechenden Information für die übertragende Behörde oder andere zuständige Behörden im Datei führenden Staat.

---

3 Daten sind Zeichen oder Symbole, die auf einem Datenträger gespeichert sind und die in Zusammenhang mit Beobachtungen oder Mitteilungen Informationen vermitteln können, *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, § 22 Rdnrn. 11 ff.; *Hoffmann-Riem*, in: ders./Schmidt-Assmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, S. 9 (12); *Scherzberg*, in: Hoffmann-Riem/Schmidt-Assmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, S. 195 (198).

4 Informationen knüpfen an Beobachtungen, Mitteilungen oder eben auch an Daten an und entstehen durch eine Interpretationsleistung der empfangenden Person bzw. Stelle, *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, § 22 Rdnr. 11; *Vesting*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, § 20 Rdnr. 19; *Scherzberg*, in: Hoffmann-Riem/Schmidt-Assmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, S. 195 (199 f.): „Erst die Zuweisung von Bedeutung macht das jeweilige Datum zur Information."
Die Begriffe „Daten" und „Informationen" werden durch den Gesetzgeber häufig synonym gebraucht und miteinander vermischt, Beispiele bei *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, § 22 Rdnr. 8 in Fn. 33; krit. auch *Vesting*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, § 21 Rdnr. 15. Solche Ungenauigkeiten haben jedoch kaum Auswirkungen auf die Praxis, *Vesting*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, § 20 Rdnr. 16. Im Folgenden werden daher die jeweiligen Begrifflichkeiten des europäischen Gesetzgebers zugrundegelegt.

5 *Esser*, in: Böse (Hrsg.), Europäisches Strafrecht mit polizeilicher Zusammenarbeit (EnzEuR Bd. 9), § 19 Rdnr. 1.

6 Vgl. nur *Vogel*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der Europäischen Union, Art. 82 AEUV Rdnr. 70.

Den Interessen an einem verstärkten und erleichterten Austausch personenbezogener Daten sind aber grund- und menschenrechtliche Grenzen gesetzt, insbesondere durch das Recht auf Datenschutz (Art. 8 Charta der Grundrechte der Europäischen Union[7], Art. 16 AEUV). Den steigenden technologischen Möglichkeiten und dem Datenhunger von vor allem in- und ausländischen Geheimdiensten,[8] Gefahrenabwehr- und Strafverfolgungsbehörden stehen eine zunehmend sensibilisierte Öffentlichkeit und kritische nationale, supranationale und internationale Gerichtsbarkeiten[9] gegenüber. Neue Chancen bieten sich in diesem Zusammenhang für die polizeiliche und die justizielle Zusammenarbeit in Strafsachen aufgrund der veränderten rechtlichen Rahmenbedingungen nach dem Inkrafttreten des Vertrags von Lissabon[10] und des Ablaufs der anwendbaren Übergangsregelungen am 1. Dezember 2014.[11] Die Sonderstellung dieser Politikbereiche ist beendet:[12] Das ordentliche Gesetzgebungsverfahren

---

7 ABl. EU v. 26.10.2012, Nr. C 326, S. 391, im Folgenden: „EU-Grundrechtecharta (GRC)".

8 Besonders im Fokus der Presse und der Öffentlichkeit steht dabei seit dem Erscheinen eines auf Informationen des Whistleblowers Edward Snowden beruhenden Artikels in der britischen Zeitung „The Guardian" (abrufbar unter http://www.theguardian.com/world/the-nsa-files, zuletzt abgerufen am 16.11.2015) die umfassende Ausspähpraxis des amerikanischen Geheimdienstes NSA (National Security Agency) und des britischen Geheimdienstes, dazu z.B. *Hansen*, DuD 2014, 439 ff.; *Roßnagel/Jandt/Richter*, DuD 2014, 545 ff.

9 Vgl. z.B. zur Vorratsdatenspeicherung nur EuGH, Urt. v. 8.4.2014, C-293/12 und C-594/12 (NJW 2014, 2169); BVerfGE 125, 260; zur sog. Antiterrordatei BVerfGE 133, 277; zur Speicherung von DNA-Daten in Großbritannien EGMR, Urt. v. 4.12.2008, S. und Marper ./. Vereinigtes Königreich, 30562/04 und 30566/04, Reports of Judgments and Decisions 2008-V, 167.

10 ABl. EU v. 17.12.2007, Nr. C 306, S. 1, zuletzt bekannt gemachte konsolidierte Fassung im ABl. EU v. 26.10.2012, Nr. C 326, S. 1. Der Vertrag von Lissabon ist am 1.12.2009 in Kraft getreten.

11 Art. 10 Protokoll über die Übergangsbestimmungen zum Vertrag von Lissabon.

12 Zu den folgenden und weiteren Auswirkungen des Inkrafttretens des Vertrags von Lissabon oder des Ablaufs der Übergangsfrist auf die polizeiliche und justizielle Zusammenarbeit in Strafsachen *Satzger*, in: Max-Planck-Institut für ausländisches und internationales Strafrecht (Hrsg.), Europäisches Strafrecht, § 1 Rdnrn. 4 ff., 20, 63 ff.; *Sieber*, in: Max-Planck-Institut für ausländisches und internationales Strafrecht (Hrsg.), Europäisches Strafrecht, Einführung Rdnrn. 164 ff.; Stellungnahme des Europäischen Datenschutzbeauftragten zur künftigen Entwicklung des Raums der Freiheit, der Sicherheit und des Rechts, abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2

(Art. 289 Abs. 1, Art. 294 AEUV) erfasst nun grundsätzlich[13] auch die polizeiliche und justizielle Zusammenarbeit in Strafsachen. Das Europäische Parlament wird hierdurch erheblich gestärkt. Auch die Bedeutung des Europäischen Gerichtshofs nimmt durch die Aufgabe der Beschränkungen seiner Gerichtsbarkeit (Art. 35 EUV a.F.) zu. Die Stärkung dieser beiden Akteure ist ein Gewinn für die aus Grundrechtssicht äußerst sensiblen Politikbereiche.

Das so skizzierte Spannungsfeld beherrscht folgerichtig die europäischen Leitlinien für ein modernes System des Informationsaustauschs. Der Europäische Rat hat die Einführung des Informationsaustauschs zwischen den zuständigen Behörden der Mitgliedstaaten nach dem Grundsatz der freien Verfügbarkeit im Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union gefordert.[14] Ziel der Einführung des Grundsatzes der Verfügbarkeit ist danach, „dass unionsweit ein Strafverfolgungsbeamter in einem Mitgliedstaat, der für die Erfüllung seiner Aufgaben Informationen benötigt, diese aus einem anderen Mitgliedstaat erhalten kann und dass die Strafverfolgungsbehörde in dem anderen Mitgliedstaat, die über diese Informationen verfügt, sie […] für den erklärten Zweck bereitstellt.“ Die nationalstaatlichen Grenzen innerhalb der Europäischen Union als solche sollen den Informationsfluss nicht mehr behindern.[15]

Im Stockholmer Programm[16] betrachtet der Europäische Rat die bis dahin auf dem Weg zu einem umfassenden Informationsmanagement der Europäischen Union unternommenen Schritte bereits mit „Zufrieden-

---

014/14-06-04_Future_AFSJ_DE.pdf (zuletzt abgerufen am 16.11.2015), S. 1; die Zusammenfassung der Stellungnahme ist im Amtsblatt der Europäischen Union veröffentlicht, ABl. EU v. 15.7.2014, Nr. C 224, S. 28; vertiefend: *Beukelmann*, NJW 2010, 2081 ff.; *Heger*, ZIS 2009, 406 ff.

13 Teilweise finden aber besondere Verfahrensvorschriften Anwendung, wie z.B. das Einstimmigkeitsprinzip im Rat in Art. 82 Abs. 3 AEUV und das Vetorecht einzelner Ratsmitglieder in Art. 83 Abs. 3 AEUV, dazu z.B. *Heger*, ZIS 2009, 406 (411, 413 ff.).

14 Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, ABl. EU v. 3.3.2005, Nr. C 53, S. 1, 7 f.

15 Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, ABl. EU v. 3.3.2005, Nr. C 53, S. 1, 7.

16 Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl. EU v. 4.5.2010, Nr. C 115, S. 1.

heit".[17] Besonders hebt er in diesem Zusammenhang den Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität[18], den Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität[19] und den Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union[20] hervor.[21]

Aber er formuliert und betont auch weitere Anforderungen an die Umsetzung dieses Grundsatzes und fordert eine Überprüfung, ob die eingeführten „Instrumente wie ursprünglich vorgesehen funktionieren und ob sie den Zielvorgaben der Strategie für das Informationsmanagement[[22]] entsprechen":[23]

Insbesondere[24] soll das Informationsmanagement den Anforderungen der Praxis gerecht werden und ein solides Datenschutzregime aufweisen.

---

17 Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl. EU v. 4.5.2010, Nr. C 115, S. 1, 18.

18 ABl. EU v. 6.8.2008, Nr. L 210, S. 1 ff., im Folgenden: „Prümer Beschluss (PB)".

19 ABl. EU v. 6.8.2008, Nr. L 210, S. 12 ff., im Folgenden: „Durchführungsbeschluss Prüm (DBP)".

20 ABl. EU v. 29.12.2006, Nr. L 386, S. 89, im Folgenden: „Rahmenbeschluss schwedische Initiative (RBSI)".

21 Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl. EU v. 4.5.2010, Nr. C 115, S. 1, 18.

22 S. Ratsdok. 16637/09.

23 Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl. EU v. 4.5.2010, Nr. C 115, S. 1, 18 f., dort auch zu den folgenden Anforderungen.

24 Außerdem unterstreicht der Europäische Rat im Stockholmer Programm die Herausforderungen, die sich insbesondere aus technischer Sicht an das System des Informationsmanagements ergeben, wie die Interoperabilität der genutzten IT-Systeme bei Einhaltung von Datenschutz- und -sicherheitsgrundsätzen und die Schaffung der erforderlichen Strukturen. Weiter forderte er die Schaffung einer Verwaltungsstelle für die technische Entwicklung und Verwaltung der großen IT-Systeme, vgl. nunmehr die Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ABl. EU v. 1.11.2011, Nr. 286, S. 1.

Als wesentliche Elemente dieses Datenschutzregimes nennt der Europäische Rat die „Zweckgebundenheit, Verhältnismäßigkeit und Rechtmäßigkeit der Verarbeitung, zeitlich begrenzte Speicherung, Sicherheit und Vertraulichkeit sowie die Achtung der Rechte des Einzelnen, eine Kontrolle durch unabhängige nationale Aufsichtsbehörden und de[n] Zugang zu einem wirksamen Rechtsschutz".[25] Die Grundrechte der Bürger sollen zudem dadurch geschützt werden, dass Daten nur gezielt erhoben werden, was zugleich die zuständigen Behörden vor einer Informationsüberflutung bewahren soll. Eine Strategie für den Datenaustausch mit Drittstaaten und eine Rationalisierung der Instrumente seien ebenso erforderlich wie die umfassende Koordination, Konvergenz und Kohärenz des Informationsmanagements.

Als Antwort auf die Forderung des Europäischen Rates im Stockholmer Programm stellte die Kommission im Dezember 2012 das europäische Modell für den Informationsaustausch vor.[26] Sie bewertete hierbei unter anderem das Funktionieren der Instrumente, die infolge der Zielsetzungen des Haager Programms eingeführt wurden,[27] und sieht zu diesem Zeitpunkt grundsätzlich keinen Bedarf für die Einführung neuer Instrumente.[28] Bestehende Instrumente sollen in der Zukunft jedoch konsequenter angewandt werden.[29] Auch die Kommission hebt die Bedeutung einer hohen Datenqualität, -sicherheit und eines hohen Datenschutzniveaus hervor.[30] Der Standpunkt der Kommission wird vom Europäischen Rat insofern bestätigt, als er allgemein die wirksame Anwendung und Konsolidierung bestehender Instrumente, einen verbesserten grenzüberschreitenden Informa-

---

25 Europäischer Rat, Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl. EU v. 4.5.2010, Nr. C 115, S. 1, 10.

26 Mitteilung der Kommission an das Europäische Parlament und den Rat, Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch, COM(2012) 735 final.

27 Z.B. den Rahmenbeschluss schwedische Initiative und den Prümer Beschluss, dazu ausführlich unten Zweiter Teil A.I, A.II und Dritter Teil B.I.1, B.I.2.

28 Mitteilung der Kommission an das Europäische Parlament und den Rat, Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch, COM(2012) 735 final, S. 1.

29 Mitteilung der Kommission an das Europäische Parlament und den Rat, Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch, COM(2012) 735 final, S. 9.

30 Mitteilung der Kommission an das Europäische Parlament und den Rat, Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch, COM(2012) 735 final, S. 1 und 14.

tionsaustausch und die Förderung des Datenschutzes in seine jüngsten strategischen Leitlinien für die gesetzgeberische Planung im Raum der Freiheit, der Sicherheit und des Rechts (sog. Brüsseler Programm) aufgenommen hat.[31]

Im Folgenden soll untersucht werden, ob die seit dem Haager Programm unternommenen Schritte und hierbei der Schwerpunktsetzung des Europäischen Rates entsprechend insbesondere der Prümer Beschluss und der Rahmenbeschluss schwedische Initiative diesen Anforderungen an ein modernes europäisches Informationsmanagement gerecht werden. Hierzu werden zunächst die Anforderungen, die im Stockholmer Programm und der Strategie der Kommission genannt wurden, präzisiert und deren rechtliche Grundlagen analysiert (Erster Teil). Als Ausgangspunkt zur Beurteilung der Erforderlichkeit der Rechtsetzung soll ein Überblick über die Situation des Informationsaustauschs zwischen den Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten vor Einführung der genannten Instrumente dienen (A). Zur Skizzierung des rechtlichen Rahmens für den grenzüberschreitenden Informationsaustausch innerhalb der polizeilichen und justiziellen Zusammenarbeit werden zunächst die Grundlagen und Facetten des primärrechtlichen Kohärenzgebots bezogen auf ein Informationsmanagement im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen dargestellt (B). Dem folgt eine Analyse der rechtlichen Grundlagen der anwendbaren Grund- und Menschenrechte, insbesondere des Rechts auf Schutz der personenbezogenen Daten. Hieraus werden konkrete Vorgaben an ein System des Austauschs personenbezogener Daten zwischen Gefahrenabwehr- und Strafverfolgungsbehörden unterschiedlicher EU-Mitgliedstaaten formuliert (C). Anforderungen an den grenzüberschreitenden Informationsaustausch technischer und organisatorischer Art sollen den Ersten Teil abschließen (D).

Im Zweiten Teil werden die maßgeblichen Rechtsetzungstätigkeiten der Europäischen Union in Umsetzung der Ziele des Haager Programms zur Einführung eines Informationsmanagements hin zum Grundsatz der Verfügbarkeit dargestellt, wobei die Schwerpunkte entsprechend der Schwer-

---

31 Schlussfolgerungen des Europäischen Rates (Tagung vom 26./27. Juni 2014), EUCO 79/14, S. 2 (Ziff. 3, 4) und 5 (Ziff. 10), vgl. auch den im Amtsblatt veröffentlichten Auszug aus den Schlussfolgerungen des Europäischen Rates (Tagung vom 26./27. Juni 2014) betreffend den Raum der Freiheit, der Sicherheit und des Rechts und einige damit zusammenhängende Querschnittsthemen, ABl. EU v. 24.7.2014, Nr. C 240, S. 13 (Ziff. 3 und 4) und 15 (Ziff. 10).

punktsetzung des Europäischen Rates und der Kommission auf dem sog. Prümer Beschluss und der schwedischen Initiative liegen sollen. Hierbei soll bereits ein besonderes Augenmerk darauf gelegt werden, ob Anforderungen, die sich aus der Praxis und dem Kohärenzgebot in seinen anwendbaren Facetten ergeben, erfüllt werden.

Im Dritten Teil werden die datenschützenden Vorschriften des Rahmenbeschlusses schwedische Initiative und des Prümer Beschlusses sowie der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[32], dargestellt, wesentliche Unterschiede zur EG-Datenschutzrichtlinie aufgezeigt und im Hinblick auf die Vorgaben der EU-Grundrechtecharta bewertet.

Im diese Arbeit abschließenden Vierten Teil soll das durch die untersuchten Instrumente geschaffene europäische Modell für einen Informationsaustausch einer abschließenden und zusammenfassenden Bewertung im Hinblick auf die aufgeworfenen und untersuchten Fragen unterzogen werden. Ein Ausblick auf die geplante EU-Datenschutzreform wird gewährt und aus dem Ergebnis der Bewertung des aktuellen Datenschutzregimes werden konkrete Anforderungen an den europäischen Gesetzgeber abgeleitet.

---

32 ABl. EU v. 30.12.2008, Nr. L 350, S. 60, im Folgenden: „Rahmenbeschluss Datenschutz (RBDS)“.

Erster Teil: Anforderungen an das System der Informationshilfe in der Europäischen Union

A. Erforderlichkeit eines effektiven Instruments betreffend die Übermittlung und den Austausch von Informationen

Zur Bekämpfung der grenzüberschreitenden Kriminalität einschließlich der Bedrohungen des internationalen Terrorismus ist angesichts des Umstands, dass diesen ein Wegfall der Binnengrenzen und damit einhergehend ein Wegfall der Grenzkontrollen im Schengen-Raum gegenübersteht, ein generelles Bedürfnis für eine effiziente Kooperation zwischen den Strafverfolgungsbehörden offensichtlich, um den konstatierten „ständigen Wettbewerbsvorsprung krimineller Strukturen“[33] einzudämmen. Die Justiz- und Innenminister unterstrichen bereits eine knappe Woche nach den Anschlägen in London am 13. Juli 2005 auf einer außerordentlichen Sitzung die Bedeutung verbesserter Kooperationsinstrumente für die Verhinderung weiterer Anschläge und eine wirksame Terrorismusbekämpfung.[34] Die Mitglieder des Europäischen Rates forderten am 12. Februar 2015 in Reaktion auf die Terroranschläge in Paris vom 7. Januar 2015 einen verstärkten Informationsaustausch zwischen den Strafverfolgungs- und Justizbehörden.[35] Die Bedeutung des Informationsaustauschs für die europäische Sicherheitsstrategie wird nicht zuletzt durch die erhebliche Nutzung[36] schon bestehender Instrumente wie den elektronischen Austausch von Informationen über zur Fahndung ausgeschriebene Personen und Gegenstän-

---

33 *Zöller*, ZIS 2011, 64.

34 Kommissionsbegründung zu ihrem Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit, KOM(2005) 490 endgültig, im Folgenden: „Entwurf Rahmenbeschluss Verfügbarkeit (E-RBV)“, S. 2.

35 Erklärung der Mitglieder des Europäischen Rates, Informelle Tagung der Staats- und Regierungschefs, Brüssel, den 12. Februar 2015, abrufbar unter http://www.consilium.europa.eu/de/press/press-releases/2015/02/150212-european-council-statement-fight-against-terrorism/ (zuletzt abgerufen am 16.11.2015).

36 So enthielt das Schengener Informationssystem (SIS) zum 1.1.2013 ca. 46,5 Mio. Datensätze, Ratsdok. 7389/13, S. 1; *Eisele*, in: Max-Planck-Institut für ausländisches und internationales Strafrecht (Hrsg.), Europäisches Strafrecht, § 49 Rdnr. 5.

de mittels des durch das Schengener Durchführungsübereinkommen vom 19. Juni 1990 (SDÜ)[37] eingeführten Schengener Informationssystems (SIS)[38], dessen Weiterentwicklung SIS II[39] seit dem 9. April 2013 in Betrieb ist,[40] deutlich.[41] Neben den Gefahren durch den Terrorismus in jeglicher Ausprägung werden auch weiterhin die sonstige organisierte Kriminalität und die grenzüberschreitende Kriminalität, aber auch Gewalt anlässlich von Veranstaltungen und Katastrophen als größte Herausforderungen für die Innere Sicherheit der Europäischen Union bezeichnet.[42]

---

37 Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen, BGBl. II 1993, S. 1013.

38 Zum SIS *Eisele*, in: Max-Planck-Institut für ausländisches und internationales Strafrecht (Hrsg.), Europäisches Strafrecht, § 49 Rdnrn. 5 ff.; *Harings*, Grenzüberschreitende Zusammenarbeit der Polizei- und Zollverwaltungen, S. 81 ff.; *Oberleitner*, Schengen und Europol, S. 74 ff.; *Würz*, Das Schengener Durchführungsübereinkommen, S. 94 ff.

39 Beschluss 2001/886/JI des Rates vom 6. Dezember 2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. EG v. 13.12.2001, Nr. L 328, S. 1; Beschluss 2006/1007/JI des Rates vom 21. Dezember 2006 zur Änderung des Beschlusses 2001/886/JI über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. EU v. 30.12.2006, Nr. L 411, S. 78; Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. EU v. 7.8.2007, Nr. L 205, S. 63; Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20.12.2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. EU v. 28.12.2006, Nr. L 381, S. 4.

40 Bericht der Kommission an das Europäische Parlament und den Rat – Letzter Fortschrittsbericht über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II), KOM(2013) 777 endgültig, S. 7.

41 Kommission in ihrer Begründung zu ihrem Entwurf Rahmenbeschluss Verfügbarkeit, KOM(2005) 490 endgültig, S. 2.

42 Ratsdok. 5842/2/2010 – Die Strategie der inneren Sicherheit der Europäischen Union: „Hin zu einem europäischen Sicherheitsmodell“, S. 5 f.; dazu *Brodowski*, Jura 2013, 492 (493). Die Strategie wurde vom Rat im Februar 2010 beschlossen und im darauffolgenden Monat vom Europäischen Rat gebilligt. Dort (S. 8) wird auch die Bedeutung, die gerade der Informationsaustausch für diese Herausforderungen hat, unterstrichen.

Seit 1995 fand der polizeiliche Informationsaustausch zwischen den zuständigen Behörden der Mitgliedstaaten[43] zur vorbeugenden Bekämpfung und Aufklärung von Straftaten auf der Grundlage von Art. 39 SDÜ[44] statt. Die Europäische Kommission kritisierte, dass hiernach keine Pflicht zur Antwort auf ein auf dieser Rechtsgrundlage eingehendes Ersuchen bestehe, weswegen der Ausgang eines solchen Ersuchens in der Praxis vielfach ungewiss war.[45] Zwar beinhaltet Art. 39 SDÜ eine Pflicht zur gegenseitigen Leistung polizeilicher Amtshilfe.[46] Jedoch fehlt es an einer ausdrücklichen Verpflichtung zur Kommunikation zwischen den beteiligten Behörden, z.B. die Information der ersuchenden Behörde, wenn sich die Leistung der Amtshilfe verzögert, und die Gründe dafür, sowie Fristenregelungen, was zu langen Wartezeiten in der Praxis führte. Darüber hinaus fand ein Austausch auf der Grundlage des Art. 39 SDÜ in der Regel nicht unmittelbar zwischen den beteiligen Polizeibehörden statt, sondern es musste ein häufig zeitraubendes Verfahren durchlaufen werden, in das übergeordnete Behörden einzubinden waren.[47]

---

43 Zwar sind nicht alle Mitgliedstaaten auch solche der Schengen-Vertragswerke, jedoch gelten die Regeln über die polizeiliche und justizielle Zusammenarbeit auch für die Nicht-Schengen-Mitglieder Vereinigtes Königreich und Irland. Darüber hinaus gilt Art. 39 SDÜ auch für alle Vertragsstaaten, die nicht Mitglieder der Europäischen Union sind (wie z.B. die Schweiz, Island und Norwegen), zum Unterzeichnerkreis im Einzelnen http://www.auswaertiges-amt.de/sid_D570BC89283B7B47C56B6F8366033240/DE/EinreiseUndAufenthalt/Schengen_node.html#doc350334bodyText3 (zuletzt abgerufen am 16.11.2015).

44 Art. 39 Abs. 1, 2 und 3 SDÜ wurden im Anwendungsbereich des Rahmenbeschlusses schwedische Initiative mit Wirkung zum 19.12.2008 ersetzt, Art. 12 Abs. 1 RBSI. Allerdings war der Rahmenbeschluss Ende 2012 – 4 Jahre nach Ablauf der Umsetzungsfrist – noch nicht in allen Mitgliedstaaten umgesetzt, Mitteilung der Kommission an das Europäische Parlament und den Rat, Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch, COM(2012) 735 final, S. 10.

45 Begründung zu ihrem Entwurf Rahmenbeschluss Verfügbarkeit, KOM(2005) 490 endgültig, S. 4.

46 Dazu *Harings*, Grenzüberschreitende Zusammenarbeit der Polizei- und Zollverwaltungen, S. 70 m. Nachw.

47 Begründung der Kommission zu ihrem Entwurf Rahmenbeschluss Verfügbarkeit, KOM(2005) 490 endgültig, S. 3 f. Im Regelfall verläuft die Kommunikation zwischen den von den Mitgliedstaaten hierzu benannten zentralen Stellen, Art. 39 Abs. 1 Satz 1 SDÜ. Allerdings besteht in Eilfällen die Möglichkeit, die Ersuchen unmittelbar zwischen den zuständigen Polizeibehörden zu bearbeiten (Art. 39 Abs. 3 Satz 2 SDÜ), worüber die zentrale Stelle des ersuchten Mitgliedstaates zu unterrichten ist (Art. 39 Abs. 3 Satz 3 SDÜ).

Große Bedeutung kommt in diesem Bereich auch Europol[48] zu. Ziel von Europol ist nach Art. 3 Europol-Beschluss und Art. 88 Abs. 1 AEUV die Tätigkeit und Zusammenarbeit der zuständigen nationalen Behörden bei der Prävention und Bekämpfung von schwerer Kriminalität (insbesondere Terrorismus und organisierte Kriminalität), die zwei oder mehr Mitgliedstaaten betrifft, zu unterstützen. Dabei hat Europol neben Koordinationstätigkeiten bei operativen Maßnahmen unter anderem die Aufgabe, Informationen und Erkenntnisse zu diesem Zweck zu sammeln, zu verarbeiten, insbesondere auch auszutauschen (Art. 5 Abs. 1 lit. a Europol-Beschluss und Art. 88 Abs. 2 lit. a AEUV) und an Mitgliedstaaten zu übermitteln (Art. 5 Abs. 1 lit. b, lit. c und e, Abs. 3 lit. b Europol-Beschluss). Die Kommission bemängelt jedoch, dass Europol diese Aufgaben effektiv besser ausfüllen könnte, wenn Europol innerhalb seiner Zuständigkeiten einen erweiterten Zugriff auf Informationen erhielte.[49]

Eine Pflicht zum Informationsaustausch im Rahmen der justiziellen Zusammenarbeit in Strafsachen besteht zwar als Teil der Rechtshilfe schon nach Art. 1 Abs. 1 EuRhÜbk[50] sowie nach der Spezialregelung des Art. 3

---

48 Errichtet durch Übereinkommen auf Grund von Art. K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (Europol-Übereinkommen), ABl. EG v. 27.11.1995, Nr. C 316, S. 2, im Folgenden: „Europol-Übereinkommen“. Das Europol-Übereinkommen wurde mittlerweile durch den Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) (2009/371/JI), ABl. EU v. 15.5.2009, Nr. L 121, S. 37, im Folgenden: „Europol-Beschluss“, ersetzt (Art. 1 Abs. 1 Europol-Beschluss). Zur geplanten Europol-Reform Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit und die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Europol) und zur Aufhebung der Beschlüsse 2009/371/JI und 2005/681/JI des Rates, COM(2013) 173 final, vgl. Mitteilung der Kommission an das Europäische Parlament und den Rat, Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch, COM(2012) 735 final, S. 9, 10.

49 Begründung zum Entwurf Rahmenbeschluss Verfügbarkeit, KOM(2005) 490 endgültig, S. 4.

50 Europäisches Übereinkommen über die Rechtshilfe in Strafsachen, BGBl. II 1964, S. 1386. Ab dem 22.5.2017 soll dieses durch die Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung, ABl. EU v. 1.5.2014, Nr. L 130, S. 1, im Folgenden: „Richtlinie über die Europäische Ermittlungsanordnung (EEA)“, ersetzt werden, Art. 34 Abs. 1 lit. a EEA.