Livia Matter

Die Interoperabilität der EU-Informationssysteme

Eine Analyse der Vereinbarkeit mit dem Grundrecht auf Datenschutz aus der Perspektive der Schweiz

EIZ Publishing

Die Interoperabilität der EU-Informationssysteme

Eine Analyse der Vereinbarkeit mit dem Grundrecht auf Datenschutz aus der Perspektive der Schweiz

Dissertation zur Erlangung der Würde einer Doktorin der Rechte an der Rechtswissenschaftlichen Fakultät der Universität Freiburg in der Schweiz

vorgelegt von

Livia Matter

Dissertation zur Erlangung der Würde einer Doktorin der Rechte, vorgelegt der Rechtswissenschaftlichen Fakultät der Universität Freiburg in der Schweiz.

Genehmigt von der Rechtswissenschaftlichen Fakultät der Universität Freiburg am 25. März 2024 auf Antrag von Frau Professorin Dr. Astrid Epiney (erste Referentin) und Frau Professorin Dr. Sarah Progin-Theuerkauf (zweite Referentin).

Mit der Annahme einer Dissertation beabsichtigt die Rechtswissenschaftliche Fakultät der Universität Freiburg nicht, zu den darin enthaltenen wissenschaftlichen Meinungen der Verfasserin Stellung zu nehmen (Fakultätsratsbeschluss vom 1. Juli 1916).

Die Interoperabilität der EU-Informationssysteme Copyright © by Livia Matter is licensed under a Creative Commons Namensnennung-Nicht kommerziell-Keine Bearbeitung 4.0 International, except where otherwise noted.

© 2025 – CC BY-NC-ND (Werk), CC BY-SA (Text)

Autor: Livia Matter
Verlag: EIZ Publishing (eizpublishing.ch)
ISBN:
978-3-03805-796-3 (Print – Softcover)
978-3-03805-797-0 (Print – Hardcover)
978-3-03805-798-7 (PDF)
978-3-03805-799-4 (ePub)
DOI: https://doi.org/10.36862/eiz-diss-202501
Version: 1.02 – 20250429

Die Dissertation wurde publiziert mit Unterstützung des Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung.

Die vorliegende Dissertation wurde von Livia Matter eingereicht und am 25. März 2024 von der Rechtswissenschaftlichen Fakultät der Universität Freiburg auf Antrag von Frau Professorin Dr. Astrid Epiney (erste Referentin) und Frau Professorin Dr. Sarah Progin-Theuerkauf (zweite Referentin) genehmigt.

Das Werk ist als gedrucktes Buch und als Open-Access-Publikation in verschiedenen digitalen Formaten verfügbar: https://eizpublishing.ch/publikationen/die-interoperabilitaet-der-eu-informationssysteme/.

Vorwort

Mein Vater pflegte stets zu sagen, dass es bei einer Dissertation nicht primär um das Thema, sondern vielmehr um den Arbeitsprozess als solchen gehe. Obwohl mir diese Aussage lange bevor ich mich für dieses Projekt entschieden hatte, bekannt war, verstehe ich sie erst jetzt, nachdem ich diesen Prozess nun selbst durchlaufen habe.

Ich bin meiner Familie und meinen FreundInnen sehr dankbar für die Begleitung und die vielseitige Unterstützung in diesem Prozess. Speziell hervorheben möchte ich an dieser Stelle die wöchentlichen Telefonate mit einer Freundin, die gleichzeitig dissertierte und somit eine Art «*Leidensgenossin*» war. Dieser Austausch war zwecks Reflektion der Arbeit sowie des Prozesses äusserst wertvoll. Aber auch andere Ohren hörten mir zu, wenn gerade etwas nicht nach Plan lief oder einfach viel mehr Zeit als geplant in Anspruch nahm. Wichtig für meine Motivation waren zudem die vielen Überraschungen, welche ich immer wieder in meinem Briefkasten vorgefunden habe. Danke, dass ihr an mich gedacht habt!

Die Diskussionen zur Interoperabilität mit unterschiedlichen Personen haben vielfach zu neuen Denkanstössen und Ideen geführt, was mich und meine Arbeit bereichert hat. Bestens in Erinnerung bleibt mir der Austausch bei meinem aktuellen Arbeitgeber bezüglich der Umsetzung der Interoperabilität in der Schweiz. Ich bin stolz, dass ich diesbezüglich einen Beitrag leisten und so den Bogen von der Wissenschaft zur Praxis schlagen konnte. Die Flexibilität meines aktuellen Arbeitgebers sowie die Unterstützung meiner ArbeitskollegInnen hat es mir zudem ermöglicht, zwischendurch für ein paar Wochen komplett in die Dissertation einzutauchen. Das ist nicht selbstverständlich und ich habe dies sehr geschätzt.

Unvergessen bleibt zudem der dreimonatige Forschungsaufenthalt am European University Institute (EUI) in Florenz. Obwohl der Austausch vor Ort aufgrund der im Zusammenhang mit der COVID-19-Pandemie erlassenen Massnahmen stark eingeschränkt war, genoss ich es, mich vor einer wunderbaren Kulisse und mit italienischer Kulinarik intensiv mit der Interoperabilität auseinanderzusetzen.

Zuletzt möchte ich allen danken, die meine Dissertation mit einem kritischen Auge Korrektur gelesen haben.

Basel, im März 2025 Livia Matter

Inhaltsübersicht

Vorwort V

Inhaltsübersicht VII

Inhaltsverzeichnis IX

Literaturverzeichnis XVII

Materialienverzeichnis XXXIII

Abkürzungsverzeichnis XLV

Gesetzesverzeichnis LIII

I. Einleitung 1
1. Einführung in die Thematik 1
2. Ziel der Untersuchung 3
3. Aufbau der Arbeit im Überblick 5
4. Begriffsdefinitionen 6

II. Datenschutz als Grundrecht 9
1. Einleitung 9
2. Entwicklung und Grundgedanke des Datenschutzes 10
3. Verzahnung der Grundrechtsinstrumente 11
4. Datenschutzrechtlicher Gehalt von Art. 8 EMRK 18
5. Informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV 31
6. Schutz personenbezogener Daten gemäss Art. 8 GRC 42
7. Gemeinsamkeiten und Unterschiede der Grundrechte 58
8. Fazit 67

III. EU-Informationssysteme 69
1. Einleitung 69
2. Schengener und Dubliner Zusammenarbeit 70
3. Assoziierung der Schweiz an Schengen und Dublin 75
4. Schengener Informationssystem 82
5. Eurodac-Datenbank 93
6. Visa-Informationssystem 105
7. Einreise-/Ausreisesystem 117
8. Europäisches Reiseinformations- und -genehmigungssystem 128
9. Europäisches Strafregisterinformationssystem für Drittstaatsangehörige 143
10. Fazit 152

IV. Interoperabilität 157
1. Einleitung 157
2. Bedeutung des Begriffs «*Interoperabilität*» 157
3. Geschichtlicher Hintergrund 159
4. Entstehung der Interoperabilität 160
5. Ausgestaltung der Interoperabilität 164

6. Beteiligung der Schweiz 190
7. Fazit 193

V. Vereinbarkeit der Interoperabilität mit dem Grundrecht auf Datenschutz 197
1. Einleitung 197
2. Schutzbereich und Eingriff 199
3. Rechtfertigung des Eingriffs 207
4. Fazit 287

VI. Schlussbemerkungen 291
1. Kontext der Entstehungsgeschichte der Interoperabilität 291
2. Paradigmenwechsel im Datenmanagement von Informationssystemen 293
3. Ausblick 294

Curriculum Vitae 298

Inhaltsverzeichnis

Vorwort V

Inhaltsübersicht VII

Inhaltsverzeichnis IX

Literaturverzeichnis XVII

Materialienverzeichnis XXXIII

Abkürzungsverzeichnis XLV

Gesetzesverzeichnis LIII

I. Einleitung 1
1. Einführung in die Thematik 1
2. Ziel der Untersuchung 3
3. Aufbau der Arbeit im Überblick 5
4. Begriffsdefinitionen 6

II. Datenschutz als Grundrecht 9
1. Einleitung 9
2. Entwicklung und Grundgedanke des Datenschutzes 10
3. Verzahnung der Grundrechtsinstrumente 11
3.1. BV und EMRK 11
3.2. GRC und EMRK 11
3.3. BV und GRC 14
4. Datenschutzrechtlicher Gehalt von Art. 8 EMRK 18
4.1. Rechtliche Verankerung 18
4.2. Adressatenkreis und Grundrechtsträger der EMRK 19
4.3. Persönlicher und sachlicher Geltungsbereich 19
4.4. Positive Schutzpflichten 22
4.5. Eingriffe in den Schutzbereich 22
4.6. Rechtfertigung eines Eingriffs 24
4.6.1 Gesetzliche Grundlage 25
4.6.2 Spezifisches legitimes Ziel 28
4.6.3 Notwendigkeit in einer demokratischen Gesellschaft 29
4.7. Abgrenzung zu anderen Grundrechten 30
5. Informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV 31
5.1. Rechtliche Verankerung 31
5.2. Adressatenkreis und Grundrechtsträger der BV 32
5.3. Persönlicher und sachlicher Schutzbereich 32
5.4. Positive Schutzpflichten 34
5.5. Eingriffe in den Schutzbereich 35
5.6. Rechtfertigung eines Eingriffs 36
5.6.1 Gesetzliche Grundlage 36
5.6.2 Öffentliches Interesse resp. Grundrechtsschutz Dritter 38

5.6.3 Verhältnismässigkeit 38
5.6.4 Kerngehalt 39
5.7. Abgrenzung zu anderen Grundrechten 40
6. Schutz personenbezogener Daten gemäss Art. 8 GRC 42
6.1. Rechtliche Verankerung 42
6.2. Adressatenkreis und Grundrechtsträger der GRC 43
6.3. Persönlicher und sachlicher Schutzbereich 44
6.4. Positive Schutzpflichten 44
6.5. Eingriffe in den Schutzbereich 45
6.6. Rechtfertigung von Eingriffen 46
6.6.1 Gesetzliche Grundlage 48
6.6.2 Wesensgehalt 48
6.6.3 Zulässiger Beeinträchtigungsgrund 52
6.6.4 Verhältnismässigkeit 53
6.6.5 Zusätzliche Anforderungen gemäss Art. 8 Abs. 2 S. 1 GRC 55
6.7. Abgrenzung zu anderen Grundrechten 56
7. Gemeinsamkeiten und Unterschiede der Grundrechte 58
7.1. Schutzbereich und Eingriff 59
7.2. Positive Schutzpflichten 59
7.3. Rechtfertigungskriterien 60
7.4. Besonderes Kriterium: der Zweck 62
7.4.1 Relevanz für Art. 8 GRC 62
7.4.2 Relevanz für Art. 8 EMRK 64
7.4.3 Relevanz für Art. 13 Abs. 2 BV 65
7.5. Abgrenzung zu anderen Grundrechten 66
8. Fazit 67
III. EU-Informationssysteme 69
1. Einleitung 69
2. Schengener und Dubliner Zusammenarbeit 70
2.1. Schengener Zusammenarbeit 70
2.2. Dubliner Zusammenarbeit 73
3. Assoziierung der Schweiz an Schengen und Dublin 75
3.1. Geschichtlicher Hintergrund 75
3.2. Assoziierungsabkommen 76
3.3. Übernahme und Umsetzung von Weiterentwicklungen des Schengen/Dublin-Besitzstands 77
3.4. Beteiligungsrechte der Schweiz 80
3.5. Einheitliche Anwendung und Auslegung des Schengen/Dublin-Besitzstands 80
3.6. Beendigungsmechanismus 81
4. Schengener Informationssystem 82
4.1. Entstehung 82
4.2. Betrieb und Aufsicht 84
4.3. Beteiligung der Schweiz 85
4.4. Gespeicherte Daten 87
4.4.1 Ausschreibungskategorien 87
4.4.2 Datenkategorien 88
4.5. Zugriffsberechtigung 90

4.6. Ausgewählte Sicherheitsmassnahmen 92
4.6.1 Übermittlung von SIS-Daten an Drittstaaten und internationale Organisationen 92
4.6.2 Protokollierungspflicht 92
4.6.3 Rechte der betroffenen Personen 92
4.6.4 Haftung und Sanktionen 93
5. Eurodac-Datenbank 93
5.1. Entstehung 93
5.2. Betrieb und Aufsicht 94
5.3. Beteiligung der Schweiz 95
5.4. Gespeicherte Daten 97
5.5. Zugriffsberechtigung 98
5.5.1 Asylbehörden 98
5.5.2 Nationale Strafverfolgungsbehörden 99
5.5.3 Europol 101
5.6. Ausgewählte Sicherheitsmassnahmen 102
5.6.1 Übermittlung von Eurodac-Daten an Drittstaaten, internationale Organisationen und private Stellen 102
5.6.2 Protokollierungspflicht 102
5.6.3 Rechte der betroffenen Personen 102
5.6.4 Haftung und Sanktionen 103
5.7. Ausblick 104
6. Visa-Informationssystem 105
6.1. Entstehung 105
6.2. Betrieb und Aufsicht 108
6.3. Beteiligung der Schweiz 109
6.4. Gespeicherte Daten 110
6.5. Zugriffsberechtigung 111
6.5.1 Visum-, Asyl- sowie Grenzkontrollbehörden 111
6.5.2 Nationale Strafverfolgungsbehörden 113
6.5.3 Europol 114
6.6. Ausgewählte Sicherheitsmassnahmen 115
6.6.1 Übermittlung von VIS-Daten an Drittstaaten und internationale Organisationen 115
6.6.2 Protokollierungspflicht 115
6.6.3 Rechte der betroffenen Personen 115
6.6.4 Haftung und Sanktionen 116
6.7. Ausblick 116
7. Einreise-/Ausreisesystem 117
7.1. Entstehung 117
7.2. Betrieb und Aufsicht 119
7.3. Beteiligung der Schweiz 120
7.4. Gespeicherte Daten 121
7.5. Zugriffsberechtigung 123
7.5.1 Grenzkontroll-, Visum- sowie Einwanderungsbehörden 123
7.5.2 Nationale Strafverfolgungsbehörden 125
7.5.3 Europol 126

7.6. Ausgewählte Sicherheitsmassnahmen 127
7.6.1 Übermittlung von EES-Daten an Drittstaaten, internationale Organisationen und private Stellen 127
7.6.2 Protokollierungspflicht 127
7.6.3 Rechte der betroffenen Personen 127
7.6.4 Haftung und Sanktionen 128
8. Europäisches Reiseinformations- und -genehmigungssystem 128
8.1. Entstehung 128
8.2. Betrieb und Aufsicht 131
8.3. Beteiligung der Schweiz 133
8.4. Gespeicherte Daten 135
8.5. Zugriffsberechtigung 138
8.5.1 ETIAS-Zentralstelle und nationale ETIAS-Stellen 138
8.5.2 Migrations- und Grenzkontrollbehörden sowie Beförderungsunternehmen 139
8.5.3 Nationale Strafverfolgungsbehörden 140
8.5.4 Europol 141
8.6. Ausgewählte Sicherheitsmassnahmen 142
8.6.1 Übermittlung von ETIAS-Daten an Drittstaaten, internationale Organisationen und private Stellen 142
8.6.2 Protokollierungspflicht 142
8.6.3 Rechte der betroffenen Personen 142
8.6.4 Haftung und Sanktionen 143
9. Europäisches Strafregisterinformationssystem für Drittstaatsangehörige 143
9.1. Entstehung 143
9.2. Betrieb und Aufsicht 145
9.3. Beteiligung der Schweiz 146
9.4. Gespeicherte Daten 146
9.5. Zugriffsberechtigung 149
9.6. Ausgewählte Sicherheitsmassnahmen 150
9.6.1 Übermittlung von ECRIS-TCN-Daten an Drittstaaten, internationale Organisationen und private Stellen 150
9.6.2 Protokollierungspflicht 150
9.6.3 Rechte der betroffenen Personen 151
9.6.4 Haftung und Sanktionen 151
10. Fazit 152
IV. Interoperabilität 157
1. Einleitung 157
2. Bedeutung des Begriffs «*Interoperabilität*» 157
3. Geschichtlicher Hintergrund 159
4. Entstehung der Interoperabilität 160
5. Ausgestaltung der Interoperabilität 164
5.1. Gesetzliche Grundlage 164
5.2. Betroffene Informationssysteme 165
5.3. Interoperabilitätskomponenten 165
5.3.1 Europäisches Suchportal 165
5.3.2 Gemeinsamer Dienst für den Abgleich biometrischer Daten 167

5.3.3 Gemeinsamer Speicher für Identitätsdaten 169
5.3.3.1 Zugang zum CIR zwecks Identifizierungen 171
5.3.3.2 Zugang zum CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten 172
5.3.3.3 Abfrage des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten 172
5.3.4 Detektor für Mehrfachidentitäten 174
5.3.4.1 Weisse und gelbe Verknüpfungen 175
5.3.4.2 Grüne Verknüpfungen 176
5.3.4.3 Rote Verknüpfungen 177
5.3.4.4 Weisse Verknüpfungen 177
5.4. Ausgewählte Sicherheitsmassnahmen 178
5.4.1 Datensicherheit 178
5.4.1.1 Veränderung der Datenverwaltungsarchitektur 178
5.4.1.2 Bestimmungen zur Datensicherheit 179
5.4.2 Datenqualität 180
5.4.2.1 Allgemeine Problematik 180
5.4.2.2 Art und Weise der Erhebung der Daten 183
5.4.2.3 Bisherige Sicherheitsmassnahmen 184
5.4.2.4 Neue Sicherheitsmassnahmen 185
5.4.2.5 Effekt der Interoperabilität auf die Datenqualität 186
5.4.3 Aufsicht 187
5.4.4 Übermittlung an Drittstaaten, internationale Organisationen sowie private Stellen 188
5.4.5 Rechte der betroffenen Personen 188
5.4.6 Haftung und Sanktionen 189
6. Beteiligung der Schweiz 190
6.1. Übernahme und Umsetzung der EU-IOP-VO 190
6.2. Ausgestaltung der Interoperabilität in der Schweiz 190
7. Fazit 193
V. Vereinbarkeit der Interoperabilität mit dem Grundrecht auf Datenschutz 197
1. Einleitung 197
2. Schutzbereich und Eingriff 199
2.1. Persönlicher Schutzbereich 199
2.2. Sachlicher Schutzbereich 200
2.2.1 Personenbezogene Daten 200
2.2.1.1 Templates 201
2.2.1.2 Einmalige Kennnummer der Identitätsbestätigungsdatei 202
2.2.2 Datenbearbeitungen 203
2.3. Eingriff 204
2.3.1 Vorliegen eines Eingriffs 204
2.3.2 Schwere des Eingriffs 205
3. Rechtfertigung des Eingriffs 207
3.1. Gesetzliche Grundlage 207
3.2. Öffentliches Interesse 211
3.3. Kerngehalt 212

3.4. Verhältnismässigkeit 215
3.4.1 Europäisches Suchportal 217
3.4.1.1 Geeignetheit 217
3.4.1.2 Erforderlichkeit 217
3.4.1.3 Zumutbarkeit 218
3.4.2 Gemeinsamer Dienst für den Abgleich biometrischer Daten 220
3.4.2.1 Geeignetheit 220
3.4.2.2 Erforderlichkeit 220
3.4.2.3 Zumutbarkeit 222
3.4.3 Abfrage des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten 223
3.4.3.1 Geeignetheit 226
3.4.3.2 Erforderlichkeit 226
3.4.3.3 Zumutbarkeit 230
a) Funktion des Kaskadenmechanismus 230
b) Zugangsbedingungen 233
c) Weitere Sicherheitsmassnahmen 235
d) Für die Abfrage verwendete Daten 237
e) Umsetzung in der Schweiz 238
f) Bewertung 238
3.4.4 Zugang zum CIR zwecks Identifizierung 241
3.4.4.1 Geeignetheit 242
3.4.4.2 Erforderlichkeit 243
3.4.4.3 Zumutbarkeit 245
a) Zugangsbedingungen 245
b) Weitere Sicherheitsmassnahmen 247
c) (Weitere) Konkretisierungen im nationalen Recht 248
d) Eignung der Daten für die Abfrage 251
e) Umsetzung in der Schweiz 253
f) Abgrenzung zu Art. 22 EU-IOP-VO 254
g) Bewertung 258
3.4.5 Zugang zum CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten 260
3.4.5.1 Geeignetheit 261
3.4.5.2 Erforderlichkeit 261
3.4.5.3 Zumutbarkeit 262
a) Zugangsbedingungen 262
b) Verweis auf das System, aus dem die Daten stammen 262
c) Missbräuchliche Verwendung von erlangten Daten 263
d) Weitere Sicherheitsmassnahmen 264
e) Umsetzung in der Schweiz 264
f) Bewertung 265
3.4.6 Gemeinsamer Speicher für Identitätsdaten 266
3.4.6.1 Geeignetheit 266
3.4.6.2 Erforderlichkeit 266
3.4.6.3 Zumutbarkeit 267
a) Umfang der gespeicherten Daten 267
b) Erhöhtes Sicherheitsrisiko 268
c) Sicherheitsmassnahmen 268

d) Entwicklung zu einer omnipotenten Datenbank? 269
e) Bewertung 270
3.4.7 Detektor für Mehrfachidentitäten 271
3.4.7.1 Geeignetheit 271
3.4.7.2 Erforderlichkeit 272
3.4.7.3 Zumutbarkeit 273
a) Zweckerweiterung? 273
b) Datenqualität 274
c) Manuelle Verifizierung 274
d) Eignung von ETIAS-Daten für die Abfrage 275
e) Vereinfachung von Identitätsprüfungen 276
f) Vorgehensweise bei Identitätsbetrug 277
g) Weitere Sicherheitsmassnahmen 278
h) Speicherfrist 278
i) Bewertung 279
3.4.8 Ausgewählte Sicherheitsmassnahmen 280
3.4.8.1 Rechte der betroffenen Personen 280
a) Recht auf Information 280
b) Recht auf Auskunft, Berichtigung und Löschung 281
c) Web-Portal 282
3.4.8.2 Datenübermittlung an Dritte 283
3.4.8.3 Aufsicht 284
3.4.8.4 Haftung und Sanktionen 285
3.4.9 Bewertung 286
4. Fazit 287
VI. Schlussbemerkungen 291
1. Kontext der Entstehungsgeschichte der Interoperabilität 291
2. Paradigmenwechsel im Datenmanagement von Informationssystemen 293
3. Ausblick 294
Curriculum Vitae 298

Literaturverzeichnis

ALEGRE SUSIE/JEANDESBOZ JULIEN/VAVOULA NIOVI, European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection, Study for the LIBE Committee, PE 583.148, April 2017, <https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583148/IPOL_STU(2017)583148_EN.pdf> (zuletzt besucht am 07.03.2025).

ALBERS MARION, Informationelle Selbstbestimmung, Habil. HU Berlin, Baden-Baden 2005.

ALBRECHT JAN PHILIPP/JOTZO FLORIAN, Das neue Datenschutzrecht der EU. Grundlagen, Gesetzgebungsverfahren, Synopse, Baden-Baden 2017.

AMREIN MARCEL/DUBACH SARAH/FÜRST THIMON/GRILLET STÉPHANIE/GOTSCH NINA/KIEFER MICHAEL/STÄUBLI GIAN CARLI/STRUB PHILIPPE/TINNER ARIANE/ZBINDEN ANDREA/ZUMBÜHL NORA, Die sektoriellen Abkommen Schweiz–EU in der praktischen Anwendung, in: Epiney Astrid/Hehemann Lena (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2017/2018, Zürich/Bern 2018, 503–525 (zit. AMREIN, et al., sektorielle Abkommen 2018).

AMREIN MARCEL/MICHEL DANIEL/GRILLET STÉPHANIE/KIEFER MICHAEL/GOTSCH NINA/RAVASI ELISA/STÄUBLI GIAN CARLI/STRUB PHILIPPE/TINNER ARIANE/ZBINDEN ANDREA/ZUMBÜHL NORA, Die sektoriellen Abkommen Schweiz-EU in der praktischen Anwendung, in: Epiney Astrid/Hehemann Lena/Zlătescu Petru Emanuel (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2018/2019, Zürich/Bern 2019, 477–501 (zit. AMREIN, et al., sektorielle Abkommen 2019).

BAUMGARTNER ESTHER/BUSCH ROMAN/BÜSSER CHRISTINE/FERNÁNDES MARIA-ANNA/MAHNIG FABIAN/MÜLLER SEBASTIAN/SCHWENDIMANN THOMAS/SELMANI ZARIFE/ZIMMERMANN FRANCINE, Die sektoriellen Abkommen Schweiz – EU in der praktischen Anwendung, in: Epiney Astrid/Gammenthaler Nina (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2009/2010, Bern 2010, 417–444.

BAUR GEORGES, Datenschutz-Grundverordnung Schengen-relevant? Vielleicht nicht, aber …, in: Breitenmoser Stephan/Lagodny Otto/Uebersax Peter (Hrsg.), Schengen und Dublin in der Praxis. Aktuelle Herausforderungen, Zürich 2018.

BELSER EVA MARIA, Der grundrechtliche Rahmen des Datenschutzes, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011, 319–410 (zit. BELSER, grundrechtlicher Rahmen).

BELSER EVA MARIA, Zur rechtlichen Tragweite des Grundrechts auf Datenschutz. Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Epiney Astrid/Fasnacht Tobias/Blaser Gaëtan (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich 2013, 19–45 (zit. BELSER, rechtliche Tragweite).

Belser Eva Maria/Waldmann Bernhard, Grundrechte II. Die einzelnen Grundrechte, Zürich 2012.

Besson Samantha, L'adhésion de l'Union européenne à la Convention européenne des droits de l'homme après l'avis 2/13, in: Epiney Astrid/Kern Markus/Hehemann Lena (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2014/2015, Zürich/Bern 2015, 423–454.

Biaggini Giovanni, BV Kommentar. Bundesverfassung der Schweizerischen Eidgenossenschaft, 2. Aufl., Zürich 2017.

Blonski Dominika, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, Diss. Bern 2015.

Boehm Franziska, Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level, Diss. Luxemburg 2011, Berlin/Heidelberg 2012.

Bolz Susanne, «Dublin»: Nur mit Vorbehalt, Plädoyer 2005/1, 45–46.

Bossung Raphael, Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit in der EU. Umsetzungsrisiken und rechtsstaatliche Anforderungen, SWP Studie, April 2018, <https://www.swp-berlin.org/publications/products/studien/2018S04_bsg.pdf> (zuletzt besucht am 07.03.2025).

Breitenmoser Stephan/Drück Michael, Die polizeiliche Zusammenarbeit im Rahmen von Schengen, in: Kaddous Christine/Jametti Greiner Monique (Hrsg.), Accords bilatéraux II Suisse-UE et autres accords récents, Basel 2006, 357–388.

Breitenmoser Stephan/Jutzeler Michel, Schengen und Dublin im Mehrebenensystem, in: Breitenmoser Stephan/Lagodny Otto/Uebersax Peter (Hrsg.), Schengen und Dublin in der Praxis. Aktuelle Herausforderungen, Zürich 2018, 3–32.

Brkan Maja, In search of the concept of essence of EU fundamental rights through the prism of data privacy, Maastricht Faculty of Law Working Paper No. 2017-01, 16.01.2017, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2900281> (zuletzt besucht am 07.03.2025) (zit. Brkan, prism of data privacy).

Brkan Maja, The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection, in: Brkan Maja/Psychogiopoulou Evangelia (Hrsg.), Courts, privacy and data protection in the digital environment, Cheltenham (UK)/Northampton (MA, USA) 2017, 10–31 (zit. Brkan, Judge-made law).

Brkan Maja, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning, German Law Journal Volume 20 (2019) No. 6, 864–883 (zit. Brkan, essence).

Brkan Maja, Privacy, data protection and the role of European Courts: Towards judicialisation and constitutionalisation of European privacy and data protection framework, in: González Fuster Gloria/van Brakel Rosamunde/De Hert Paul (Hrsg.), Research handbook on privacy and data protection law. Values, norms and global politics, Cheltenham (UK)/Northampton (MA, USA) 2022, 274–302 (zit. Brkan, judicialisation and constitutionalisation).

Brouwer Evelien, A Point of No Return in Purpose Limitation? Interoperability and the Blurring of Migration and Crime, <https://migrationpolicycentre.eu/point-no-return-migration-and-crime/> (zuletzt besucht am 25.10.2023) (zit. Brouwer, A point of no return).

Brouwer Evelien Renate, Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation, in: Besselink Leonard F. M./Pennings Frans/Prechal Sacha (Hrsg.), The eclipse of the legality principle in the European Union, Alphen aan den Rijn 2011, 273–294 (zit. Brouwer, purpose limitation).

Brouwer Evelien Renate, Interoperability of Databases and Interstate Trust: a Perilous Combination for Fundamental Rights, <https://verfassungsblog.de/interoperability-of-databases-and-interstate-trust-a-perilous-combination-for-fundamental-rights/> (zuletzt besucht am 07.03.2025) (zit. Brouwer, Interoperability of Databases).

Callewaert Johan, vingt ans de coexistance entre la Charte et la Convention européenne des droits de l'homme : un bilan mitigé, Cahiers de droit européen 1/2021, 169–181.

Caroni Martina, Das neue Asylverfahren – ein Überblick, recht 2/2019, 85–94.

Caroni Martina/Scheiber Nicole/Preisig Christa/Plozza Monika, Migrationsrecht, 5. Aufl., Bern 2022.

Carrera Sergio, Towards interoperable justice, Interoperability and its asymmetry in access rights by EU digital citizens, <https://migrationpolicycentre.eu/towards-interoperable-justice/> (zuletzt besucht am 25.10.2023).

Cassani Ursula/Gless Sabine/Ludwiczak Glassey Maria/Wahl Thomas, Schweizerische Praxis zum Strafrecht im internationalen Umfeld (2018), SRIEL 3/2019, 419–459.

Colella Stéphanie U., La restriction des droits fondamentaux dans l'Union européenne. Notions, cadre et régime, Diss. Fribourg 2018, Brüssel 2019 (zit. Colella, restriction).

Colella Stéphanie U., La protection des données à caratère personnel dans la coopération Schengen : (ré-)concilier les pratiques suisses et de l'UE grâce aux droits fondamentaux ?, in: Breitenmoser Stephan/Uebersax Peter/Hilpold Peter (Hrsg.), Schengen und Dublin in der Praxis. In der EU, in der Schweiz und in einzelnen europäischen Staaten, mit einem Blick auf 70 Jahre Flüchtlingskonvention, Zürich/St. Gallen/Baden-Baden/Wien 2023, 399–419 (zit. Colella, protection).

Cornu Anne, Les aspects institutionnels des Accords d'association de la Suisse à Schengen et à Dublin, in: Kaddous Christine/Jametti Greiner Monique (Hrsg.), Accords bilatéraux II Suisse-UE et autres accords récents, Basel 2006, 207–244.

De Hert Paul/Gutwirth Serge, Interoperability of police databases within the EU: An accountable political choice?, International Review of Law, Computers & Technology Volume 20, Issue 1-2 (2006), 21–35 (zit. De Hert/Gutwirth, police databases).

De Hert Paul/Gutwirth Serge, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in: Gutwirth Serge/Poullet Yves/De Hert Paul/De Terwangne Cécile/Nouwt Sjaak (Hrsg.), Reinventing data protection?, Berlin 2009, 3–44 (zit. De Hert/Gutwirth, Case Law).

De Terwangne Cécile, Le droits fondamentaux à la vie privée et à la protection des données personnelles des migrants et des réfugiés, in: Turgis Sandrine (Hrsg.), Les données numériques des migrants et des réfugiés sous l'angle du droit européen, Rennes 2020, 97–116 (zit. De Terwangne, migrants et réfugiés).

De Terwangne Cécile, Privacy and data protection in Europe: Council of Europe's Convention 108+ and the European Unions's GDPR, in: González Fuster Gloria/van Brakel Rosamunde/De Hert Paul (Hrsg.), Research handbook on privacy and data protection law. Values, norms and global politics, Cheltenham(UK)/Northampton (MA, USA) 2022, 10–35 (zit. De Terwangne, Convention 108+ and GDPR).

Dimitrova Diana, Surveillance at the borders: Travellers and their data protection rights, in: González Fuster Gloria/van Brakel Rosamunde/De Hert Paul (Hrsg.), Research handbook on privacy and data protection law. Values, norms and global politics, Cheltenham (UK)/Northampton (MA, USA) 2022, 303–334.

Donatsch Andreas, Die Umsetzung der Menschenrechte (EMRK, IPBPR) in der Praxis – aus der Sicht eines ehemaligen schweizerischen Richters, in: Demko Daniela/Brudermüller Gerd/Seelmann Kurt (Hrsg.), Menschenrechte: Begründung – Bedeutung – Durchsetzung, Würzburg 2015, 185–196.

Edgar Timothy H., Beyond Snowden. Privacy, mass surveillance, and the struggle to reform the NSA, Washington D.C. 2017.

EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11. April 2017, <https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> (zuletzt besucht am 07.03.2025) (zit. EDPS, necessity).

EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19. Dezember 2019, <https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf> (zuletzt besucht am 07.03.2025) (zit. EDPS, Proportionality).

EHLERS DIRK/GERMELMANN CLASS FRIEDRICH (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 5. Aufl., Berlin 2023 (zit. VERFASSERIN, in: Ehlers-Kommentar-EuGR).

EHRENZELLER BERNHARD/EGLI PATRICIA/HETTICH PETER/HONGLER PETER/SCHINDLER BENJAMIN/SCHMID STEFAN G./SCHWEIZER RAINER J. (Hrsg.), Die schweizerische Bundesverfassung. St. Galler Kommentar, 4. Aufl., Zürich/St. Gallen/Genf 2023 (zit. VERFASSERIN, in: St. Galler Kommentar).

EISELE KATHARINA, Interoperabiltiy between EU information systems through the lens of impact assessment – what does the evidence say?, <https://migrationpolicycentre.eu/interoperability-eu-information-systems/> (zuletzt besucht am 25.10.2023) (zit. EISELE, impact assessment).

EISELE KATHARINA, Initial Appraisal of a European Commission Impact Assessment. Interoperability between EU information systems for security, border and migration management, EPRS, PE 615.649, Februar 2018, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/615649/EPRS_BRI(2018)615649_EN.pdf> (zuletzt besucht am 07.03.2025) (zit. EISELE, Initial Appraisal).

EJPD, Bericht EJPD zuhanden der GPK-EJPD/BK. Stand der Umsetzung von Schengen/Dublin 2020/21, 28. Mai 2021, <https://www.bj.admin.ch/bj/de/home/sicherheit/schengen-dublin/berichte.html> (zuletzt besucht am 07.03.2025) (zit. EJPD, GPK-Bericht 2021).

EJPD, Kurzbericht des EJPD zuhanden der GPK-EJPD/BK. Stand der Umsetzung von Schengen/Dublin 2021/22, 25. Mai 2022, <https://www.bj.admin.ch/bj/de/home/sicherheit/schengen-dublin/berichte.html> (zuletzt besucht am 07.03.2025) (zit. EJPD, GPK-Bericht 2022).

EJPD, Kurzbericht des EJPD zuhanden der GPK-EJPD/BK. Stand der Umsetzung von Schengen/Dublin 2022/23, 26. Mai 2023, <https://www.bj.admin.ch/bj/de/home/sicherheit/schengen-dublin/berichte.html> (zuletzt besucht am 07.03.2025) (zit. EJPD, GPK-Bericht 2023).

ENGEL DANIEL, Der Beitritt der Europäischen Union zur EMRK. Vom defizitären Kooperationsverhältnis zum umfassenden EMRK-Rechtsschutz durch den EGMR?, Tübingen 2015.

EPINEY ASTRID, Schengen, Dublin und die Schweiz, AJP 2002, 300–311 (zit. EPINEY, Schengen, Dublin).

EPINEY ASTRID, Zu ausgewählten Herausforderungen des Datenschutzrechts, in: Epiney Astrid/Theuerkauf Sarah (Hrsg.), Datenschutz in Europa und die Schweiz, Zürich/Basel/Genf 2006, 1–38 (zit. EPINEY, Herausforderungen).

EPINEY ASTRID, Zur Verbindlichkeit der EU-Grundrechte in der und für die Schweiz, in: Casasus Gilbert/Altermatt Bernhard (Hrsg.), 50 Jahre Engagement der Schweiz im Europarat 1963 – 2013. Die Schweiz als Akteur oder Zaungast der europäischen Integration?, Zürich 2013, 141–158 (zit. EPINEY, Verbindlichkeit).

Epiney Astrid, Staatliche Überwachung versus Rechtsstaat: Wege aus dem Dilemma?, AJP 2016, 1503–1515 (zit. Epiney, Überwachung).

Epiney Astrid, Rechtsschutz und Streitbeilegung im Bilateralen Recht. Zu den Implikationen eines Einbezugs des EuGH im Vergleich zum status quo, Jusletter vom 19. Dezember 2022 (zit. Epiney, Rechtsschutz).

Epiney Astrid/Meier Annekathrin/Theuerkauf Sarah, «Schengen»: Ein neuer Prüfstein für die Schweiz, Plädoyer 2005/1, 38–44.

Epiney Astrid/Metz Beate/Pirker Benedikt, Zur Parallelität der Rechtsentwicklung in der EU und in der Schweiz. Ein Beitrag zur rechtlichen Tragweite der «Bilateralen Abkommen», Zürich/Genf/Basel 2012.

Epiney Astrid/Nüesch Daniela/Rovelli Sophia, Datenschutzrecht in der Schweiz. Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Bern 2023.

Epiney Astrid/Pirker Benedikt, The Binding Effect of EU Fundamental Rights for Switzerland, in: Thouvenin Jean-Marc/Weiss Norman (Hrsg.), The Influence of Human Rights on International Law, Cham 2015, 229–243.

Epiney Astrid/Schleiss Yvonne, Völkerrecht; in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011, 53–118.

eu-LISA, Eurodac 2022 Annual Report, August 2023, <https://www.eulisa.europa.eu/sites/default/files/documents/Eurodac%20Annual%20Report%202022.pdf> (zuletzt besucht am 07.03.2025) (zit. eu-LISA, Eurodac 2022).

eu-LISA, Eurodac 2023 Annual Report, Dezember 2024, <https://www.eulisa.europa.eu/sites/default/files/documents/eurodac-annual-report-2023.pdf> (zuletzt besucht am 07.03.2025) (zit. eu-LISA, Eurodac report 2023).

eu-LISA, List of designated authorities which have access to data recorded in the Central System of Eurodac pursuant to Article 27(2) of Regulation (EU) No 603/2013, for the purpose laid down in Article 1(1) of the same Regulation, November 2024, <https://www.eulisa.europa.eu/sites/default/files/documents/2024-eurodac-loa.pdf> (zuletzt besucht am 07.03.2025) (zit. eu-LISA, Eurodac list of designated authorities 2024).

eu-LISA, Report on the technical functioning of the Visa Information System (VIS), August 2020, <https://www.eulisa.europa.eu/sites/default/files/documents/2019%20VIS%20Report.pdf> (zuletzt besucht am 07.03.2025) (zit. eu-LISA, VIS report 2020).

eu-LISA, Report on the technical functioning of the Visa information System (VIS), August 2022, <https://www.eulisa.europa.eu/sites/default/files/documents/2021%20VIS%20Report.pdf> (zuletzt besucht am 07.03.2025) (zit. eu-LISA, VIS report 2022).

EU-LISA, SIS, 2023 annual statistics, Mai 2024, <https://www.eulisa.europa.eu/sites/default/files/documents/SIS%202023%20Annual%20Statistics%20-%20Report.pdf> (zuletzt besucht am 07.03.2025) (zit. EU-LISA, SIS report 2023).

EU-LISA, Technical reports on the functioning of VIS as per Article 50(3) of the VIS Regulation and Article 17(3) of the VIS Decision, Mai 2018, <https://www.eulisa.europa.eu/sites/default/files/documents/2018%20VIS%20reports.pdf> (zuletzt besucht am 07.03.2025) (zit. EU-LISA, VIS report 2018).

EU-LISA, VIS Technical Report (2021-2023), August 2024, <https://www.eulisa.europa.eu/sites/default/files/documents/vis_2021-2023_report.pdf> (zuletzt besucht am 07.03.2025) (zit. EU-LISA, VIS report 2024).

Europäische Kommission, Bericht der Kommission an das Europäische Parlament und den Rat über die Evaluierung des Schengener Informationssystems der zweiten Generation (SIS II) nach den Artikeln 24 Absatz 5, 43 Absatz 3 und 50 Absatz 5 der Verordnung (EG) Nr. 1987/2006 in Verbindung mit Artikel 59 Absatz 3 und Artikel 66 Absatz 5 des Beschlusses 2007/533/JI, COM(2016) 880 final, 21.12.2016 (zit. Europäische Kommission, Bericht Evaluierung SIS II).

Europol, European Union Terrorism Situation and Trend Report (TE-SAT) 2016, Den Haag, 2016, <https://www.europol.europa.eu/cms/sites/default/files/documents/europol_tesat_2016.pdf> (zuletzt besucht am 07.03.2025) (zit. Europol, Terrorism Situation 2016).

Fiolka Gerhard/Stalder Leonie, Entwicklungen im Bereich der polizeilichen Zusammenarbeit 2017-2019; in: Epiney Astrid/Hehemann Lena/Zlătescu Petru Emanuel (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2018/2019, Zürich/Bern 2019, 163–186.

Flückiger Alexandre, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, in: AJP 2013, 837–864.

Forgó Nikolaus/Hänold Stefanie/Schütze Benjamin, The principle of Purpose Limitation and Big Data, in: Corrales Marcelo/Fenwick Mark/Forgó Nikolaus (Hrsg.), New technology, Big Data and the law, Singapur 2017, 17–42.

FRA, Under watchful eyes: biometrics, EU IT systems and fundamental rights, Luxemburg 2018, <http://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf> (zuletzt besucht am 07.03.2025) (zit. FRA, biometrics).

FRA, Right to information. Guide for authorities when taking fingerprints for Eurodac, Luxemburg 2019, <http://fra.europa.eu/sites/default/files/2021-12/fra-2020-guide-eurodac_en_3.pdf> (zuletzt besucht am 07.03.2025) (zit. FRA, Practical Guide Eurodac).

FRA, Gesichtserkennungstechnologien: grundrechtsrelevante Erwägungen im Rahmen der Strafverfolgung, 2022, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper_de.pdf> (zuletzt besucht am 07.03.2025) (zit. FRA, Gesichtserkennungstechnologien).

FRA/Europarat/EDSB, Handbuch zum europäischen Datenschutzrecht, Ausgabe 2018, <https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-de/format-PDF/source-101384707> (zuletzt besucht am 07.03.2025) (zit. FRA/Europarat/EDSB, Handbuch).

Gächter Thomas/Egli Philipp, Informationsaustausch im Umfeld der Sozialhilfe, Jusletter vom 6. September 2010.

Gächter Thomas/Werder Gregori, Einbettung ausgewählter Konzepte in das schweizerische Datenschutzrecht, in: Epiney Astrid/Fasnacht Tobias/Blaser Gaëtan (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich 2013, 87–111.

Gaudin Hélène, Le statut de la convention européenne des droits de l'Homme dans l'ordre juridique de l'Union européenne. Débats récurrents et questions à venir, RTDEur 1/2022, 27–38.

Glass Philip, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz. Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Diss. Basel 2016, Zürich/St.Gallen 2017.

Gloor Scheidegger Caroline, Datenschutz und Rechtsschutz bei SIS, Eurodac und VIS, in: Breitenmoser Stephan/Gless Sabine/Lagodny Otto (Hrsg.), Rechtsschutz bei Schengen und Dublin, Zürich/St. Gallen 2013, 119–152.

Gonin Luc/Bigler Olivier, Convention européenne des droits de l'homme (CEDH). Commentaire des articles 1 à 18 CEDH, Bern 2018.

Good Paul-Lukas, Die Schengen-Assoziierung der Schweiz, Diss. St. Gallen, Lachen 2010.

Grabenwarter Christoph, European Convention on Human Rights. Commentary, München, 2014.

Grabenwarter Christoph (Hrsg.), Europäischer Grundrechteschutz. Zugleich Band 2 der Enzyklopädie Europarecht, Baden-Baden 2021 (zit. VerfasserIn, in: Europäischer Grundrechteschutz).

Grabenwarter Christoph/Pabel Katharina, Europäische Menschenrechtskonvention. Ein Studienbuch, 7. Aufl., München/Basel/Wien 2021.

Groenendijk Kees, Nothing new under the sun? Interoperability of EU justice and home databases, <https://migrationpolicycentre.eu/interoperability-eu-justice-databases/> (zuletzt besucht am 25.10.2023).

Gruber Reto, Die Übernahme und Umsetzung von Weiterentwicklungen des Schengen-Besitzstands – ausgewählte institutionelle Aspekte, in: Epiney Astrid/Gammenthaler Nina (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2009/2010, Bern 2010, 479–509.

Guerra Clara, Interoperability and refugees from a data protection perspective, <https://migrationpolicycentre.eu/interoperability-refugees-data-protection/> (zuletzt besucht am 25.10.2023).

Gutheil Mirja/Liger Quentin/Eager James/Oviosu Yemi/Bogdanovic Daniel, Interoperability of Justice and Home Affairs Information Systems, Study for the LIBE Committee, PE 604.947, April 2018, <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf> (zuletzt besucht am 07.03.2025).

Gutzwiller Susanne, Komitologie und Gemischte Ausschüsse im Rahmen der Assoziierung der Schweiz an Schengen/Dublin, in: Kaddous Christine/Jametti Greiner Monique (Hrsg.), Accords bilatéraux II Suisse-UE et autres accords récents, Basel 2006, 245–266.

Heselhaus Sebastian/Nowak Carsten (Hrsg.), Handbuch der Europäischen Grundrechte, 2. Aufl., München 2020 (VerfasserIn, in: EU-Grundrechte-HdB).

Hruschka Constantin, Grundrechtsschutz in Dublin-Verfahren, in: Breitenmoser Stephan/Gless Sabine/Lagodny Otto (Hrsg.), Rechtsschutz bei Schengen und Dublin, Zürich/St. Gallen 2013, 153–184 (zit. Hruschka, Grundrechtsschutz).

Hruschka Constantin, Reformvorschläge zum Gemeinsamen Europäischen Asylsystem, ASYL 3/2023, 22–23 (zit. Hruschka, Reformvorschläge).

Hruschka Constantin/Frei Nula, Verantwortungsteilung im Dublin-Raum – aktueller Stand und Entwicklungsperspektiven, in: Breitenmoser Stephan/Uebersax Peter/Hilpold Peter (Hrsg.), Schengen und Dublin in der Praxis. In der EU, in der Schweiz und in einzelnen europäischen Staaten, mit einem Blick auf 70 Jahre Flüchtlingskonvention, Zürich/St. Gallen/Baden-Baden/Wien 2023, 554–571.

Hustinx Peter, The Reform of EU Data Protection: towards more effective and more consistent data protection across the EU, in: Epiney Astrid/Fasnacht Tobias (Hrsg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz, Zürich 2013, 15–22.

Jacobs Francis Geoffrey/White Robin C. A./Ovey Clare/Rainey Bernadette/McCormick Pamela, The European Convention on Human Rights, 8. Aufl., Oxford 2020.

Jarass Hans D., Charta der Grundrechte der Europäischen Union. Unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK: Kommentar, 4. Aufl., München 2021.

Jarass Hans D./Kment Martin, EU-Grundrechte, 2. Aufl., München 2019.

Jones Chris, Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status, November 2019, <https://www.statewatch.org/media/documents/analyses/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf> (zuletzt besucht am 07.03.2025).

Jorns Angela, Das Dublin-System: Die Assoziierung der Schweiz und die Konsequenzen für Asylsuchende, AJP 2009, 1589–1601.

Karpenstein Ulrich/Mayer Franz C. (Hrsg.), Konvention zum Schutz der Menschenrechte und Grundfreiheiten. Kommentar, 3. Aufl., München/Basel 2022 (zit. VerfasserIn, in: Karpenstein/Mayer, Kommentar EMRK).

Kellerbauer Manuel/Klamert Marcus/Tomkin Jonathan (Hrsg.), The EU Treaties and the Charter of Fundamental Rights. A Commentary. Volume I: Treaty on European Union and Charter of fundamental rights, 2. Aufl., Oxford 2024 (zit. VerfasserIn, in: Commentary EU Treaties and CFR).

Khennouf Laura, Brèves remarques sur le pacte migration et asile et le droit international public, Revue de l'Union européenne, N° 681, September 2024, 473-479.

Kiener Regina/Kälin Walter/Wyttenbach Judith, Grundrechte, 4. Aufl., Bern 2024.

Koehler Ulrich, Praxiskommentar zum Europäischen Asylzuständigkeitssystem. Dublin III-Verordnung/Durchführungsverordnung zur Dublin III-Verordnung/Eurodac-Verordnung/Europäisches Unterstützungsbüro für Asylfragen (EASO), Berlin/Wien 2018.

Kokott J./Sobotta C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law Volume 3 Issue 4 (2013), 222–228.

Koller Heinrich, Schengen/Dublin und die Bilateralen II – eine neue Dimension in der Integrationspolitik. Vom einheitlichen Wirtschafts- zum europäischen Sicherheitsraum, AJP 2005, 909–917.

Koning Merel Elise, The purpose and the limitiations of purpose limitation, Diss. Nijmegen 2020, <http://hdl.handle.net/2066/221665> (zuletzt besucht am 07.03.2025).

Kranenborg Herke, Google and the Right to Be Forgotten (Case C-131/12, Google Spain), EPDL 1/2015, 70–79.

Lemmens Paul/Piret Mathilde, The charter of fundamental rights of the european Union and the european convention on human rights, from the perspective of the european court of human rights, Cahiers de droit européen 1/2021, 183–210.

Lenz Carl Otto/Borchardt Klaus-Dieter (Hrsg.), EU-Verträge Kommentar. EUV – AEUV – GRCh, 6. Aufl., Köln/Wien 2013 (zit. VerfasserIn, in: Lenz/Borchardt, EU-Verträge Kommentar).

Lobsiger Adrian/Gloor Scheidegger Caroline, Rechtliche Fragen bei der Bearbeitung von Migrationsdaten, in: Breitenmoser Stephan/Lagodny Otto/Uebersax Peter (Hrsg.), Schengen und Dublin in der Praxis. Aktuelle Herausforderungen, Zürich 2018, 317–337.

Majcher Izabella, The Schengen-wide entry ban: how are non-citizens' personal data protected?, jems Volume 48 Issue 8 (2022), 1944–1960.

Matter Livia, Die Vorratsdatenspeicherung auf dem Prüfstand, sui-generis 2019, 257 ff.

Matz René Detlef, Europol. Datenschutz und Individualrechtsschutz im Hinblick auf die Anforderungen der EMRK, Diss. Mainz 2002, Aachen 2003.

Meyer Jürgen/Hölscheidt Sven (Hrsg.), Charta der Grundrechte der Europäischen Union, 6. Aufl., Baden-Baden/Bern/Wien 2024 (zit. VerfasserIn, in: NomosKommentar GRC).

Meyer-Ladewig Jens/Nettesheim Martin/von Raumer Stefan (Hrsg.), EMRK Europäische Menschenrechtskonvention. Handkommentar, 5. Aufl., Baden-Baden 2023 (zit. VerfasserIn, in: HK-EMRK).

Michéa Frédérique, Les finalités des systèmes d'information européens à vocation migratoire. L'Union européenne et la tentation du panoptique, in: Turgis Sandrine (Hrsg.), Les données numériques des migrants et des réfugiés sous l'angle du droit européen, Rennes 2020, 37–63.

Michl Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh — zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD Volume 41 Issue 6 (2017), 349–353.

Mitsilegas Valsamis/Vavoula Niovi, Databases, in: Mitsilegas Valsamis (Hrsg.), EU criminal law, Oxford/London/New York/New Delhi/Sydney 2022, 480–611.

Mohler Markus H.F., Die EU hat mit dem Kernbereich von «Schengen» und mit «Dublin» den Stresstest bisher nicht bestanden, Sicherheit & Recht 1/2016, 3–26 (zit. Mohler, Stresstest).

Mohler Markus H.F., Schengen- und Dublin-Weiterentwicklungen als rechtsstaatliche Herausforderung in der Schweiz, in: Breitenmoser Stephan/Uebersax Peter/Hilpold Peter (Hrsg.), Schengen und Dublin in der Praxis. In der EU, in der Schweiz und in einzelnen europäischen Staaten, mit einem Blick auf 70 Jahre Flüchtlingskonvention, Zürich/St. Gallen/Baden-Baden/Wien 2023, 3–40 (zit. Mohler, Herausforderung).

Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz. Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Aufl., Bern 2008.

Naef Tobias, Data Protection without Data Protectionism. The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law, Diss. Zürich, Cham 2023.

Nygård Ann-Charlotte, EU wide availability of personal data of third country nationals for migration and security purposes – the challenge of ensuring fundamental rights safeguards, <https://migrationpolicycentre.eu/eu-personal-data-third-country-nationals-for-migration-security/> (zuletzt besucht am 25.10.2023).

Oesch Matthias, Bilaterale Verträge Schweiz-EU und Verweise auf (allenfalls ungültige) EU-Rechtsakte, in: Epiney Astrid/Diezig Stefan (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2013/2014, Zürich/Bern 2014, 283–299 (zit. Oesch, Bilaterale Verträge).

Oesch Matthias, Grundrechte als Elemente der Wertegemeinschaft Schweiz-EU. Zur Auslegung der bilateralen Verträge, ZBl 115/2014, 171–202 (zit. Oesch, Grundrechte).

Oesch Matthias, Die bilateralen Abkommen Schweiz – EU und die Übernahme von EU-Recht, AJP 2017, 638–652 (zit. Oesch, bilaterale Abkommen).

Oesch Matthias, Europarecht. Band I: Grundlagen, Institutionen, Verhältnis Schweiz-EU, 3. Aufl., Bern 2024 (zit. Oesch, Europarecht).

Oesch Matthias, Schweiz – Europäische Union. Grundlagen, Bilaterale Abkommen, Autonomer Nachvollzug, Zürich 2020 (zit. Oesch, Schweiz-EU).

Oesch Matthias, Der EuGH und die Schweiz, Zürich 2023 (zit. Oesch, EuGH).

Oesch Matthias/Naef Tobias, EU-Grundrechte, der EuGH und die Schweiz, ZSR 2017, 117-144.

Oesch Matthias/Neier Christina, Die Komitologie im Unionsrecht und die Schweiz, in: Belser Eva Maria/Waldmann Bernhard (Hrsg.), Mehr oder weniger Staat? Festschrift für Peter Hänni zum 65. Geburtstag, Bern 2015, 59–72.

Parkin Joanna, The difficult road to the Schengen Information System II. The legacy of 'laboratories' and the cost for fundamental rights and the rule of law, April 2011, <https://www.ceps.eu/wp-content/uploads/2011/04/SIS_II_paper_liberty_security_formatted1.pdf> (zuletzt besucht am 07.03.2025).

Pirker Benedikt/Epiney Astrid, The Integration of Switzerland into the Framework of EU Law by Means of the 'Bilateral Agreements', in: Müller-Graff Peter-Christian/Mestad Ola (Hrsg.), The Rising Complexity of European Law, Berlin 2014, 39–66.

Probst Thomas, Die Verknüpfung von Personendaten und deren rechtliche Tragweite, in: Epiney Astrid/Probst Thomas/Gammenthaler Nina (Hrsg.), Datenverknüpfung. Problematik und rechtlicher Rahmen, Zürich 2011, 1–40.

Progin-Theuerkauf Sarah/Egbuna-Joss Andrea, Europäisches Asylrecht. Rechtsrahmen und Funktionsweise, Bern 2019.

Progin-Theuerkauf Sarah/Zoeteweij-Turhan Margarite/Turhan Ozan, Interoperabilität der Informationssysteme im Migrationsbereich – Digitale Grenzkontrollen 2019 in: Achermann Alberto/Boillet Véronique/Caroni Martina/Epiney Astrid/Künzli Jörg/Uebersax Peter (Hrsg.), Jahrbuch für Migrationsrecht 2018/2019, Bern 2019, 3–41.

PSYCHOGIOPOULOU EVANGELIA, The European Court of Human Rights, privacy and data protection in the digital era, in: Brkan Maja/Psychogiopoulou Evangelia (Hrsg.), Courts, privacy and data protection in the digital environment, Cheltenham (UK)/Northampton (MA, USA) 2017, 32–62.

QUINTEL TERESA, Why should we care about the Privacy of Asylum Seekers?, <https://migrationpolicycentre.eu/data-privacy-of-asylum-seekers/> (zuletzt besucht am 25.10.2023) (zit. QUINTEL, Privacy).

QUINTEL TERESA, Connecting personal data of Third Country Nationals: Interoperability of EU databases in the light of the CJEU's case law on data retention, University of Luxembourg Law Working Paper No. 002-2018, März 2018, <https://orbilu.uni.lu/handle/10993/35318> (zuletzt besucht am 07.03.2025) (zit. QUINTEL, data retention).

RAIMONDO GUILIA, The European Integrated Border Management. Frontex, Human Rights, and International Responsibility, Modern Studies in European Law, Volume 120, Oxford 2024.

RIEHLE CORNELIA, FRA Opinion on Interoperability, 22.06.2018, <https://eucrim.eu/news/fra-opinion-interoperability/> (zuletzt besucht am 07.03.2025).

RIEPL FRANK, Informationelle Selbstbestimmung im Strafverfahren. Diss. Tübingen 1998.

RUDIN BEAT, Datenschutzreform in der Schweiz: EU-Nachvollzug – idealistisch und realpolitisch, in: Breitenmoser Stephan/Lagodny Otto/Uebersax Peter (Hrsg.), Schengen und Dublin in der Praxis. Aktuelle Herausforderungen, Zürich 2018, 215–238.

RUSINOVA VERA, A European Perspective on Privacy and Mass Surveillance at the Crossroads, Higher School of Economics Research Paper No. WP BRP 87/LAW/2019, 06.03.2019, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347711> (zuletzt besucht am 07.03.2025).

SCHLEGEL STEFAN/AMMANN ODILE (Hrsg.), Onlinekommentar zur Bundesverfassung. <https://onlinekommentar.ch/de> (zuletzt besucht am 07.03.2025) (zit. VERFASSERIN, in: Onlinekommentar BV).

SCHWEIZER RAINER J., Wie das europäische Recht die schweizerische Rechtsordnung fundamental beeinflusst und wie die Schweiz darauf keine systematische Antwort findet, in: Epiney Astrid/Rivière Florence (Hrsg.), Auslegung und Anwendung von «Integrationsverträgen». Zur Übernahme des gemeinschaftlichen Besitzstandes durch Drittstaaten, insbesondere die Schweiz, Zürich/Basel/Genf 2006, 23–56 (zit. SCHWEIZER, europäisches Recht).

SCHWEIZER RAINER J., Zusammenwirken im Grundrechtsschutz durch den Europarat und durch die Europäische Union. Auswirkungen in einem assoziierten Staat, in: Spenlé Christoph André (Hrsg.), Die Europäische Menschenrechtskonvention und die nationale Grundrechtsordnung. Spannungen und gegenseitige Befruchtung, Basel 2007, 29–44 (zit. SCHWEIZER, Grundrechtsschutz).

Schweizer Rainer J., Das Recht auf eine wirksame Beschwerde in Schengen- und Dublin-Verfahren aus schweizerischer Sicht, in: Breitenmoser Stephan/Lagodny Otto/Uebersax Peter (Hrsg.), Schengen und Dublin in der Praxis. Aktuelle Herausforderungen, Baden-Baden/Wien/Zürich/St. Gallen 2018, 33–144 (zit. Schweizer, wirksame Beschwerde).

Schweizer Rainer J., Datenschutzrechte der betroffenen Personen in Schengen- und Dublin-Verfahren, Jusletter vom 3. September 2018 (zit. Schweizer, Datenschutzrechte).

Siemen Birte, Datenschutz als europäisches Grundrecht, Diss. Kiel, Berlin 2006.

Spescha Marc/Bolzli Peter/de Weck Fanny/Priuli Valerio, Handbuch zum Migrationsrecht, 4. Aufl., Zürich 2019.

Spescha Marc/Zünd Andreas/Bolzli Peter/Hruschka Constantin/de Weck Fanny (Hrsg.), Migrationsrecht. Kommentar: Schweizerisches Ausländer- und Integrationsgesetz (AIG), Asylgesetz (AsylG) und Freizügigkeitsabkommen (FZA) sowie Bürgerrechtsgesetz (BüG) mit weiteren Erlassen, 5. Aufl., Zürich 2019 (zit. VerfasserIn, in: Kommentar Migrationsrecht).

Stadelmann Joel, Fingerabdrücke, Biometrie, DNA-Tests bei der migrationsrechtlichen Zulassung. Was kann ausländischen Personen bei der migrationsrechtlichen Zulassung alles zugemutet werden?, Zürich 2018.

Stämpfli Sandra, Das Schengener Informationssystem und das Recht der informationellen Selbstbestimmung, Diss. Basel, Bern 2009.

Stengel Cornelia/Stäuble Luca, Vom Persönlichkeitsprofil zum Profiling mit hohem Risiko. Ein Beitrag zur Begriffsabgrenzung im Differenzbereinigungsverfahren für ein totalrevidiertes Datenschutzgesetz, Jusletter vom 20. Januar 2020.

Stern Klaus/Sachs Michael (Hrsg.), Europäische Grundrechte-Charta (GRCh). Kommentar, München 2016 (zit. VerfasserIn, in: Stern/Sachs-Kommentar-GRC).

Thür Hanspeter, Datenschutz im Ausländer- und Asylbereich, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, 943–972.

Tobler Christa, Zur Beteiligung der Schweiz an der Europäischen IT-Agentur, Jusletter vom 1. Oktober 2012, 1–15 (zit. Tobler, IT-Agentur).

Tobler Christa, Homogenität im Rechtsbestand der Schengen- und Dublin-Abkommen: Übernimmt die Schweiz im Assoziationsrahmen nicht notifiziertes Asyl- und Datenschutzrecht der EU?, SRIEL 2/2017, 211–226 (zit. Tobler, Homogenität).

Turgis Sandrine, Propos introductifs, in: Turgis Sandrine (Hrsg.), Les données numériques des migrants et des réfugiés sous l'angle du droit européen, Rennes 2020, 13–32.

Tzanou Maria, The fundamental right to data protection. Normative value in the context of counter-terrorism surveillance, Diss. EUI Florenz, Oxford 2017.

Vavoula Niovi, EU immigration databases under scrutiny. Towards the normalisation of surveillance of movement in an era of «Privacy Spring»?, in: Vermeulen Gert/Lievens Eva (Hrsg.), Data protection and privacy under pressure. Transatlantic tensions, EU surveillance, and big data, Antwerpen/Apeldoorn/Portland 2017, 215–248 (zit. Vavoula, EU immigration databases).

Vavoula Niovi, Interoperability of European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals' Privacy?, 08.07.2019, <https://eumigrationlawblog.eu/interoperability-of-european-centralised-databases-another-nail-in-the-coffin-of-third-country-nationals-privacy/> (zuletzt besucht am 07.03.2025) (zit. Vavoula, IOP Privacy).

Vavoula Niovi, Transforming Eurodac from 2016 to the New Pact. From the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration, ECRE Working Paper 13, Brüssel 2020, <https://ecre.org/wp-content/uploads/2021/01/ECRE-Working-Paper-Transforming-Eurodac-from-2016-to-the-New-Pact-January-2021.pdf> (zuletzt besucht am 07.03.2025) (zit. Vavoula, Transforming Eurodac).

Vavoula Niovi, Police Information Exchange. The future developments regarding Prüm and the API Directive, Study for the LIBE Committee, PE 658.542, September 2020, <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/658542/IPOL_STU(2020)658542_EN.pdf> (zuletzt besucht am 07.03.2025) (zit. Vavoula, Police Information Exchange).

Vavoula Niovi, Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?, European Public Law Volume 26 Issue 1 (2020), 131–156 (zit. Vavoula, Deathblow).

Vavoula Niovi, Consultation of EU Immigration Databases for Law Enforcement Purposes: A Privacy and Data Protection Assessment, European Journal of Migration and Law Volume 22 Issue 2 (2020), 139–177 (zit. Vavoula, Assessment).

Vavoula Niovi, Databases for Non-EU Nationals and the Right to Private Life. Towards a System of Generalised Surveillance of Movement?, in: Bignami Francesca (Hrsg.), EU Law in Populist Times. Crises and Prospects, Cambridge (UK)/New York (NY, USA) 2020, 227–266 (zit. Vavoula, Right to Private Life).

Vavoula Niovi, Interoperability of EU Information Systems in a 'Panopticon' Union: A Leap Towards Maximised Use of Third-Country Nationals' Data or a Step Backwards in the Protection of Fundamental Rights?, in: Mitsilegas Valsamis/Vavoula Niovi (Hrsg.), Surveillance and privacy in the digital age. European, transatlantic and global perspectives, London 2021, 159–195 (zit. Vavoula, Interoperability).

Vavoula Niovi, Immigration and Privacy in the Law of the European Union. The Case of Information Systems, Diss. QMUL London 2017, Leiden/Boston 2022 (zit. Vavoula, Immigration and Privacy).

VILLIGER MARK E., Handbuch der Europäischen Menschenrechtskonvention (EMRK). Mit besonderer Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in Schweizer Fällen, 3. Aufl., Zürich/Basel/Genf 2020.

VON GRAFENSTEIN MAXIMILIAN, The principle of purpose limitation in data protection laws. The risk-based approach, principles, and private standards as elements for regulating innovation, Diss. Hamburg 2017, Baden-Baden 2018.

WAGNER ECKART, The Integration of Schengen into the Framework of the European Union, Legal Issues of European Integration Volume 25 Issue 2 (1998), 1–60.

WAHL THOMAS, Data Protection Experts Give Critical Statement on Planned Interoperability, 29.06.2018, <https://eucrim.eu/news/data-protection-experts-give-critical-statement-planned-interoperability/> (zuletzt besucht am 07.03.2025) (zit. WAHL, Interoperability).

WAHL THOMAS, EU Creates New Central Database for Convicted Third Country Nationals, 10.09.2019, <https://eucrim.eu/news/eu-creates-new-central-database-convicted-third-country-nationals/> (zuletzt besucht am 07.03.25) (zit. WAHL, ECRIS-TCN).

WALDMANN BERNHARD/BELSER EVA MARIA/EPINEY ASTRID (Hrsg.), Bundesverfassung, Basel 2015 (zit. VERFASSERIN, in: BSK BV).

WP29, Working document on biometrics, WP 80, 1. August 2003, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf> (zuletzt besucht am 07.03.2025) (zit. WP29, Biometrics).

WP29, Opinion 03/2013 on purpose limitation, WP 203, 2. April 2013, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> (zuletzt besucht am 07.03.2025) (zit. WP29, Opinion purpose limitation).

WP29, Leitlinien für die Umsetzung des Urteils des Gerichtshofs der Europäischen Union in der Rechtssache C-131/12 «Google Spanien und Inc/Agencia Española de Protección de Datos (AEPD) und Mario Costeja González», WP 225, 26. November 2014, <https://ec.europa.eu/newsroom/article29/items/667236/en> (zuletzt besucht am 07.03.2025) (zit. WP29, Google Spain).

WÜGER DANIEL, Das für die Schengen- und die Dublin-Assoziierung massgebliche Recht: Publikation und Zugang, LeGes 24 (2013) 1, 63–87.

ZÜND ANDREAS, Grundrechtsverwirklichung ohne Verfassungsgerichtsbarkeit, AJP 2013, 1349–1357.

Materialienverzeichnis

Bundesamt für Migration, Erläuterungen zur Verordnung über das zentrale Visa-Informationssystem (C-VIS) und das nationale Visumsystem (ORBIS), Dezember 2013, <https://www.newsd.admin.ch/newsd/message/attachments/82848.pdf> (zuletzt besucht am 07.03.2025) (zit. Bundesamt für Migration, Erläuterungen C-VIS und ORBIS 2013).

Bundesamt für Polizei, Verordnung über die Interoperabilität zwischen den Schengen/Dublin-Informationssystemen. N-IOP-Verordnung, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, November 2021, <https://www.newsd.admin.ch/newsd/message/attachments/82848.pdf> (zuletzt besucht am 07.03.2025) (zit. Bundesamt für Polizei, Erläuternder Bericht N-IOP-Verordnung).

Bundesbeschluss vom 18. Dezember 2020 über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) (Weiterentwicklungen des Schengen-Besitzstands), AS 2021 365 (zit. Bundesbeschluss vom 18. Dezember 2020).

Bundesbeschluss vom 19. März 2021 über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2019/817 und (EU) 2019/818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Weiterentwicklungen des Schengen-Besitzstands), BBl 2021 674 (zit. Bundesbeschluss IOP).

Bundesbeschluss vom 21. Juni 2019 über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen zur Errichtung und Nutzung des Einreise- und Ausreisesystems (EES) (Verordnungen [EU] 2017/2226 und 2017/2225) (Weiterentwicklungen des Schengen-Besitzstands), AS 2021 732 (zit. Bundesbeschluss vom 21. Juni 2019).

Bundesrat, Botschaft über eine neue Bundesverfassung vom 20. November 1996, BBl 1997 I 1, 20. November 1996 (zit. Bundesrat, Botschaft BV 1996).

Bundesrat, Botschaft zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II»), BBl 2004 5965, 1. Oktober 2004 (zit. Bundesrat, Botschaft Bilaterale II).

Bundesrat, Botschaft zum Bundesbeschluss über die Genehmigung der Notenaustausche zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Rechtsgrundlagen zur Anpassung des Schengener Informationssystems (Weiterentwicklung des Schengen-Besitzstands), BBl 2007 8591, 14. November 2007 (zit. Bundesrat, Botschaft SIS 2007).

BUNDESRAT, Botschaft über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung und des Beschlusses über das Visa-Informationssystem (VIS) (Weiterentwicklungen des Schengen-Besitzstands), BBl 2009 4245, 29. Mai 2009 (zit. BUNDESRAT, Botschaft VIS).

BUNDESRAT, Botschaft über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) Nr. 603/2013 und (EU) Nr. 604/2013 (Weiterentwicklungen des Dublin/Eurodac-Besitzstands) (Weiterentwicklungen des Dublin/Eurodac-Besitzstands), BBl 2014 2675, 7. März 2014 (zit. BUNDESRAT, Botschaft Dublin-III-VO/Eurodac-VO).

BUNDESRAT, Botschaft zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen zur Errichtung und Nutzung des Einreise- und Ausreisesystems (EES) (Verordnungen [EU] 2017/2226 und 2017/2225; Weiterentwicklungen des Schengen-Besitzstands) und Änderung des Ausländer- und Integrationsgesetzes (AIG), BBl 2019 175, 21. November 2018 (zit. BUNDESRAT, Botschaft EES).

BUNDESRAT, Botschaft zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) (Weiterentwicklung des Schengen-Besitzstands) und zur Änderung des Bundesgesetzes über das Informationssystem für den Ausländer- und den Asylbereich, BBl 2020 3465, 6. März 2020 (zit. BUNDESRAT, Botschaft SIS 2020).

BUNDESRAT, Botschaft zur Genehmigung und Umsetzung des Notenaustauschs zwischen der Schweiz und der EU betreffend die Übernahme der Verordnung (EU) 2018/1240 über das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) (Weiterentwicklung des Schengen-Besitzstands) und zur Änderung des Ausländer- und Integrationsgesetzes (Unterstellung des Nachrichtendienstes des Bundes unter das Schengen-Datenschutzgesetz), BBl 2020 2885, 6. März 2020 (zit. BUNDESRAT, Botschaft ETIAS).

BUNDESRAT, Botschaft zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2019/817 und (EU) 2019/818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Weiterentwicklungen des Schengen-Besitzstands), BBl 2020 7983, 2. September 2020 (zit. BUNDESRAT, Botschaft IOP).

BUNDESRAT, Botschaft zur Genehmigung des Abkommens über die grenzüberschreitende Zusammenarbeit (Prümer Zusammenarbeit), des Eurodac-Protokolls zwischen der Schweiz und der EU, des Abkommens mit den Vereinigten Staaten über die Verhinderung und Bekämpfung schwerer Straftaten sowie zu deren Umsetzung (Anpassung des Strafgesetzbuchs, des DNA-Profil-Gesetzes, des Asylgesetzes und des Ausländer- und Integrationsgesetzes) und über einen Verpflichtungskredit für die Umsetzung des Programms Prüm Plus, BBl 2021 738, 5. März 2021 (zit. BUNDESRAT, Botschaft Prüm/Eurodac-Protokoll).

BUNDESRAT, Botschaft zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2021/1133 und (EU) 2021/1134 zur Reform des Visa-Informationssystems und der damit verbundenen Bedingungen für den Zugang zu anderen EU-Informationssystemen für VIS-Zwecke (Weiterentwicklungen des Schengen-Besitzstands) sowie zur Änderung des Ausländer- und Integrationsgesetzes (Zugriff auf den CIR und Zugang zu den Daten von drei EU-Informationssystemen), BBl 2022 1421, 18. Mai 2022 (zit. BUNDESRAT, Botschaft VIS Recast).

BUNDESRAT, Botschaft zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2021/1150 und (EU) 2021/1152 zur Festlegung der Bedingungen für den Zugang zu anderen EU-Informationssystemen für die Zwecke des Europäischen Reiseinformations- und –Genehmigungssystems (ETIAS) (Weiterentwicklungen des Schengen-Besitzstands) und zur Änderung des Ausländer- und Integrationsgesetzes, BBl 2022 1449, 18. Mai 2022 (zit. BUNDESRAT, Botschaft ETIAS Consequential Amendments).

EDSB, Kommentare zu der Mitteilung der Kommission über die Interoperabilität der europäischen Datenbanken, Brüssel 10. März 2006, <https://edps.europa.eu/sites/edp/files/publication/06-03-10_interoperability_de.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, Kommentare IOP 2006).

EDSB, Stellungnahme des Europäischen Datenschutzbeauftragten [vom 7. Oktober 2009] zum geänderten Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von «Eurodac» für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EG) Nr. (…/…) (zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist), und zum Vorschlag für einen Beschluss des Rates über die Beantragung eines Abgleichs mit Eurodac-Daten durch Strafverfolgungsbehörden der Mitgliedstaaten und Europol zu Strafverfolgungszwecken, ABl. C 92 vom 10.4.2010, S. 1 ff. (zit. EDSB, Stellungnahme Eurodac 2009).

EDSB, Stellungnahme des Europäischen Datenschutzbeauftragten zum geänderten Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von «EURODAC» für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. [.../...] [...] (Neufassung), 5. September 2012, <https://www.edps.europa.eu/sites/default/files/publication/12-09-05_eurodac_de.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, Stellungnahme Vorschlag Eurodac 2012).

EDPS, EDPS Opinion on the Second EU Smart Borders Package. Recommendations on the revised Proposal to establish an Entry/Exit System, Opinion 06/2016, 21. September 2016, <https://www.edps.europa.eu/sites/default/files/publication/16-09-21_smart_borders_en.pdf> (zuletzt besucht am 07.03.2025) (zit. EDPS, Opinion EES).

EDSB, Stellungnahme des Europäischen Datenschutzbeauftragten zum ersten Reformpaket zur Überarbeitung des Gemeinsamen Europäischen Asylsystems (Eurodac-Verordnung, Verordnung zur Einrichtung eines Europäischen Unterstützungsbüros für Asylfragen und Dublin-Verordnung). Stellungnahme 07/2016, 21. September 2016, <https://edps.europa.eu/sites/default/files/publication/16-09-21_ceas_opinion_de_0.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, Stellungnahme Reformpaket GEAS 2016).

EDSB, Stellungnahme des EDSB zu dem Vorschlag für ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS). Stellungnahme 3/2017, 7. März 2017, <https://edps.europa.eu/sites/default/files/publication/17-03-070_etias_opinion_de.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, Stellungnahme Vorschlag ETIAS).

EDSB, Stellungnahme des EDSB zur neuen Rechtsgrundlage für das Schengener Informationssystem. Stellungnahme 7/2017, 2. Mai 2017, <https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_de.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, SIS recast).

EDSB, Reflexionspapier zur Interoperabilität von Informationssystemen im Raum der Freiheit, der Sicherheit und des Rechts, 17. November 2017, <https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_de_0.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, Reflexionspapier IOP).

EDSB, Stellungnahme des EDSB zum Vorschlag für eine Verordnung über ECRIS-TCN. Stellungnahme 11/2017, 12. Dezember 2017, <https://edps.europa.eu/sites/edp/files/publication/17-12-12_opinion_ecris_tcn_2017_0542_de_1.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, Stellungnahme Vorschlag ECRIS-TCN).

EDSB, Stellungnahme 4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Grosssystemen der EU, 16. April 2018, <https://edps.europa.eu/sites/edp/files/publication/18-04-16_edps-opinion-on-interoperability_de.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, Stellungnahme Vorschläge EU-IOP-VO).

EDSB, Stellungnahme des EDSB zum neuen Migrations- und Asylpaket. Stellungnahme 9/2020, 30. November 2020, <https://edps.europa.eu/system/files/2021-03/20-11-30_opinion_new-pact-migration-asylum_de.pdf> (zuletzt besucht am 07.03.2025) (zit. EDSB, Stellungnahme Asyl- und Migrationspaket).

EU-LISA, Shared Biometric Matching Service (sBMS). Feasibility Study – final report, 2018, <https://www.eulisa.europa.eu/sites/default/files/documents/Shared%20Biometric%20Matching%20Service%20sBMS%20-%20Feasibility%20Study.pdf> (zuletzt besucht am 07.03.2025) (zit. EU-LISA, Feasibility Study sBMS).

EU-LISA, Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA. Summary of the Feasibility Study, 2019, <https://www.eulisa.europa.eu/sites/default/files/documents/eu-LISA%20Feasibility%20Study%20-%20Interoperability.pdf> (zuletzt besucht am 07.03.2025) (zit. EU-LISA, Feasibility Study Summary IOP).

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament und den Rat. Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht, KOM(2010)385 endg., 20. Juli 2010 (zit. KOM(2010)385 endg.).

Europäische Kommission, Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit, COM(2016) 205 final, 6. April 2016 (zit. COM(2016) 205 final).

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Aussengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung der Verordnung (EG) Nr. 767/2008 und der Verordnung (EU) Nr. 1077/2011, COM(2016) 194 final, 6. April 2016 (zit. Europäische Kommission, Vorschlag EES).

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der [Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist], für die Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten (Neufassung), COM(2016) 272 final, 4. Mai 2016 (zit. Europäische Kommission, Vorschlag Eurodac Neufassung 2016).

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist (Neufassung), COM(2016) 270 final, 4. Mai 2016 (zit. Europäische Kommission, Vorschlag Dublin-III-VO Neufassung 2016).

Europäische Kommission, Mehr Sicherheit in einer von Mobilität geprägten Welt: Besserer Informationsaustausch bei der Terrorismusbekämpfung und ein stärkerer Schutz der Aussengrenzen, COM(2016) 602 final, 14. September 2016 (zit. COM(2016) 602 final).

Europäische Kommission, Vorschlag für Verordnung des Europäischen Parlaments und des Rates über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/794 und (EU) 2016/1624, COM(2016) 731 final, 16. November 2016 (zit. Europäische Kommission, ETIAS-Vorschlag).

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat. Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Siebter Fortschrittsbericht, COM(2017) 261 final, 16. Mai 2017 (zit. COM(2017) 261 final).

Europäische Kommission, Bericht der Kommission an das Europäische Parlament und den Rat über den Austausch von Strafregisterinformationen zwischen den Mitgliedstaaten mittels des Europäischen Strafregisterinformationssystems (ECRIS), COM(2017) 341 final, 29. Juni 2017 (zit. COM(2017) 341 final).

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (TCN) vorliegen, sowie zur Ergänzung und Unterstützung des Europäischen Strafregisterinformationssystems (ECRIS) und zur Änderung der Verordnung (EU) Nr. 1077/2011 (ECRIS-TCN), COM(2017) 344 final, 29. Juni 2017 (zit. Europäische Kommission, Vorschlag ECRIS-TCN).

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Arbeitsprogramm der Kommission 2018. Agenda für ein enger vereintes, stärkeres und demokratischeres Europa, COM(2017) 650 final, 24. Oktober 2017 (zit. COM(2017) 650 final).

EUROPÄISCHE KOMMISSION, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Grenzen und Visa) und zur Änderung der Entscheidung 2004/512/EG des Rates, der Verordnung (EG) Nr. 767/2008, des Beschlusses 2008/633/JI des Rates, der Verordnung (EU)2016/399 und der Verordnung (EU)2017/2226, COM(2017) 793 final, 12. Dezember 2017 (zit. EUROPÄISCHE KOMMISSION, Vorschlag IOP-Grenze).

EUROPÄISCHE KOMMISSION, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration), COM(2017) 794 final, 12. Dezember 2017 (zit. EUROPÄISCHE KOMMISSION, Vorschlag IOP-Polizei).

EUROPÄISCHE KOMMISSION, Vorschlag für Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 767/2008, der Verordnung (EG) Nr. 810/2009, der Verordnung (EU) 2017/2226, der Verordnung (EU) 2016/399, der Verordnung (EU) 2018/XX [Interoperabilitäts-Verordnung] und der Entscheidung 2004/512/EG sowie zur Aufhebung des Beschlusses 2008/633/JI des Rates, COM(2018) 302 final, 16. Mai 2018 (zit. COM(2018) 302 final).

EUROPÄISCHE KOMMISSION, Geänderter Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von Eurodac für den Abgleich biometrischer Daten zum Zwecke der effektiven Anwendung der Verordnung (EU) XXX/XXX [Verordnung über Asyl und Migrationsmanagement] und der Verordnung (EU) XXX/XXX [Neuansiedlungsverordnung], für die Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnungen (EU) 2018/1240 und (EU) 2019/818, COM(2020) 614 final, 23. September 2020 (zit. EUROPÄISCHE KOMMISSION, Geänderter Vorschlag Eurodac Neufassung 2020).

EUROPÄISCHE KOMMISSION, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Ein neues Migrations- und Asylpaket, COM(2020) 609 final, 23. September 2020 (zit. COM(2020) 609 final).

EUROPÄISCHE KOMMISSION, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit («Prüm II») und zur Änderung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates sowie der Verordnungen (EU) 2018/1726, 2019/817 und 2019/818 des Europäischen Parlaments und des Rates, COM(2021) 784 final, 8. Dezember 2021 (zit. COM(2021) 784 final).

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Massnahmen für ein hohes Mass an Interoperabilität des öffentlichen Sektors in der Union (Gesetz für ein interoperables Europa), COM(2022) 720 final, 18. November 2022 (zit. COM(2022) 720 final).

European Commission, Communication from the Commission to the European Parliament and the Council. Smart borders – options and the way ahead, COM(2011) 680 final, 25. Oktober 2011 (zit. COM(2011) 680 final).

European Commission, Feasibility Study for a European Travel Information and Authorisation System (ETIAS). Final Report, Written by PwC, Luxemburg, 16. November 2016, <https://op.europa.eu/en/publication-detail/-/publication/b0a7efa5-ac91-11e6-aab7-01aa75ed71a1/language-en> (zuletzt besucht am 07.03.2025) (zit. European Commission, Feasibility Study ETIAS).

European Commission, Inception impact assessment. Interoperability of information systems for migration and security, 26. Juli 2017, <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1469-Interoperability-of-information-systems-for-migration-and-security_de> (zuletzt besucht am 07.03.2025) (zit. European Commission, Inception impact assessment IOP).

European Commission, Commission staff working document, Impact assessment. Accompanying the document Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), SWD(2017) 473 final, Part 1/2, 12. Dezember 2017 (zit. European Commission, Impact assessment IOP Part 1).

European Commission, Commission staff working document, Impact assessment. Accompanying the document Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), SWD(2017) 473 final, Part 2/2, 12. Dezember 2017 (zit. European Commission, Impact assessment IOP Part 2).

EUROPEAN COMMISSION, Feasibility Study of a Common Identity Repository (CIR). Final Report, Written by PwC, Luxemburg, Dezember 2017, <https://op.europa.eu/en/publication-detail/-/publication/f717e488-0c82-11e8-966a-01aa75ed71a1/language-en> (zuletzt besucht am 07.03.2025) (zit. EUROPEAN COMMISSION, Feasibility Study CIR).

FRA, The impact of the proposal for a revised Eurodac Regulation on fundamental rights. Opinion of the European Union Agency for Fundamental Rights, Wien, 22. Dezember 2016, <http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-opinion-06-2016-eurodac-0_en.pdf> (zuletzt besucht am 07.03.2025) (zit. FRA, Opinion Eurodac 2016).

FRA, Fundamental rights and the interoperability of EU information systems: borders and security, Mai 2017, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf> (zuletzt besucht am 07.03.2025) (zit. FRA, borders and security).

FRA, The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS). Opinion of the European Union Agency for Fundamental Rights, Wien, 30. Juni 2017, <http://fra.europa.eu/sites/default/files/fra_uploads/fra-opinion-02-2017-etias.pdf> (zuletzt besucht am 07.03.2025) (zit. FRA, Opinion proposed ETIAS).

FRA, Interoperability and fundamental rights implications. Opinion of the European Union Agency for Fundamental Rights, Wien, 11. April 2018, <http://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-01-2018-interoperability_en.pdf> (zuletzt besucht am 07.03.2025) (zit. FRA, Opinion IOP).

HLEG, Scoping Paper, Juni 2016, <https://www.statewatch.org/media/documents/news/2016/sep/eu-com-hleg-interoperability-info-systems-scoping-paper-6-16.pdf> (zuletzt besucht am 07.03.2025) (zit. HLEG, Scoping Paper).

HLEG, Interim Report, Dezember 2016, <https://www.statewatch.org/observatories/interoperability-eu-big-brother-database/official-documents/hleg/hleg-interim-report/> (zuletzt besucht am 25.10.2023) (zit. HLEG, Interim Report).

HLEG, final report, Mai 2017, <https://www.statewatch.org/media/documents/news/2017/may/eu-com-hleg-info-systems-interoperability-final-report-5-17.pdf> (zuletzt besucht am 07.03.2025) (zit. HLEG, final report).

MEIJERS COMMITTEE, Note on the proposal for a Regulation on the establishment of Eurodac (COM(2012)254), 10. Oktober 2012, CM1216, <https://www.statewatch.org/media/documents/news/2012/oct/eu-meijers-committee-eurodac-proposal.pdf> (zuletzt besucht am 07.03.2025) (zit. MEIJERS COMMITTEE, Vorschlag Eurodac 2012).

MEIJERS COMMITTEE, Note on the definition of third-country nationals in the Commission's ECRIS-TCN proposal, 2. Oktober 2017, CM1710, <https://www.commissie-meijers.nl/wp-content/uploads/2021/09/CM1710_EN.pdf> (zuletzt besucht am 07.03.2025) (zit. MEIJERS COMMITTEE, third country national ECRIS-TCN).

PRIVACY INTERNATIONAL, Privacy International response to consultation on the interoperability of EU information systems for borders and security, 7. November 2017, <https://privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20response%20to%20consultation%20on%20the%20interoperability%20of%20EU%20information%20systems%20for%20borders%20and%20security%20.pdf> (zuletzt besucht am 07.03.2025).

RAT DER EUROPÄISCHEN UNION, Schlussfolgerungen des Rates zum weiteren Vorgehen zur Verbesserung des Informationsaustauschs und zur Sicherstellung der Interoperabilität der EU-Informationssysteme, 10151/17, 8. Juni 2017 (zit. RAT DER EUROPÄISCHEN UNION, Schlussfolgerungen).

SEM, Erläuternder Bericht zu den Verordnungsanpassungen aufgrund der Übernahme der SIS-Verordnungen (EU) 2018/1860, 2018/1861 und 2018/1862 (Weiterentwicklungen des Schengen-Besitzstands) und der Anpassung des BGIAA zur Erstellung einer umfassenden Statistik im Rückkehrbereich, Oktober 2022, <https://www.sem.admin.ch/sem/de/home/sem/rechtsetzung/archiv/sis-vo-anpassungen.html> (zuletzt besucht am 07.03.2025) (zit. SEM, Erläuternder Bericht SIS Recast).

SFH, Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklungen des Schengen-Besitzstands). Vernehmlassungsantwort der Schweizerischen Flüchtlingshilfe, 9. Januar 2020, <https://www.fluechtlingshilfe.ch/fileadmin/user_upload/Publikationen/Vernehmlassungsantworten/200105-vernehmlassung-sfh-eu-vo-ipo-de.pdf> (zuletzt besucht am 07.03.2025) (zit. SFH, Vernehmlassungsantwort).

UN HIGH COMMISSIONER FOR REFUGEES, An efficient and protective Eurodac. UNHCR comments on the Commission's amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), November 2012, <https://www.unhcr.org/media/unhcr-comments-eu-rodac> (zuletzt besucht am 07.03.2025) (zit. UN HIGH COMMISSIONER FOR REFUGEES, Comment Eurodac 2012).

Verordnung über die Interoperabilität zwischen den Schengen/Dublin-Informationssystemen. (N-IOP-Verordnung), Vorentwurf, <https://www.newsd.admin.ch/newsd/message/attachments/69645.pdf> (zuletzt besucht am 07.03.2025) (zit. Vorentwurf N-IOP-Verordnung).

WP29, Stellungnahme 3/2005 zur Umsetzung der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, WP 112, 30. September 2012, <https://cnpd.public.lu/dam-assets/de/publications/groupe-art29/wp112_de.pdf> (zuletzt besucht am 07.03.2025) (zit. WP29, Pässe und Reisedokumente).

WP29, Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration, WP 266, 11. April 2018, <https://www.statewatch.org/media/documents/news/2019/aug/EU-Art-29-opinion-interoperability.pdf> (zuletzt besucht am 07.03.2025) (zit. WP29, Opinion proposals IOP).

Abkürzungsverzeichnis

Abs.	Absatz / Absätze
altEurodac-VO	Verordnung (EG) Nr. 2725/2000 (siehe Gesetzesverzeichnis)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union (siehe Gesetzesverzeichnis)
AFIS	*Automated Fingerprint Identification System* (automatisiertes Fingerabdruck-Identifizierungssystem)
AIG	Ausländer- und Integrationsgesetz (siehe Gesetzesverzeichnis)
AJP	Aktuelle juristische Praxis
API	*Advanced Passenger Information* (Fluggastdaten)
Art.	Artikel
AS	Amtliche Sammlung des Bundesrechts
ASYL	Schweizerische Zeitschrift für Asylrecht und -praxis
AsylG	Asylgesetz (siehe Gesetzesverzeichnis)
AsylV 3	Asylverordnung 3 (siehe Gesetzesverzeichnis)
Aufl.	Auflage
BAG	Bundesamt für Gesundheit
BAZG	Bundesamt für Zoll und Grenzsicherheit
BAZL	Bundesamt für Zivilluftfahrt
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
BGBl.	Bundesgesetzblatt
BGE	Entscheidungen des Schweizerischen Bundesgerichts (Amtliche Sammlung)
BGer	Schweizerisches Bundesgericht
BGIAA	Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich (siehe Gesetzesverzeichnis)
BJ	Bundesamt für Justiz
BMS	*Biometric Matching Service* (Gemeinsamer Dienst für den Abgleich biometrischer Daten)
BPI	Bundesgesetz über die polizeilichen Informationssysteme des Bundes (siehe Gesetzesverzeichnis)
BSK	Basler Kommentar

Bst.	Buchstabe
bspw.	beispielsweise
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft (siehe Gesetzesverzeichnis)
BVGE	Entscheid(e) des Schweizerischen Bundesverwaltungsgerichts
BVGer	Bundesverwaltungsgericht
bzw.	beziehungsweise
CEDH	*Convention européenne des droits de l'homme* (siehe EMRK)
CEPS	*Centre for European Policy Studies*
CFR	*Charter of Fundamental Rights* (siehe GRC)
CH	*Confoederatio Helvetica* (Schweizerische Eidgenossenschaft)
CIR	*Central Identity Repository* (Gemeinsamer Speicher für Identitätsdaten)
COM	*European Commission*
COVID-19	*coronavirus disease* 2019 (Coronavirus-Krankheit-2019)
CRRS	*Central repository for reporting and statistics* (Zentraler Speicher für Berichte und Statistiken)
C-VIS	Zentrales Visa-Informationssystem
DAA	Dublin-Assoziierungsabkommen (siehe Gesetzesverzeichnis)
D.C.	District of Columbia
Diss.	Dissertation
DNA	*deoxyribonucleic acid* (Desoxyribonukleinsäure)
DSG	Datenschutzgesetz (siehe Gesetzesverzeichnis)
DSGVO	VO 2016/679 (siehe Gesetzesverzeichnis)
DÜ	Dubliner Übereinkommen (siehe Gesetzesverzeichnis)
Dublin-II-VO	Verordnung (EG) Nr. 343/2003 (siehe Gesetzesverzeichnis)
Dublin-III-VO	Verordnung (EU) Nr. 604/2013 (siehe Gesetzesverzeichnis)
DuD	Datenschutz und Datensicherheit
E.	Erwägung
E-AIG	Entwurf zum Ausländer- und Integrationsgesetzes (BBl 2020 2065)
E-BPI	Entwurf zum Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BBl 2020 2065)

ECtHR	*European Court of Human Rights* (siehe EGMR)
EASO	*European Asylum Support Office* (Europäisches Unterstützungsbüro für Asylfragen)
ECHR	*European Convention on Human Rights* (siehe EMRK)
ECLI	*European Case Law Identifier* (Europäischer Rechtsprechungs-Identifikator)
ECRIS	*European Criminal Records Information System* (Europäisches Strafregisterinformationssystem)
ECRIS-TCN	*European Criminal Records Information System on Third-Country Nationals* (Europäisches Strafregisterinformationssystem für Drittstaatsangehörige)
ECRIS-TCN-VO	Verordnung 2019/816 (siehe Gesetzesverzeichnis)
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte
EDPL	*European Data Protection Law Review*
EDPS	*European Data Protection Supervisor* (siehe EDSB)
EDSB	Europäischer Datenschutzbeauftragter
EES	*Entry/Exit-System* (Einreise-/Ausreisesystem)
EESV	Verordnung über das Einreise- und Ausreisesystem (siehe Gesetzesverzeichnis)
EES-VO	Verordnung (EU) 2017/2226 (siehe Gesetzesverzeichnis)
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Europäische Menschrechtskonvention (siehe Gesetzesverzeichnis)
endg.	endgültig
EPRS	*European Parliamentary Reseach Service* (Wissenschaftlicher Dienst des Europäischen Parlaments)
ESP	*European Search Portal* (Europäisches Suchportal)
ETIAS	*European Travel Information and Authorization System* (Europäisches Reiseinformations- und -genehmigungssystem)
ETIAS-VO	VO 2018/1240 (siehe Gesetzesverzeichnis)
ErwG.	Erwägungsgrund / Erwägungsgründe

et. al.	*et alia*
etc.	*et cetera*
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EuGR	Europäische Grundrechte
EuGRZ	Europäische Grundrechte-Zeitschrift
EUI	*European University Institute*
eu-LISA	*European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice* (Europäische Agentur für das Betriebsmanagement von IT-Grosssystemen)
EU-IOP-VO	IOP-Grenze-VO und IOP-Polizei-VO
Eurodac	*European Asylum Dactyloscopy Database*
Eurodac-VO	Verordnung (EU) Nr. 603/2013 (siehe Gesetzesverzeichnis)
Eurojust	*European Union Agency for Criminal Justice Cooperation* (Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen)
Europol	*European Union Agency for Law Enforcement Cooperation* (Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung)
Europol-VO	VO 2016/794 (siehe Gesetzesverzeichnis)
EUV	Vertrag über die Europäische Union (siehe Gesetzesverzeichnis)
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
EZ fedpol	Einsatzzentrale fedpol
f. / ff.	folgende / fortfolgende
fedpol	Bundesamt für Polizei
FRA	*European Union Agency for Fundamental Rights* (Agentur der Europäischen Union für Grundrechte)
FRTD	*Facilitated Rail Transit Document* (Dokument für den erleichterten Transit im Eisenbahnverkehr)
FTD	*Facilitated Transit Document* (Dokument für den erleichterten Transit)
Frontex	Europäische Agentur für Grenz- und Küstenwache
FZA	Freizügigkeitsabkommen (siehe Gesetzesverzeichnis)

GEAS	Gemeinsames Europäisches Asylsystem
ggf.	gegebenenfalls
GPK	Geschäftsprüfungskommissionen
GRC	Charta der Grundrechte der Europäischen Union (siehe Gesetzesverzeichnis)
GRCh	siehe GRC
Habil.	Habilitation
HdB	Handbuch
HK	Handkommentar
HLEG	*High-level expert group on information systems and interoperability* (hochrangige Expertengruppe für Informationssysteme und Interoperabilität)
Hrsg.	Herausgeber
HU	Humboldt Universität Berlin
i.S.v.	im Sinne von
Interpol	*International Criminal Police Organization* (Internationale Kriminalpolizeiliche Organisation)
IOM	*International Organization for Migration* (Internationale Organisation für Migration)
IOP	Interoperabilität
IOP-Grenze-VO	VO 2019/817 (siehe Gesetzesverzeichnis)
IOP-Polizei-VO	VO 2019/818 (siehe Gesetzesverzeichnis)
IP	*Internet protocol* (Internetprotokoll)
IPBPR	Internationaler Pakt über bürgerliche und politische Rechte
jems	*Journal of Ethnic and Migration Studies*
JI	Justiz und Inneres
KOM	Kommission der Europäischen Union
LeGes	Mitteilungsblatt der Schweizerischen Gesellschaft für Gesetzgebung und der Schweizerischen Evaluationsgesellschaft
LIBE	*Committee on Civil Liberties, Justice and Home Affairs* (Ausschuss für bürgerliche Freiheiten, Justiz und Inneres)
lit.	*litera*
MA	*Massachusetts*
MID	*Multiple Identity Detector* (Detektor für Mehrfachidentitäten)

m.w.H.	mit weiteren Hinweisen
N	Randnote
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz (siehe Gesetzesverzeichnis)
N-ETIAS	Nationales ETIAS-System
No.	*number*
NSA	*National Security Agency*
N-SIS	nationaler Teil des Schengener Informationssystems
Nr.	Nummer
OFK	Orell Füssli Kommentar
ORBIS	nationales Visa-Informationssystem
PICUM	*Platform for International Cooperation on Undocumented Migrants* (Plattform für internationale Zusammenarbeit zu irregulären Migranten)
PNR	*Passenger Name Record* (erweiterte Fluggastdaten)
resp.	respektive
PwC	PricewaterhouseCoopers
QMUL	*Queen Mary University of London*
RL	Richtlinie
RTDEur	*Revue trimestrielle de droit européen*
Rz.	Randziffer
S.	Seite / Satz
SAA	Schengen-Assoziierungsabkommen (siehe Gesetzesverzeichnis)
SDÜ	Schengener Durchführungsübereinkommen (siehe Gesetzesverzeichnis)
SEM	Staatssekretariat für Migration
SEV	Sammlung Europäischer Verträge
SFH	Schweizerische Flüchtlingshilfe
SIRENE	*Supplementary Information Request at the National Entry*
SIS	*Schengen Information System* (Schengener Informationssystem)
SIS-II Beschluss	Beschluss 2007/533/JI (siehe Gesetzesverzeichnis)
SIS-II-Kfz-VO	Verordnung (EG) Nr. 1986/2006 (siehe Gesetzesverzeichnis)
SIS-II-VO	Verordnung (EG) Nr. 1987/2006 (siehe Gesetzesverzeichnis)

L

SIS-Grenze-VO	VO 2018/1861 (siehe Gesetzesverzeichnis)
SIS-Polizei-VO	VO 2018/1862 (siehe Gesetzesverzeichnis)
SIS-Rückkehr-VO	VO 2018/1860 (siehe Gesetzesverzeichnis)
SJZ	Schweizerische Juristen-Zeitung
SLTD	*Stolen and Lost Travel Documents* (Datenbank für gestohlene und verlorene Reisedokumente)
sog.	sogenannt(en) / sogenannte
SR	Systematische Rechtssammlung
SRIEL	*Swiss Review of International and European Law*
SÜ	Schengener Übereinkommen (siehe Gesetzesverzeichnis)
SWD	*Staff Working Document* (Arbeitsunterlage der Dienststellen)
SWP	Stiftung Wissenschaft und Politik
TDWAN	*Travel Documents Associated with Notices* (Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten)
TSI	Technische Spezifikationen für die Interoperabilität
u.a.	unter anderem
UAbs.	Unterabsatz
UK	*United Kingdom*
UMF	*Universal Message Format* (Universelles Nachrichtenformat)
UNHCR	*United Nations High Commissioner for Refugees* (Flüchtlingshochkommissariat der Vereinten Nationen)
UNO	*United Nations Organization*
u.U.	unter Umständen
USA	*United States of America* (Vereinigte Staaten von Amerika)
VEV	Verordnung über die Einreise und die Visumerteilung (siehe Gesetzesverzeichnis)
VerfBlog	Verfassungsblog
VG	Verantwortlichkeitsgesetz (siehe Gesetzesverzeichnis)
vgl.	vergleiche
VIS	*Visa Information System* (Visa-Informationssystem)
Visakodex	Verordnung (EG) Nr. 810/2009 (siehe Gesetzesverzeichnis)
VIS-Beschluss	Beschluss 2008/633/JI (siehe Gesetzesverzeichnis)

VIS SCG	*Visa Supervision Coordination Group* (Koordinierungsgruppe VIS)
VIS-VO	Verordnung (EG) Nr. 767/2008 (siehe Gesetzesverzeichnis)
VISV	Visa-Informationssystem-Verordnung (siehe Gesetzesverzeichnis)
VO	Verordnung
VwVG	Verwaltungsverfahrensgesetz (siehe Gesetzesverzeichnis)
WP29	*Article 29 Working Party* (Artikel-29-Datenschutzgruppe)
z.B.	zum Beispiel
ZBl	Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht
Zemis	Zentrales Migrationsinformationssystem
Ziff.	Ziffer
zit.	zitiert
ZSR	Zeitschrift für Schweizerisches Recht

Gesetzesverzeichnis

Abkommen Prüm CH-EU	Abkommen zwischen der Schweiz und der Europäischen Union zur Vertiefung der grenzüberschreitenden Zusammenarbeit (Prümer Zusammenarbeit), BBl 2021 742.
Abkommen CH-Europol	Abkommen vom 24. September 2004 zwischen der Schweizerischen Eidgenossenschaft und dem Europäischen Polizeiamt, SR 0.362.2.
AEUV	Vertrag über die Arbeitsweise der Europäischen Union (Konsolidierte Fassung), ABl. C 326 vom 26.10.2012, S. 47.
AIG	Bundesgesetz über die Ausländerinnen und Ausländer und über die Integration vom 16. Dezember 2005, SR 142.20.
AsylG	Asylgesetz vom 26. Juni 1998, SR 142.31.
AsylV 3	Asylverordnung 3 über die Bearbeitung von Personendaten vom 11. August 1999, SR 142.314.
Beschluss 1999/435/EG	Beschluss 1999/435/EG des Rates vom 20. Mai 1999 zur Bestimmung des Schengen-Besitzstands zwecks Festlegung der Rechtsgrundlagen für jede Bestimmung und jeden Beschluss, die diesen Besitzstand bilden, nach Massgabe der einschlägigen Bestimmungen des Vertrags zur Gründung der Europäischen Gemeinschaft und des Vertrags über die Europäische Union, ABl. L 239 vom 22.9.2000, S. 1.
Beschluss 1999/436/EG	Beschluss 1999/436/EG des Rates vom 20. Mai 1999 zur Festlegung der Rechtsgrundlagen für die einzelnen Bestimmungen und Beschlüsse, die den Schengen-Besitzstand bilden, nach Massgabe der einschlägigen Bestimmungen des Vertrags zur Gründung der Europäischen Gemeinschaft und des Vertrags über die Europäische Union, ABl. L 176 vom 10.7.1999, S. 17.
Beschluss 2007/533/JI	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. L 205 vom 7.8.2007, S. 63 (zit. SIS-II Beschluss).
Beschluss 2008/615/JI	Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl. L 210 vom 6.8.2008, S. 1.

Beschluss 2008/616/JI	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, ABl. L 210 vom 6.8.2008, S. 12.
Beschluss 2008/633/JI	Beschluss 2008/633/JI des Rates vom 23.06.2008 über den Zugang der benannten Behörden der Mitgliedstaaten von Europol zum Visa-Informationssystem für Datenabfragen zum Zweck der Verhütung, Aufdeckung und Ermittlung terroristischer und sonst schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008, S. 129 (zit. VIS-Beschluss).
Briefwechsel zur Komitologie	Abkommen vom 26. Oktober 2004 in Form eines Briefwechsels zwischen dem Rat der Europäischen Union und der Schweizerischen Eidgenossenschaft über die Ausschüsse, die die Europäische Kommission bei der Ausübung ihrer Durchführungsbefugnisse unterstützen, SR 0.362.1.
BPI	Bundesgesetz über die polizeilichen Informationssysteme des Bundes vom 13. Juni 2008, SR 361.
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.
DAA	Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags, SR 0.142.392.68.
DSG	Bundesgesetz über den Datenschutz vom 25. September 2020, SR 235.1.
DÜ	Übereinkommen über die Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat der Europäischen Gemeinschaften gestellten Asylantrags – Dubliner Übereinkommen, ABl. C 254 vom 19.8.1997, S. 1.
Durchführungsbeschluss 2013/115	Durchführungsbeschluss (EU) 2013/115/EU der Kommission vom 26. Februar 2013 über das SIRENE-Handbuch und andere Durchführungsbestimmungen für das Schengener Informationssystem der zweiten Generation (SIS II) (Bekannt gegeben unter Aktenzeichen C(2013) 1043), ABl. L 71 vom 13.3.2013, S. 1 (zit. SIRENE-Handbuch).

Durchführungsbeschluss 2023/201	Durchführungsbeschluss (EU) 2023/201 der Kommission vom 30. Januar 2023 zur Festlegung des Zeitpunkts, zu dem der Betrieb des Schengener Informationssystems gemäss der Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates aufgenommen wird, ABl. L 27 vom 31.1.2023, S. 29.
EESV	Verordnung über das Einreise- und Ausreisesystem vom 10. November 2021, SR 142.206.
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten, SR 0.101.
Entscheidung 2004/512/EG	Entscheidung 2004/512/EG des Rates vom 8.6.2004 zur Einrichtung des Visa-Informationssystems (VIS), ABl. L 213 vom 15.6.2004, S. 5.
Eurodac-Protokoll	Protokoll zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union, und dem Fürstentum Liechtenstein betreffend den Zugang zu Eurodac für Gefahrenabwehr- und Strafverfolgungszwecke, BBl 2021 743.
EUV	Vertrag über die Europäische Union (konsolidierte Fassung), ABl. C 326 vom 26.10.2012, S. 13.
FZA	Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits über die Freizügigkeit, SR 0.142.112.681.
GRC	Charta der Grundrechte der Europäischen Union, ABl. C 202 vom 7.6.2016, S. 389.
Komitologievereinbarung	Vereinbarung vom 22. September 2011 zwischen der Europäischen Union sowie der Republik Island, dem Fürstentum Liechtenstein, dem Königreich Norwegen und der Schweizerischen Eidgenossenschaft über die Beteiligung dieser Staaten an der Arbeit der Ausschüsse, die die Europäische Kommission bei der Ausübung ihrer Durchführungsbefugnisse in Bezug auf die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands unterstützen, SR 0.362.11.
Konvention 108	Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SEV Nr. 108.
Konvention 108+	Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SEV Nr. 223.

NDG	Bundesgesetz über den Nachrichtendienst vom 25. September 2015, SR 121.
Notenaustausch EES-VO	Notenaustausch vom 14. Februar 2018 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2017/2226 über ein Einreise-/Ausreisesystem (EES) und zur Änderung des Schengener Durchführungsübereinkommens sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011 (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.380.088.
Notenaustausch VO 2017/2225	Notenaustausch vom 14. Februar 2018 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2017/2225 zur Änderung der Verordnung (EU) 2016/399 in Bezug auf die Nutzung des Einreise-/Ausreisesystems (EES) (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.380.087.
Notenaustausch IOP-Grenze-VO	Notenaustausch vom 19. Juni 2019 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2019/817 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861, der Entscheidung 2004/512/EG und des Beschlusses 2008/633/JI (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.380.098.
Notenaustausch IOP-Polizei-VO	Notenaustausch vom 19. Juni 2019 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2019/818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.380.099.
Notenaustausch VO 2021/1133	Notenaustausch vom 11. August 2021 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2021/1133 zur Änderung der Verordnungen (EU) Nr. 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 und (EU) 2019/818 hinsichtlich der Festlegung der Voraussetzungen für den Zugang zu anderen Informationssystemen der EU für Zwecke des Visa-Informationssystems (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.381.019.

Notenaustausch VO 2021/1134	Notenaustausch vom 11. August 2021 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2021/1134 zur Änderung der Verordnungen (EG) Nr. 767/2008, (EG) Nr. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 und (EU) 2019/1896 und zur Aufhebung der Entscheidung 2004/512/EG und des Beschlusses 2008/633/JI zur Reform des Visa-Informationssystems (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.381.020.
Notenaustausch VO 2021/1150	Notenaustausch vom 11. August 2021 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2021/1150 zur Änderung der Verordnungen (EU) 2018/1862 und (EU) 2019/818 hinsichtlich der Festlegung der Bedingungen für den Zugang zu anderen EU-Informationssystemen für die Zwecke des Europäischen Reiseinformations- und -genehmigungssystems (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.381.017.
Notenaustausch VO 2021/1152	Notenaustausch vom 11. August 2021 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2021/1152 zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861 und (EU) 2019/817 hinsichtlich der Festlegung der Bedingungen für den Zugang zu anderen EU-Informationssystemen für die Zwecke des Europäischen Reiseinformations- und -genehmigungssystems (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.381.018.
N-SIS-Verordnung	Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro, SR 362.0.
Rahmenbeschluss 2002/584/JI	Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten, ABl. L 190 vom 18.7.2002, S. 1.
Rahmenbeschluss 2009/315/JI	Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten, ABl. L 93 vom 7.4.2009, S. 23.
RL 95/46/EG	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.95, S. 31 (zit. Datenschutzrichtlinie).

RL 2016/680	Richtlinie (EU) 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016, S. 89.
RL 2017/541	Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. L 88 vom 31.3.2017, S. 6.
RL 2019/884	Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS), sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates, ABl. L 151 vom 7.6.2019, S. 143.
RL 2006/24/EG	Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.4.2006, S. 54.
RL 2011/95/EU	Richtlinie 2011/95/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 über Normen für die Anerkennung von Drittstaatsangehörigen oder Staatenlosen als Personen mit Anspruch auf internationalen Schutz, für einen einheitlichen Status für Flüchtlinge oder für Personen mit Anrecht auf subsidiären Schutz und für den Inhalt des zu gewährenden Schutzes, ABl. L 337 vom 20.12.2011, S. 9 (zit. Qualifikationsrichtlinie).
RL 2013/32/EU	Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 zu gemeinsamen Verfahren für die Zuerkennung und Aberkennung des internationalen Schutzes, ABl. L 180 vom 29.6.2013, S. 60 (zit. Asylverfahrensrichtlinie).
RL 2013/33/EU	Richtlinie 2013/33/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Festlegung von Normen für die Aufnahme von Personen, die internationalen Schutz beantragen, ABl. L 180 vom 29.6.2013, S. 96 (zit. Aufnahmerichtlinie).

SAA	Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes, SR 0.362.31.
Saarbrücker Regierungsübereinkommen	Regierungsabkommen über den schrittweisen Abbau der Kontrollen an den Grenzen Frankreichs und der Bundesrepublik Deutschland, BGBl. 1984 II vom 13.7.1984, S. 767.
Schengen-Protokoll	Protokoll zur Einbeziehung des Schengen-Besitzstands in den Rahmen der Europäischen Union, ABl. C 340 vom 10.11.1997, S. 93.
SDÜ	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, ABl. L 239 vom 22.9.2000, S. 19.
SÜ	Übereinkommen 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, ABl. L 239 vom 22.9.2000, S. 13.
Verordnung (EG) Nr. 1986/2006	Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II), ABl. L 381 vom 28.12.2006, S. 1 (zit. SIS-II-Kfz-VO).
Verordnung (EG) Nr. 1987/2006	Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 381 vom 28.12.2006, S. 4 (zit. SIS-II-VO).
Verordnung (EG) Nr. 2725/2000	Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von «Eurodac» für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl. L 316 vom 15.12.2000, S. 1 (zit. altEurodac-VO).

Verordnung (EG) Nr. 343/2003	Verordnung (EG) Nr. 343/2003 des Rates vom 18. Februar 2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Mitgliedstaat gestellten Asylantrags zuständig ist, ABl. L 50 vom 25.2.2003, S. 1 (zit. Dublin-II-VO).
Verordnung (EG) Nr. 767/2008	Verordnung (EG) Nr. 767/2008 des Europäischen Parlament und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl. L 218 vom 13.8.2008, S. 60 (zit. VIS-VO).
Verordnung (EG) Nr. 810/2009	Verordnung (EG) Nr. 810/2009 des Europäischen Parlaments und des Rates über einen Visakodex der Gemeinschaft (Visakodex), ABl. L 243 vom 15.9.2009, S. 1 (zit. Visakodex).
Verordnung (EU) Nr. 1077/2011	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. L 286 vom 1.11.2011, S. 1.
Verordnung (EU) Nr. 603/2013	Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Grosssystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung), ABl. L 180 vom 29.6.2013, S. 1 (zit. Eurodac-VO).
Verordnung (EU) Nr. 604/2013	Verordnung (EU) Nr. 604/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist (Neufassung), ABl. L 180 vom 29.6.2013, S. 31 (zit. Dublin-III-VO).

VO 2016/399	Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) (kodifizierter Text), ABl. L 77 vom 23.3.2016, S. 1 (zit. Schengener Grenzkodex).
VO 2016/679	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), ABl. L 119 vom 4.5.2016, S. 1 (zit. DSGVO).
VO 2016/794	Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. L 135 vom 24.5.2016, S. 53.
VO 2017/2225	Verordnung (EU) 2017/2225 des Europäischen Parlaments und des Rates vom 30. November 2017 zur Änderung der Verordnung (EU) 2016/399 in Bezug auf die Nutzung des Einreise-/Ausreisesystems, ABl. L 327 vom 9.12.2017, S. 1.
VO 2017/2226	Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Aussengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011, ABl. L 327 vom 9.12.2017, S. 20 (zit. EES-VO).
VO 2018/1240	Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226, ABl. L 236 vom 19.9.2018, S. 1 (zit. ETIAS-VO).

VO 2018/1241	Verordnung (EU) 2018/1241 des Europäischen Parlaments und des Rates vom 12. September 2018 zur Änderung der Verordnung (EU) 2016/794 für die Zwecke der Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS), ABl. L 236 vom 19.9.2018, S. 72.
VO 2018/1806	Verordnung (EU) 2018/1806 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Aufstellung der Liste der Drittländer, deren Staatsangehörige beim Überschreiten der Aussengrenzen im Besitz eines Visums sein müssen, sowie der Liste der Drittländer, deren Staatsangehörige von dieser Visumpflicht befreit sind, ABl. L 303 vom 28.11.2018, S. 39.
VO 2018/1860	Verordnung (EU) 2018/1860 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger, ABl. L 312 vom 7.12.2018, S. 1 (zit. SIS-Rückkehr-VO).
VO 2018/1861	Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006, ABl. L 312 vom 7.12.2018, S. 14 (zit. SIS-Grenze-VO).
VO 2018/1862	Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission, ABl. L 312 vom 7.12.2018, S. 56 (zit. SIS-Polizei-VO).

VO 2019/816	Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726, ABl. L 135 vom 22.5.2019, S. 1 (zit. ECRIS-TCN-VO).
VO 2019/817	Verordnung (EU) 2019/817 vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27 (zit. IOP-Grenze-VO).
VO 2019/818	Verordnung (EU) 2019/818 vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816, ABl. L 135 vom 22.5.2019, S. 85 (zit. IOP-Polizei-VO).
VO 2021/1133	Verordnung (EU) 2021/1133 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EU) 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 und (EU) 2019/818 in Bezug auf die Festlegung der Bedingungen für den Zugriff auf andere EU-Informationssystem zu Visazwecken, ABl. L 248 vom 13.7.2021, S. 1.
VO 2021/1134	Verordnung (EU) 2021/1134 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EG) Nr. 767/2008, (EG) Nr. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 und (EU) 2019/1896 des Europäischen Parlaments und des Rates und zur Aufhebung der Entscheidung 2004/512/EG und des Beschlusses 2008/633/JI des Rates zur Reform des Visa-Informationssystems, ABl. L 248 vom 13.7.2021, S. 11.

VO 2021/1150	Verordnung (EU) 2021/1150 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EU) 2018/1862 und (EU) 2019/818 hinsichtlich der Festlegung der Bedingungen für den Zugang zu anderen EU-Informationssystemen für die Zwecke des Europäischen Reiseinformations- und -genehmigungssystems, ABl. L 249 vom 14.7.2021, S. 1.
VO 2021/1151	Verordnung (EU) 2021/1151 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EU) 2019/816 und (EU) 2019/818 hinsichtlich der Festlegung der Bedingungen für den Zugang zu anderen EU-Informationssystemen für die Zwecke des Europäischen Reiseinformations- und -genehmigungssystems, ABl. L 249 vom 14.7.2021, S. 7.
VO 2021/1152	Verordnung (EU) 2021/1152 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861 und (EU) 2019/817 hinsichtlich der Festlegung der Bedingungen für den Zugang zu anderen EU-Informationssystemen für die Zwecke des Europäischen Reiseinformations- und -genehmigungssystems, ABl. L 249 vom 14.7.2021, S. 15.
VO 2023/2667	Verordnung (EU) 2023/2667 des Europäischen Parlaments und des Rates vom 22. November 2023 zur Änderung der Verordnungen (EG) Nr. 767/2008, (EG) Nr. 810/2009 und (EU) 2017/2226 des Europäischen Parlaments und des Rates, der Verordnungen (EG) Nr. 693/2003 und (EG) Nr. 694/2003 des Rates und des Übereinkommens zur Durchführung des Übereinkommens von Schengen in Hinblick auf die Digitalisierung des Visumverfahrens, ABl. L, 2023/2667, 7.12.2023.
VO 2023/2685	Verordnung (EU) 2023/2685 des Europäischen Parlaments und des Rates vom 22. November 2023 zur Änderung der Verordnung (EG) Nr. 1683/95 des Rates im Hinblick auf die Digitalisierung des Visumverfahrens, ABl. L, 2023/2685, 7.12.2023.
VO 2024/982	Verordnung (EU) 2024/982 des Europäischen Parlaments und des Rates vom 13. März 2024 über die automatisierte Abfrage und den Austausch von Daten für die polizeiliche Zusammenarbeit und zur Änderung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates sowie der Verordnungen (EU) 2018/1726, (EU) 2019/817 und (EU) 2019/818 des Europäischen Parlaments und des Rates (Prüm-II-Verordnung), ABl. L, 2024/982, 5.4.2024.

VO 2024/1358	Verordnung (EU) 2024/1358 des Europäischen Parlaments und des Rates vom 14. Mai 2024 über die Einrichtung von Eurodac für den Abgleich biometrischer Daten zur effektiven Anwendung der Verordnungen (EU) 2024/1351 und (EU) 2024/1350 des Europäischen Parlaments und des Rates und der Richtlinie 2001/55/EG sowie zur Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten, zur Änderung der Verordnungen (EU) 2018/1240 und (EU) 2019/818 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates, ABl. L, 2024/1358, 22.5.2024.
Vertrag von Amsterdam	Vertrag von Amsterdam zur Änderung des Vertrags über die Europäische Union, der Verträge zur Gründung der Europäischen Gemeinschaften sowie einiger damit zusammenhängender Rechtsakte, ABl. C 340 vom 10.11.1997, S. 1.
VEV	Verordnung über die Einreise und die Visumerteilung vom 15. August 2018, SR 142.204.
VG	Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Behördenmitglieder und Beamten vom 14. März 1958, SR 170.32.
VISV	Verordnung über das Visa-Informationssystem und das nationale Visumsystem vom 18. Dezember 2013, SR 142.512.
VwVG	Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1986, SR 172.021.

I. Einleitung

1. Einführung in die Thematik

Mit dem Ziel der Abschaffung der Binnengrenzen wurde im Rahmen eines multilateralen Vertrags im Jahr 1985 der Schengen-Raum geschaffen. Einige Jahre später wurde – ebenfalls durch einen völkerrechtlichen Vertrag – die Dubliner Zusammenarbeit begründet. Mit dem Dubliner Übereinkommen sollte eine gewisse Vereinheitlichung des Asylbereichs erzielt werden. Sowohl die Schengener als auch die Dubliner Zusammenarbeit wurden schliesslich in den EU-Rechtsrahmen überführt. Abgesehen von den Mitgliedstaaten der EU partizipieren auch einige assoziierte Staaten, wie u.a. die Schweiz, an Schengen und Dublin.[1]

Im Schengen- resp. Dublin-Raum sind seit einigen Jahren drei Informationssysteme im Einsatz. So können im Schengener Informationssystem (*Schengen Information System*, SIS) verschiedene Ausschreibungen von Personen und Sachen vorgenommen werden. In der Eurodac-Datenbank werden insbesondere die Fingerabdruckdaten von asylsuchenden Personen registriert. Des Weiteren werden Daten von visumpflichtigen Personen aus Drittstaaten (also nicht Mitgliedstaaten der EU und nicht Schengen-assoziierte Staaten), die für einen kurzfristigen Aufenthalt in den Schengen-Raum einreisen wollen, im Visa-Informationssystem (*Visa Information System*, VIS) bearbeitet.[2]

Um die Daten von weiteren Personenkategorien bearbeiten zu können, plant die EU die Inbetriebnahme von drei weiteren Informationssystemen. So soll mit dem Einreise- und Ausreisesystem (*Exit/Entry System*, EES) das Abstempeln des Reisepasses von Drittstaatsangehörigen digitalisiert werden. Mit der Einführung des Europäischen Reiseinformations- und -genehmigungssystems (*European Travel Information and Authorization System*, ETIAS) werden bestimmte Personengruppen verpflichtet, vor ihrer Einreise in den Schengen-Raum eine Reisegenehmigung zu beantragen. Das Europäische Strafregisterinformationssystem für Drittstaatsangehörige (*European Criminal Record Information System for Third-country Nationals*, ECRIS-TCN) soll schliesslich

---

1 Siehe zur Schengener und Dubliner Zusammenarbeit Kapitel III.2. Siehe zur Assoziierung der Schweiz an Schengen und Dublin Kapitel III.3.

2 Siehe zu diesen Systemen ausführlich Kapitel III.4; III.5 und III.6.

dazu dienen, in Erfahrung zu bringen, ob eine Person in einem Mitgliedstaat der EU strafrechtlich verurteilt wurde.[3]

Abgesehen von diesen neuen Informationssystemen soll auch eine Verknüpfung zwischen den Datenbanken hergestellt werden. Das Bedürfnis nach der sog. Interoperabilität zwischen den EU-Informationssystemen entstand vor dem Hintergrund der Migrationskrise im Jahr 2015 sowie der Bedrohung durch terroristische Aktivitäten. Das dadurch erstarkte Bedürfnis nach Sicherheit machte neue Datenbearbeitungen möglich, um die Nutzung der Daten zu optimieren und die Ziele der Informationssysteme zu stärken. Die Interoperabilität bewirkt, dass bisher eigenständige Informationssysteme miteinander verknüpft werden. Vier (technische) Komponenten – das Europäische Suchportal (*European Search Portal*, ESP), der Dienst für den biometrischen Abgleich (*Biometric Matching System*, BMS), der gemeinsame Speicher für Identitätsdaten (*Common Identity Repository*, CIR) sowie der Detektor für Mehrfachidentitäten (*Multiple Identity Detector*, MID) – sollen diese Verknüpfung der Informationssysteme ermöglichen.[4] Aufgrund der Einführung von neuen Datenbearbeitungen sowie der verschiedenen Komponenten stellen sich im Zusammenhang mit der Interoperabilität vor allem datenschutzrechtliche Fragen.

Der Datenschutz ist in den gesetzlichen Grundlagen der Interoperabilität ein präsentes Thema. So wird z.B. im Zusammenhang mit der Wahrung der Grundrechte hervorgehoben, dass (neben dem Recht auf Achtung der Privatsphäre) der Schutz der personenbezogenen Daten uneingeschränkt gewahrt werden müsse.[5] Ähnlich wie auch die gesetzlichen Grundlagen der einzelnen Systeme widmen beide EU-Verordnungen, welche die Interoperabilität regeln, dem Datenschutz ein komplettes Kapitel.[6] Einerseits wird der Datenschutz in der gesetzlichen Grundlage der Interoperabilität selbst geregelt. Andererseits wird auch verschiedentlich auf datenschutzrechtliches EU-Sekundärrecht verwiesen. Dabei handelt es um die Verordnung 2016/679 (DSGVO), die im Strafverfolgungsbereich einschlägige Richtlinie (EU) 2016/680 sowie die für die EU-Organe anwendbare Verordnung (EU) 2018/1725.[7]

---

3 Siehe zu diesen Systemen ausführlich Kapitel III.7; III.8 und III.9.

4 Siehe zur Interoperabilität ausführlich Kapitel IV.

5 Siehe dazu Art. 5 EU-IOP-VO. Siehe ferner auch die Hervorhebung im Vergleich mit anderen Grundrechten in ErwG. 9 EU-IOP-VO.

6 Siehe dazu Kapitel VII EU-IOP-VO. Als Beispiel bei den Informationssystemen siehe Kapitel XII ETIAS-VO.

7 Siehe zu diesen Verweisen z.B. Art. 46 ff. EU-IOP-VO. Diese EU-Sekundärrechtsakte sehen verschiedene Datenschutzregime vor. Teilweise ist nicht klar, welches anwendbar ist. Siehe dazu QUINTEL, data retention, 16. Für die Abgrenzung dieser Regime ist auf den ver-

2. Ziel der Untersuchung

Da sich die Interoperabilität auf die Systemarchitektur der von dieser Verknüpfung betroffenen Informationssysteme auswirkt und neue (systemübergreifende) Abfragen ermöglicht werden, stellt sich insbesondere die Frage, ob dadurch der in verschiedenen Grundrechtsinstrumenten verankerte Datenschutz noch gewährleistet werden kann.[8]

Im Folgenden wird deshalb der Frage nachgegangen, ob die Interoperabilität der EU-Informationssysteme mit dem grundrechtlich geschützten Datenschutz vereinbar ist. Im Vordergrund steht dabei die Perspektive der Schweiz.[9]

Gemäss dieser Fragestellung steht also die Verknüpfung der Informationssysteme im Fokus. Inwiefern die von der Interoperabilität umfassten Informationssysteme den datenschutzrechtlichen Vorgaben entsprechen, ist somit nicht Gegenstand der vorliegenden Untersuchung. Für das bessere Verständnis der Ausgestaltung sowie des Ausmasses der Interoperabilität werden die für die Interoperabilität relevanten Systeme jedoch in einem eigenen Kapitel einzeln dargestellt.[10]

Als Grundlage für die Prüfung der Vereinbarkeit der Interoperabilität mit dem Datenschutz werden drei Grundrechtsinstrumente berücksichtigt.[11] Dabei

folgten Zweck abzustellen und nicht auf die bearbeitende Behörde. Vgl. dazu CASSANI, et al., 455 ff. Des Weiteren ist zu beachten, dass nicht alle relevanten EU-Sekundärrechtsakte für die Schweiz verbindlich sind. Dies hat zur Konsequenz, dass für die Schweiz eine andere gesetzliche Grundlage als für die Mitgliedstaaten gilt. Siehe dazu COLELLA, protection, 404 ff. m.w.H.

8 Die Interoperabilität kann sich auch auf andere Grundrechte auswirken. Siehe dazu FRA, borders and security; HLEG, final report, 43 ff.; FRA, Opinion IOP, 13 ff.; WP29, Opinion proposals IOP, 17 f.; NYGÅRD. Dem Aspekt der Nichtdiskriminierung wurde vereinzelt in den EU-IOP-VO Ausdruck verliehen. Siehe dazu die horizontale Klausel in Art. 5 EU-IOP-VO sowie Art. 18 Abs. 5 EU-IOP-VO. In der Folgenabschätzung werden zudem auch Vorteile der Interoperabilität für weitere Grundrechte aufgezeigt, so wie bspw. bei der Suche nach vermissten Kindern. Siehe dazu EUROPEAN COMMISSION, Impact assessment IOP Part 1, 33 f. Der Einfluss der Interoperabilität auf diese Grundrechte ist jedoch nicht Bestandteil dieser Untersuchung.

9 Siehe dazu Kapitel V.

10 Siehe zu den Informationssystemen Kapitel III.4; III.5; III.6; III.7; III.8 und III.9.

11 Ausdrücklich nicht näher betrachtet wird der Rechtsrahmen der Vereinten Nationen. Siehe für weitere Hinweise dazu FRA/EUROPARAT/EDSB, Handbuch, 25 f. Des Weiteren wird auch nicht auf die als Konvention 108 bekannte Datenschutzkonvention des Europarats resp. das Änderungsprotokoll, welches als Konvention 108+ bekannt ist, eingegangen. Dieses Instrument des Europarats stellt zwar das einzige rechtsverbindliche Instrument im Bereich des Datenschutzes dar. Die Konvention untersteht aber nicht der richterlichen

handelt es sich u.a. um die Charta der Grundrechte der EU (GRC). Auf dieses Grundrechtsinstrument nehmen die zwei EU-Verordnungen (im Folgenden EU-IOP-VO genannt) explizit Bezug.[12] Davon abgesehen ist auch zu berücksichtigen, dass die Mitgliedstaaten der EU, an welche sich die EU-IOP-VO primär richten, ebenfalls die Europäische Menschenrechtskonvention (EMRK) ratifiziert haben. Aus Sicht der EU-Mitgliedstaaten hat die Interoperabilität also auch diesem Grundrechtsinstrument zu entsprechen.[13] Des Weiteren richten sich die EU-IOP-VO, als sog. Schengen-Weiterentwicklungen, nicht nur an die EU-Mitgliedstaaten, sondern auch an die an Schengen-assoziierten Staaten, wie u.a. die Schweiz.[14] Die nationale Regelung der Interoperabilität in der Schweiz wird berücksichtigt, sofern die EU-rechtlichen Vorgaben den Schengen-Staaten Umsetzungsspielraum belassen. Da die Schweizerische Bundesverfassung (BV) ebenfalls grundrechtliche Gewährleistungen zum Datenschutz enthält, erscheint folglich auch dieses Grundrechtsinstrument für die vorliegende Fragestellung unter Berücksichtigung der gewählten Perspektive der Schweiz einschlägig.

Diese Grundrechtsinstrumente weisen teilweise einen engen Bezug zueinander auf.[15] Es ist deshalb wenig erstaunlich, dass der datenschutzrechtliche Gehalt dieser drei Grundrechtsinstrumente (also von Art. 8 GRC, Art. 13 Abs. 2 BV sowie Art. 8 EMRK) sehr ähnlich ausgestaltet ist. Es bietet sich deshalb für die vorliegende Fragestellung an, den datenschutzrechtlichen Gehalt dieser Grundrechtsinstrumente als ein Grundrecht (nämlich das Grundrecht auf Datenschutz) zusammenzufassen und als Grundlage für die Prüfung der Vereinbarkeit heranzuziehen.

Explizit nicht von der Fragestellung umfasst ist die Frage nach einem möglichen Rechtsschutz.

Aufsicht durch den EGMR. Dieser nimmt in seinen Urteilen jedoch teilweise dennoch darauf Bezug. Siehe dazu z.B. EGMR, Urteil v. 25.02.1997, *Z v. Finland*, Beschwerde Nr. 22009/93, Rz. 95. Siehe für weitere Hinweise zur Konvention 108 FRA/Europarat/EDSB, Handbuch, 28 ff.; Epiney/Nüesch/Rovelli, 14 ff. Siehe zu den Gemeinsamkeiten und Unterschieden betreffend die Konvention 108+ sowie die VO 2016/679 (DSGVO) De Terwangne, Convention 108+ and GDPR, 10 ff.

12 Siehe dazu ErwG. 40 EU-IOP-VO.

13 Wie sich im Folgenden noch genauer zeigen wird, stehen die GRC und die EMRK in einem engen Verhältnis. Siehe dazu Kapitel II.3.2.

14 Siehe zur Beteiligung der Schweiz an der Interoperabilität Kapitel IV.6.

15 Siehe zum Verhältnis dieser Grundrechtsinstrumente zueinander Kapitel II.3.

3. Aufbau der Arbeit im Überblick

Im Anschluss an die Einleitung wird in Kapitel II der Datenschutz als Grundrecht ausführlich erarbeitet und dargelegt. Dabei steht der datenschutzrechtliche Gehalt von Art. 8 EMRK, Art. 13 Abs. 2 BV und Art. 8 GRC im Fokus. Dieses Kapitel beginnt mit einleitendenden Bemerkungen zum Grundgedanken des Datenschutzes. Ausserdem wird das Verhältnis der drei Grundrechtsinstrumente zueinander diskutiert. Danach werden die Schutzbereiche der einzelnen, vorgenannten Grundrechte abgesteckt und mögliche Rechtfertigungsgründe für Eingriffe in diese Schutzbereiche erläutert. Das Kapitel schliesst mit einem punktuellen Vergleich dieser drei Grundrechte, in welchem insbesondere die relevanten Gemeinsamkeiten und Unterschiede herausgearbeitet werden.

In Kapitel III werden, nach einigen allgemeinen Ausführungen zur Schengener und Dubliner Zusammenarbeit sowie der entsprechenden Assoziierung der Schweiz, die von der Interoperabilität betroffenen Informationssysteme vorgestellt. Es werden verschiedene Aspekte wie u.a. die Anwendungsbereiche, die gespeicherten Daten, der Betrieb, die zugriffsberechtigten Personen sowie die Rechte der von der Datenbearbeitung betroffenen Personen näher erläutert. Dabei wird auch auf die jeweilige Ausgestaltung dieser Systeme in der Schweiz eingegangen. Da verschiedene Aspekte der Informationssysteme gleich oder zumindest ähnlich geregelt sind, kann dieses Kapitel teilweise repetitiv wirken. Dies wird bewusst in Kauf genommen. Jedes von der Interoperabilität betroffene System wird in diesem Kapitel unabhängig voneinander dargestellt. So wird es der Leserschaft ermöglicht, sich über jedes einzelne System umfassend zu informieren.

In Kapitel IV wird ausführlich auf die Entstehung sowie die Ausgestaltung der Interoperabilität eingegangen. Nach einer kurzen Erläuterung der Definition des Begriffs «*Interoperabilität*» liegt der Fokus in diesem Kapitel insbesondere auf den vier (technischen) Komponenten, mit welchen die Verknüpfung der einzelnen Informationssysteme ermöglicht werden soll. Zudem wird in diesem Kapitel auch auf die Beteiligung der Schweiz an der Interoperabilität eingegangen.

In Kapitel V werden die in den vorangehenden Kapiteln erarbeiteten Erkenntnisse zur Prüfung der Vereinbarkeit der Interoperabilität mit dem Grundrecht auf Datenschutz angewendet. Auf der Grundlage der bei Art. 13 Abs. 2 BV verwendeten Rechtfertigungskriterien wird insbesondere untersucht, ob die Interoperabilität einen verhältnismässigen Eingriff in das Grundrecht auf Daten-

schutz darstellt. Dabei stehen die vier Interoperabilitätskomponenten sowie die Abfragen gemäss Art. 20-22 EU-IOP-VO im Zentrum.

Im Rahmen einiger Schlussbemerkungen in Kapitel VI wird die Interoperabilität in den Kontext der Entstehungsgeschichte eingebettet. Ausserdem wird versucht, den Einfluss der Interoperabilität auf die zukünftige Datenbearbeitung im Zusammenhang mit Informationssystemen zu prognostizieren resp. die mögliche Weiterentwicklung der Interoperabilität zu antizipieren.

4. Begriffsdefinitionen

Der Begriff «*Interoperabilität*» ist grundsätzlich mehrdeutig. In der vorliegenden Untersuchung wird er ausschliesslich als die Verknüpfung der EU-Informationssysteme verstanden, welche in Kapitel III ausführlich erläutert wird.[16]

Ebenfalls häufig werden die beiden Begriffe «*EU-Informationssysteme*» und «*Schengen/Dublin-Informationssysteme*» verwendet. Der erstgenannte Begriff umfasst neben den Systemen EES, VIS, ETIAS, Eurodac und SIS auch das ECRIS-TCN.[17] Da das ECRIS-TCN weder der Schengener noch der Dubliner Zusammenarbeit zuzurechnen ist, kann dieses System nicht unter den Begriff Schengen/Dublin-Informationssysteme subsumiert werden.[18] Schliesslich werden die Begriffe «*Informationssystem*», «*Datenbank*» resp. «*System*» in der vorliegenden Untersuchung als Synonyme verstanden. Darunter wird ein elektronisches System subsumiert, in welchem grosse Bestände an Daten an einem zentralen Ort gespeichert sind.[19]

Des Weiteren sind verschiedene Begrifflichkeiten des Datenschutzrechts zu klären. Unter dem Begriff «*Daten*» wird grundsätzlich jede Art von Informationen verstanden. Gewisse Daten sind «*personenbezogen*», d.h. sie beziehen sich auf eine bestimmte resp. bestimmbare Person. Nur personenbezogene Daten werden vom Datenschutzrecht geschützt.[20] Im Folgenden wurde häufig darauf verzichtet, die Daten explizit als personenbezogen zu deklarieren, da der Personenbezug in der Regel zweifelsfrei vorliegt.[21]

---

16 Siehe dazu Kapitel IV.
17 Siehe dazu Art. 4 Ziff. 15 EU-IOP-VO.
18 Siehe dazu Kapitel III.9.
19 Siehe dazu die Definition von «*Datenbank*» im Duden, abrufbar unter <https://www.duden.de/rechtschreibung/Datenbank>, zuletzt besucht am 07.03.2025.
20 Blonski, 5. Siehe dazu auch Kapitel II.4.3; II.5.3 sowie II.6.3.
21 Siehe dazu jedoch auch Kapitel V.2.2.1.

Als bestimmte Arten von Daten werden insbesondere die «*alphanumerischen*» und die «*biometrischen*» Daten unterschieden. Bei Ersteren handelt es sich um Angaben in der Form von Buchstaben, Ziffern, Sonderzeichen, Leerzeichen sowie Satzzeichen.[22] Als biometrische Merkmale gelten physiologische und verhaltensspezifische Eigenschaften, welche sich zur Unterscheidung von Individuen eignen. Biometrische Merkmale zeichnen sich insbesondere dadurch aus, dass sie grundsätzlich bei jedem Menschen vorhanden, aber immer einzigartig ausgestaltet sind. Hinzu kommt, dass sich solche Merkmale im Laufe der Zeit kaum verändern.[23] Da biometrische Daten bei jedem Menschen einzigartig sind, eignen sie sich besonders gut für die Identifikation von Personen.[24] Als biometrische Merkmale werden im Allgemeinen u.a. die Schrift, die Stimme, der Fingerabdruck, das Gesicht, die Hand, die Iris resp. die DNA, verwendet.[25]

In Art. 8 Abs. 2 GRC wird der Begriff «*Verarbeitung*» von Daten verwendet. In der schweizerischen Datenschutzgesetzgebung ist hingegen der Begriff «*Bearbeitung*» von Daten üblich.[26] Diese beiden Begriffe werden als Synonyme verstanden, wobei für die vorliegende Untersuchung primär der letztgenannte Begriff verwendet wird.[27] Ebenfalls als Synonyme werden die im Zusammenhang mit Informationssystemen vorgenommenen «*Zugriffe*» resp. «*Abfragen*» verstanden. Im Rahmen dieser Art der Datenbearbeitung werden dem Endnutzer (in einem Informationssystem gespeicherte) Daten zugänglich gemacht.

Verschiedene Datenbearbeitungen, welche durch die Interoperabilität ermöglicht werden, zielen auf die «*Identifikation*» von Personen. Bei diesem Verfahren werden Daten, z.B. ein Gesichtsbild einer Person, mit einer Vielzahl von anderen Daten derselben Art abgeglichen. Durch diesen Vergleich wird ein Wert erstellt, welcher eine Wahrscheinlichkeit darstellt, dass es sich bei einem Treffer um dieselbe Person handelt.[28] Die Identifikation einer Person ist von

22 Art. 4 Ziff. 7 EU-IOP-VO.

23 Im Allgemeinen wird unter dem Begriff der Biometrie, welcher sich aus den griechischen Wörtern *bios* (Leben) und *metron* (Mass) ableitet, die Messung von Lebewesen verstanden. Siehe zum Ganzen STADELMANN, 1 ff.

24 FRA, biometrics, 20.

25 Siehe dazu BLONSKI, 16 ff. m.w.H.

26 Siehe dazu Art. 5 lit. d DSG.

27 Siehe zum Verständnis des Begriffs der Datenbearbeitung Kapitel II.4.3; II.5.3 sowie II.6.3.

28 Siehe dazu FRA, Gesichtserkennungstechnologien, 7.

der «*Verifikation*» einer Person zu unterscheiden. Bei Letzterer wird der Abgleich nur mit einem anderen Datenset derselben Art vorgenommen.[29]

Da für die vorliegende Untersuchung die Perspektive der Schweiz im Fokus steht, werden primär die Bezeichnungen «*Schengen-Staat(en)*» *und* «*Dublin-Staat(en)*» verwendet. Darunter werden alle Staaten verstanden, welche an Schengen resp. Dublin partizipieren (also u.a. auch diejenigen Staaten, welche durch ein entsprechendes Assoziierungsabkommen gebunden sind). *E contrario* wird mit der Verwendung des Begriffs «*Mitgliedstaat(en)*» zum Ausdruck gebracht, dass damit nur die Mitgliedstaaten der EU gemeint sind.[30] Im Zusammenhang mit der Interoperabilität wird der Begriff «*Schengen/Dublin-Staaten*» verwendet. Denn die gesetzlichen Grundlagen der Interoperabilität stellen Schengen-Weiterentwicklungen dar.[31] Mit Eurodac ist jedoch auch ein System der Dubliner Zusammenarbeit von der Interoperabilität betroffen.[32]

29 Dieses Verfahren kommt z.B. am Flughafen zum Einsatz. Dort wird das im Reisepass gespeicherte Bild eingelesen und mit einem Livebild vor Ort abgeglichen. FRA, Gesichtserkennungstechnologien, 7.

30 In der vorliegenden Untersuchung wird nicht näher berücksichtigt, dass nicht alle Mitgliedstaaten (vollumfänglich) an den verschiedenen Informationssystemen partizipieren.

31 Siehe dazu für die Schweiz ErwG. 81 IOP-Grenze-VO; ErwG. 77 IOP-Polizei-VO. Es ist jedoch zu beachten, dass sich aufgrund der Revision der Eurodac-VO in den gesetzlichen Grundlagen der Interoperabilität (noch) keine konkreten Verweise auf diese Verordnung finden. Siehe dazu BUNDESRAT, Botschaft IOP, 8002 f.

32 Siehe zu Eurodac Kapitel III.5. Auch in der Botschaft zur Genehmigung und Umsetzung der gesetzlichen Grundlage der Interoperabilität wird der Begriff «*Schengen/Dublin-Staaten*» verwendet. Hingegen wird der Begriff «*Schengen-Raum*» und nicht etwa «*Schengen/Dublin-Raum*» verwendet. Siehe dazu BUNDESRAT, Botschaft IOP. Diese Bezeichnungen werden ebenso in der vorliegenden Untersuchung verwendet.

II. Datenschutz als Grundrecht

1. Einleitung

Verschiedene Grundrechtsinstrumente weisen einen datenschutzrechtlichen Gehalt auf. Ausgangslage der vorliegenden Untersuchung sind die datenschutzrechtlichen Gewährleistungen von drei Grundrechtsinstrumenten: die GRC, die EMRK sowie die BV. Diese Relevanz ergibt sich daraus, dass die Interoperabilität dem EU-Recht entspringt und deshalb die gesetzliche Regelung der Interoperabilität mit der GRC vereinbar sein muss. Abgesehen davon, dass die GRC einen engen Bezug zur EMRK aufweist, sind auch die EU-Mitgliedstaaten an Letztere gebunden. Insofern drängt sich eine Berücksichtigung der EMRK auf. Die Interoperabilität richtet sich jedoch nicht nur an die EU-Mitgliedstaaten, sondern ebenfalls an Schengen-assoziierte Staaten wie die Schweiz. Da die nationale Regelung der Interoperabilität in der Schweiz zum Teil näher berücksichtigt wird, erscheint es angezeigt, auch die BV als Grundrechtsinstrument in die vorliegende Fragestellung miteinzubeziehen.[33]

Im Folgenden wird nach einigen Ausführungen zum Grundgedanken des Datenschutzes das Verhältnis der genannten Grundrechtsinstrumente zueinander geklärt. Die nachfolgend aufgezeigte partielle Verzahnung der Grundrechtsinstrumente kann erklären, weshalb deren datenschutzrechtlicher Gehalt sehr ähnlich ausgestaltet ist.

Die weiteren Ausführungen in diesem Kapitel dienen dazu, den datenschutzrechtlichen Gehalt der drei Grundrechtsinstrumente einzeln darzustellen und miteinander zu vergleichen. In diesem Vergleich werden die weitgehend ähnlichen Schutzbereiche und Rechtfertigungskriterien für Grundrechtseingriffe herausgearbeitet und deren Gemeinsamkeiten sowie allfällige Abweichungen untersucht.[34] Diese Ausführungen bilden die Grundlage für die Prüfung der Vereinbarkeit der Interoperabilität mit dem datenschutzrechtlichen Gehalt dieser drei Grundrechtsinstrumente.[35]

---

33 Siehe zu dieser Eingrenzung Kapitel I.2.

34 Die Thematik der Einwilligung in die Datenbearbeitung wird dabei ausgeklammert, da diese für die vorliegende Untersuchung nicht von Bedeutung ist.

35 Siehe dazu Kapitel V.

2. Entwicklung und Grundgedanke des Datenschutzes

Der Datenschutz ist ein jüngeres Grundrecht, welches sich erst in den 1970er Jahren aufgrund der Entwicklung der Technologie und der damit möglichen automatisierten Datenverarbeitung entwickelt hatte. Aufgrund dessen wurde der Datenschutz in vielen Verfassungen nicht ausdrücklich kodifiziert, sondern wurde durch die Interpretation bereits bestehender verfassungsrechtlicher Bestimmungen – häufig im Rahmen des Rechts auf Privatheit resp. Privatleben – geschaffen. Durch zahlreiche Entwicklungen, wie insbesondere die Ausbreitung des Internets, die Nutzung von portablen Geräten sowie das Aufkommen von sozialen Netzwerken haben sich die Gefährdungspotentiale für den Datenschutz stark erhöht und gewandelt.[36] Aus datenschutzrechtlicher Sicht ist die rasante Weiterentwicklung der Technologie, welche immer wieder neue rechtliche Fragen aufwirft, besonders herausfordernd.[37]

Dem Datenschutz liegt der Gedanke zu Grunde, dass es für ein selbstbestimmtes Entscheiden resp. Handeln einer Person unabdingbar ist, dass diese weiss oder zumindest abschätzen kann, welche persönlichen Angaben andere Personen über sie in Erfahrung bringen können. Durch eine uneingeschränkte Bearbeitung der persönlichen Daten sind nicht nur die Privatsphäre, sondern auch die geistige Unversehrtheit sowie die grundlegendsten Aspekte der Persönlichkeitsentfaltung tangiert.[38] Dabei gilt es stets zu berücksichtigen, dass im Rahmen des Datenschutzes die Daten nicht aufgrund ihrer selbst geschützt werden, sondern dass damit vielmehr der Privatsphären- resp. der Persönlichkeitsschutz der betroffenen Person sichergestellt werden soll.[39] Die Datenschutzgesetzgebung soll die Individuen nicht grundsätzlich vor Datenbearbeitungen schützen. Sie soll jedoch Schutz vor unberechtigter resp. nicht verhältnismässiger Datenbearbeitung bieten.[40]

36 Breuer, in: EU-Grundrechte-HdB, § 25 N 1.
37 Belser, rechtliche Tragweite, 20 f.
38 Belser/Waldmann, 79.
39 Gächter/Werder, 88; Albrecht/Jotzo, 44.
40 De Hert/Gutwirth, Case Law, 3 f.

3. Verzahnung der Grundrechtsinstrumente

3.1. BV und EMRK

Die Schweiz ist der EMRK im Jahr 1974 beigetreten.[41] Die in der EMRK garantierten Rechte sind in der Schweiz direkt anwendbar.[42] Oftmals sind sie zudem im innerstaatlichen Recht als verfassungsmässige Grundrechte in der BV verankert. Die EMRK konkurriert jedoch nicht mit den in der BV verankerten Grundrechten. Vielmehr sollen letztere den primären Grundrechtsschutz darstellen, wobei der EMRK ein subsidiärer Charakter zukommt. Mit der EMRK wird ein europäischer Mindeststandard gesichert, der von den innerstaatlichen Grundrechten übertroffen werden kann. Geht der innerstaatlich vorgesehene Schutz über die EMRK hinaus, vermag die EMRK diesen Schutz nicht einzuschränken.[43]

Die Rechtsprechung des BGer im Bereich des Datenschutzes zeigt, dass in vielen Fällen sowohl eine Verletzung von Art. 13 BV als auch von Art. 8 EMRK geltend gemacht wird.[44] Ausserdem verweist das BGer in seiner Rechtsprechung regelmässig auf den datenschutzrechtlichen Gehalt von Art. 8 EMRK.[45]

3.2. GRC und EMRK

Die Mitgliedstaaten der EU haben die Grundrechte gemäss der GRC bei der Anwendung resp. Durchführung von EU-Recht grundsätzlich anzuwenden.[46] Neben ihrer Mitgliedschaft in der EU, sind alle Mitgliedstaaten auch Vertragsparteien der EMRK.[47] Da diese dadurch an die EMRK gebunden sind, bedeutet

41 VILLIGER, N 10.

42 DONATSCH, 185.

43 Es handelt sich dabei um das sog. Günstigkeitsprinzip gemäss Art. 53 EMRK. Siehe zum Ganzen VILLIGER, N 274 ff. m.w.H. Siehe zum Einfluss der EMRK in der Schweiz auch SCHWEIZER, Grundrechtsschutz, 29 ff. Siehe für die Frage der Normenhierarchie zwischen dem Völkerrecht und dem Verfassungsrecht im Falle eines echten Normenkonflikts BELSER, in: BSK BV, Einleitung N 53 ff. Demnach ist ein grundsätzlicher Vorrang des Völkerrechts umstritten. Bezogen auf die EMRK bejaht das BGer jedoch einen solchen Vorrang.

44 Siehe dazu z.B. BGE 127 I 6; BGE 137 I 167; BGE 140 I 353; BGE 140 I 381; BGE 144 I 126.

45 Siehe dazu u.a. BGE 137 I 167, E. 3.2.; BGE 140 I 353, E. 8.3.; BGE 144 I 126, E. 4.1.

46 Dabei werden verschiedene Fallgruppen unterschieden. Siehe dazu EPINEY, Verbindlichkeit, 149 ff. m.w.H.

47 MAYER, in: Karpenstein/Mayer, Kommentar EMRK, Einleitung N 114. Die Protokolle wurden jedoch nicht von allen Staaten ratifiziert. Einige Staaten haben zudem Vorbehalte i.S.v. Art. 57 EMRK angebracht. Siehe dazu JARASS/KMENT, § 1 N 10.

dies, dass die nationalen Richter der Mitgliedstaaten Unionsrecht stets im Einklang mit der EMRK anwenden müssen.[48]

Die EU selbst ist (noch) nicht Partei der EMRK. Ein entsprechender Beitritt ist gemäss dem Primärrecht der EU zwar vorgesehen.[49] Durch das Gutachten 2/13[50] des EuGH fanden aufgenommene Beitrittsverhandlungen jedoch ein jähes Ende. Der Gerichtshof hatte darin feststellt, dass der vorgesehene Beitritt der EU zur EMRK das Gleichgewicht in der EU stören und die Autonomie des EU-Rechts untergraben könnte.[51] Vor ein paar Jahren wurden auf Initiative der Kommission die Verhandlungen wieder aufgenommen, um der im Primärrecht enthaltenen rechtlichen Verpflichtung nachzukommen. Mit dem Beitritt der EU zur EMRK soll der Schutz der Menschenrechte in Europa gestärkt werden.[52]

Abgesehen von dem im Primärrecht der EU vorgesehenen Beitritt der EU zur EMRK nimmt auch die GRC explizit Bezug zur EMRK.[53] Gemäss Art. 52 Abs. 3 GRC haben die in der GRC verankerten Rechte, sofern sie denjenigen in der EMRK entsprechen, «*die gleiche Bedeutung und Tragweite, wie sie ihnen in der Konvention verliehen wird*», wobei das EU-Recht einen weitergehenden Schutz gewähren kann. Der Gehalt der EMRK stellt also den Mindestschutzgehalt der Grundrechte der Union dar.[54]

Die EMRK enthält hingegen keine dem Art. 52 Abs. 3 GRC entsprechende Bestimmung. Dennoch wurde in einigen Urteilen des EGMR auf die GRC Bezug

48 Siehe dazu Callewaert, 171 f.; Jacobs, et al., 13.

49 Siehe dazu Art. 6 Abs. 2 S. 1 EUV.

50 EuGH, Gutachten 2/13, 18.12.2014, ECLI:EU:C:2014:2:2454.

51 Mangels Vereinbarkeit mit den Verträgen hatte sich der EuGH bereits im Jahr 1994 in einem Gutachten kritisch zu einem Beitritt geäussert. Siehe dazu EuGH, Gutachten 2/94, 28.3.1996, ECLI:EU:C:1996:140. Siehe zur Entwicklung der Bestrebungen zum Beitritt der EU zur EMRK Besson, 430 ff. Vgl. dazu auch Engel.

52 Zumindest beim ersten Beitrittsversuch ging es weniger um inhaltliche Aspekte als vielmehr um die prozessualen Möglichkeiten. Siehe zum Beitritt der EU zur EMRK auch Mayer, in: Karpenstein/Mayer, Kommentar EMRK, Einleitung N 154 ff. m.w.H.; Jarass/Kment, § 1 N 11 f.; Grabenwarter/Pabel, § 4 N 13 ff. m.w.H. Siehe zu den aktuellen Verhandlungen <https://www.coe.int/en/web/human-rights-intergovernmental-cooperation/accession-of-the-european-union-to-the-european-convention-on-human-rights>; <https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-completion-of-eu-accession-to-the-echr>, beide zuletzt besucht am 07.03.2025. Vgl. dazu auch Gaudin.

53 In diesem Zusammenhang wird auch von einer externen resp. inneren Kontrolle gesprochen. Siehe dazu Callewaert, 172 f.

54 Siehe dazu auch Breuer, in: EU-Grundrechte-HdB, § 25 N 20. Siehe zu Art. 52 Abs. 3 GRC ausführlich Colella, restriction, 155 ff.

genommen. Der Einfluss der GRC ist dabei eher von untergeordneter Bedeutung. Dies ist insofern nicht erstaunlich, als die Grundrechte in der GRC derart verankert wurden, dass diese mindestens den Gehalt der EMRK aufwiesen.[55]

Der Konvention ist jedoch zu entnehmen, dass durch die Übertragung von Hoheitsrechten an eine internationale Organisation der Schutz der EMRK nicht umgangen werden darf.[56] Die Konvention erlaubt dementsprechend eine Übertragung von Kompetenzen auf eine internationale Organisation nur, sofern die in der EMRK garantierten Rechte weiterhin sichergestellt sind.[57] Grundsätzlich geht der EGMR von der Annahme aus, dass die EU einen gleichwertigen Grundrechtsschutz gewährleistet wie die EMRK.[58]

Der EGMR muss in seiner Rechtsprechung nur die EMRK beachten. Der EuGH hat hingegen aufgrund von Art. 52 Abs. 3 GRC neben der GRC auch die EMRK zu berücksichtigen.[59] Die Urteile des EGMR sind für den EuGH jedoch nicht verbindlich. Die beiden Gerichte sind grundsätzlich bemüht, Auslegungsdivergenzen zu vermeiden.[60] Der Rechtsprechung von beiden Gerichten ist zu entnehmen, dass sie regelmässig auf die Rechtsprechung des jeweils anderen Gerichts verweisen.[61] Der EGMR wurde zudem auch schon mit Beschwerden

55 Siehe dazu LEMMENS/PIRET, 185 ff. mit Hinweisen auf die Rechtsprechung.

56 Vgl. dazu Art. 1 EMRK.

57 Siehe dazu EGMR, Urteil v. 18.02.1999, *Matthews v. The United Kingdom*, Beschwerde Nr. 24833/94, Rz. 32.

58 Der EGMR überprüft deshalb nur in bestimmten Fällen Beschwerden, welche EU-Recht betreffen. Siehe dazu EGMR, Urteil v. 30.06.2005, *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland*, Beschwerde Nr. 45036/98, insbesondere Rz. 154 ff. Siehe dazu auch EGMR, Urteil v. 06.12.2012, *Michaud v. France*, Rz. 101 ff.; JACOBS, et al., 14.

59 BRKAN, judicialisation and constitutionalisation, 291 ff.

60 MAYER, in: Karpenstein/Mayer, Kommentar EMRK, Einleitung N 151.

61 Siehe zur Rechtsprechung des EuGH u.a. EuGH, Urteil v. 20.05.2003, *Österreichischer Rundfunk u.a.*, ECLI:EU:C:2003:294, Rz. 73, 77; EuGH, Urteil v. 09.11.2010, *Volker und Markus Schecke und Eifert*, ECLI:EU:C:2010:662; EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238; EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970; EuGH, Urteil v. 06.10.2020, *La Quadrature du Net u.a.*, ECLI:EU:C:2020:791. Siehe zur Rechtsprechung des EGMR u.a. EGMR, Urteil v. 16.06.2015, *Delfi AS v. Estonia*, Beschwerde Nr. 64569/09; EGMR, Urteil v. 04.12.2015, *Roman Zakharov v. Russia*, Beschwerde Nr. 47143/06; EGMR, Urteil v. 12.01.2016, *Szabó and Vissy v. Hungary*, Beschwerde Nr. 37138/14; EGMR, Urteil v. 13.09.2018, *Big Brother Watch and others v. The United Kingdom*, Beschwerde Nr. 58170/13, 62322/14 und 24960/15; EGMR, Urteil v. 25.05.2021, *Big Brother Watch and others v. The United Kingdom*, Beschwerde Nr. 58170/13, 62322/14 und 24960/15. Es ist zu berücksichtigen, dass diese Verweise nicht immer im Teil der Argumentation der Gerichte aufgeführt sind (sondern z.B. bei den einschlägigen Rechtsquellen oder den Feststellungen der Parteien). Ein Verweis bedeutet demnach nicht *per se*, dass sich das Gericht von der Rechtsprechung eines anderen Gerichts inspirieren lässt. Siehe dazu BRKAN, judicialisation and constitutionalisation, 293 ff.

konfrontiert, mit welchen sich bereits der EuGH auseinandergesetzt hatte.[62] Abgesehen davon können die beiden Gerichte auch bezüglich einer spezifischen Thematik in einen Dialog miteinander treten.[63] Der EGMR bedient sich zudem vereinzelt der GRC sowie der Rechtsprechung des EuGH, um eine dynamische und evolutive Interpretation der EMRK zu ermöglichen und letztlich eine Ausweitung des Schutzes der Menschenrechte zu bewirken. Der EMRK-Mindeststandard kann nämlich nur dann angehoben werden, wenn diesbezüglich ein Konsens in der europäischen Gesellschaft vorhanden ist.[64] Die GRC dient dabei als Stärkung der Argumentation des EGMR.[65]

Im Bereich des Schutzes der personenbezogenen Daten stellt die Rechtsprechung des EuGH (jedoch nicht unbedingt die GRC) eine wichtige Quelle der Interpretation für den EGMR dar. In einzelnen Urteilen verweist der EGMR umfangreich (bei der Aufführung des einschlägigen rechtlichen Rahmens sowie der Praxis) auf die GRC und die Rechtsprechung des EuGH.[66] Auch der EuGH beachtet in seiner Argumentation in Urteilen in diesem Bereich die Rechtsprechung des EGMR.[67]

3.3. BV und GRC

Da die Schweiz kein Mitgliedstaat der EU ist, ist sie nicht an die GRC gebunden.[68] Davon abgesehen wird in keinem der verschiedenen zwischen der

62 So kann es z.B. vorkommen, dass der EGMR in einer Angelegenheit angerufen wird, in welcher der EuGH bereits in einem Vorabentscheidungsverfahren entschieden hat. Siehe dazu BRKAN, judicialisation and constitutionalisation, 291 ff. m.w.H. Siehe dazu die folgenden Urteile: EuGH, Urteil v. 16.12.2008, *Satakunnan Markkinapörssi und Satamedia Oy v Finland*, ECLI:EU:C:2008:727; EGMR, Urteil v. 21.07.2015, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Beschwerde Nr. 931/13; EGMR, Urteil v. 27.06.2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Beschwerde Nr. 931/13.

63 So bspw. im Bereich der Vorratsdatenspeicherung. Siehe dazu BRKAN, judicialisation and constitutionalisation, 281.

64 Siehe dazu VILLIGER, N 274.

65 Siehe zum Ganzen LEMMENS/PIRET, 185 ff. m.w.H.

66 LEMMENS/PIRET, 197. Siehe dazu die Urteile EGMR, Urteil v. 13.09.2018, *Big Brother Watch and others v. The United Kingdom*, Beschwerde Nr. 58170/13, 62322/14 und 24960/15, z.B. Rz. 22; EGMR, Urteil v. 25.05.2021, *Big Brother Watch and others v. The United Kingdom*, Beschwerde Nr. 58170/13, 62322/14 und 24960/15, z.B. Rz. 209 ff.; EGMR, Urteil v. 25.05.2021, *Centrum för Rättvisa v. Sweden*, Beschwerde Nr. 35252/08, z.B. Rz. 98 ff.

67 Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 35, 54 f.; EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 119 f.; EuGH, Urteil v. 06.10.2020, *La Quadrature du Net u.a.*, ECLI:EU:C:2020:791, Rz. 115 f., 126.

68 EPINEY, in: BSK BV, Art. 36 BV N 28.

Schweiz und der EU existierenden bilateralen Abkommen, darunter die Schengen/Dublin-Assoziierungsabkommen, explizit festgehalten, die GRC sei bei der Auslegung dieser Abkommen einschlägig. Daraus könnte der Schluss gezogen werden, dass die GRC sowie die Rechtsprechung des EuGH zu den EU-Grundrechten im bilateralen Verhältnis nicht zu beachten ist. Die EU-Grundrechte sind jedoch bei der Auslegung und Anwendung des gesamten EU-Rechts zu berücksichtigen. Ob diese nicht auch in den bilateralen Abkommen berücksichtigt werden müssten, ist daher fraglich.[69] Schliesslich knüpfen die bilateralen Abkommen verschiedentlich an EU-Recht an.[70]

In der Lehre wird die Ansicht vertreten, dass für die bilateralen Abkommen, welche auf EU-Recht basieren und deren Ziel und Zweck es ist, eine parallele Rechtslage zu schaffen, die EU-Grundrechte einen inhärenten Bestandteil darstellen.[71] Dieses Verständnis hat zur Folge, dass Konzepte und Begriffe der bilateralen Abkommen, welche aus dem EU-Recht stammen, gemäss den EU-Grundrechten angewandt und ausgelegt werden. Ebenso müssen Ermessensspielräume, welche von solchen Konzepten resp. Begriffen gewährt werden, im Einklang mit den EU-Grundrechten genutzt werden.[72] Diese Auffassung führt jedoch nicht dazu, dass die EU-Grundrechte eigenständige Rechte, wie bspw. die in der EMRK verankerten Rechte, darstellen. Eine eigenständige Geltendmachung ist daher nicht möglich. Sie können jedoch bei der Auslegung und Anwendung von relevanten Bestimmungen in den bilateralen Abkommen herangezogen werden.[73]

Ein solches Verständnis zur Verbindlichkeit von EU-Grundrechten im Rahmen der bilateralen Abkommen ist jedoch mit Unsicherheiten und Schwierigkeiten verbunden. So kann es nicht immer eindeutig sein, ob es sich im Einzelfall um einen unionsrechtlichen Grundsatz oder Begriff handelt. Dies muss nicht zwingend explizit aus den Abkommen hervorgehen.[74] Umstrittene Fragen müssen von den höchsten Gerichten entschieden werden. Damit verbunden

69 Siehe zum Ganzen Oesch, Grundrechte, 192; Epiney, Verbindlichkeit, 141 f.; Epiney/Pirker, 230.

70 Siehe dazu auch Epiney, Verbindlichkeit, 143 f. m.w.H.

71 Oesch, Grundrechte, 195; Oesch, Bilaterale Verträge, 296 f.

72 Siehe zur Bedeutung der EU-Grundrechte für die Schweiz Epiney/Pirker; Epiney, Verbindlichkeit; Oesch, Grundrechte, 193 ff.; Zünd, 1356 f. Das BGer geht – im Zusammenhang mit dem FZA – von einer Verschmelzung der EU-Grundrechte und einem unionsrechtlichen Begriff aus, sofern auf erstere für die Auslegung des Begriffs zurückgegriffen wird. Die sich daraus ergebende Auslegung stellt einen Teil des gemeinschaftlichen Besitzstands dar. Siehe dazu BGE 130 II 113, E. 6.5.

73 Epiney/Pirker, 240. Siehe dazu auch Epiney, Verbindlichkeit, 156.

74 Epiney, Verbindlichkeit, 147 ff.

ist Rechtsunsicherheit. Hinzu kommt, dass es mangels eines verbindlichen Streitbeilegungsmechanismus nicht ausgeschlossen werden kann, dass letztlich Meinungsverschiedenheiten zwischen den Vertragsparteien entstehen können.[75]

Gegen eine Relevanz der EU-Grundrechte im Bereich der bilateralen Abkommen spricht, dass diese nicht in den Abkommen – auch nicht in den Präambeln – aufgeführt sind. Auch könnte argumentiert werden, dass die bilateralen Abkommen nicht unbedingt auf eine Integration abzielen.[76]

Die Rechtsprechung zeigt, dass insbesondere im Zusammenhang mit der Dublin-III-VO die schweizerischen Gerichte teilweise Bezug auf die GRC genommen haben. So hat sich das Bundesverwaltungsgericht (BVGer) dahingehend geäussert, dass die Dublin-III-VO im Sinne der EMRK «*und für die Schweiz als Nicht-EU-Mitglied etwas systemfremd der EU-Grundrechtecharta auszulegen*» sei.[77] Davon abgesehen nimmt das BVGer bei der Prüfung der Zulässigkeit des Nichteintretens des SEM und der Anordnung der Wegweisung regelmässig Bezug auf Art. 4 GRC (Verbot der Folter und unmenschlicher oder erniedrigender Strafe oder Behandlung).[78] Da diese Bestimmung dieselbe Bedeutung und Tragweite wie Art. 3 EMRK (Verbot der Folter) hat, dürfte es im Ergebnis letztlich jedoch keine Rolle spielen, auf welches Grundrechtsinstrument sich das Gericht abstützt.[79]

Das BGer hat in einem Urteil die Ansicht vertreten, dass der Inhalt eines Verweises in der Dublin-III-VO auf Bestimmungen eines EU-Rechtsaktes, welcher für die Schweiz nicht verbindlich ist, durch Inkorporation Teil der Dublin-III-VO wird und somit «*als Teil des acquis auch im Verhältnis zur Schweiz anwendbar*» ist.[80] Dieses Urteil könnte den Schluss nahe legen, dass Verweise in Schengen/Dublin-Rechtsakten auf Rechtsakte, welche grundsätzlich nicht für die Schweiz verbindlich sind, durch die Verweisung Teil des Schengen/Dublin-*acquis* werden. Diese Argumentation liesse sich auch auf die für die Schweiz grundsätzlich nicht verbindliche GRC anwenden, sofern diese mittels Verweisung Eingang in Schengen/Dublin-Rechtsakte findet. Nochmals bezugnehmend auf das oben genannte Urteil des BGer ist jedoch festzuhalten, dass

75 Epiney/Pirker, 234. Siehe zum Ganzen auch Epiney, Verbindlichkeit, 146 f.

76 Anders der EWR, welcher auf eine Integration in den Binnenmarkt der EU abzielt. Siehe zum Ganzen Epiney, Verbindlichkeit, 154 f.; Epiney/Pirker, 239 f.

77 BVGE 2015/41, E. 5.3.3.

78 Siehe dazu Oesch/Naef, 126 mit Hinweisen auf die Rechtsprechung.

79 Siehe dazu Oesch/Naef, 127.

80 BGE 143 II 361, E. 3.3.

sich diese Auslegung u.a. «*ausdrücklich*» auf die einschlägige Botschaft stützt.[81] Aus derselben geht doch gerade ausdrücklich hervor, dass die besagte Richtlinie, auf welche verwiesen wird, nicht verbindlich ist. Dieser soll lediglich «*Rechnung getragen*» werden. Diesbezüglich wird lediglich von «*ähnlichen*» Standards gesprochen.[82] Gemäss der hier vertretenen Auffassung ergibt sich aus dieser Fundstelle in der Botschaft gerade kein ausdrücklicher Hinweis, dass die Bestimmungen, auf welche verwiesen wird, durch Inkorporation für die Schweiz Verbindlichkeit beanspruchen sollten. Vielmehr soll die Schweiz zumindest ähnliche Standards bezüglich der Haft anwenden (gerade weil die besagte Richtlinie nicht verbindlich ist für die Schweiz).[83]

Der EuGH hat sich bis anhin nicht explizit zur Relevanz der EU-Grundrechte im bilateralen Verhältnis zur Schweiz geäussert.[84]

In der Regel dürften die Konsequenzen der Beachtung der EU-Grundrechte von den schweizerischen Behörden hinsichtlich der Auslegung von unionsrechtlichen Begriffen in der Praxis gering ausfallen. So orientiert sich die GRC doch stark an der EMRK, weshalb es primär nicht entscheidend erscheint, ob auf die GRC oder die EMRK abgestellt wird. Obwohl formal unterschiedliche Rechtsquellen herangezogen werden und folglich dogmatisch anders argumentiert wird, führt eine Berufung auf die EMRK resp. die GRC in diesen Fällen inhaltlich zum gleichen Ergebnis. Unklar dürften hingegen diejenigen Fälle sein, in welchen Grundrechte betroffen sind, welche von der EMRK nicht gewährleistet werden.[85]

---

81 BGE 143 II 361, E. 3.3.

82 Botschaft Dublin-III-VO/Eurodac-VO, 2707.

83 In der Rechtsprechung des BGer zur Gegenausnahme der Schubert-Praxis findet sich kein expliziter Verweis auf die GRC. Gemäss dieser Rechtsprechung findet die Ausnahme gemäss der Schubert-Praxis bei menschenrechtlichen sowie freizügigkeitsrechtlichen Verpflichtungen keine Anwendung. Siehe zu den menschenrechtlichen Verpflichtungen BGE 148 II 169, 5.2; Oesch, EuGH, 105 f. Siehe zu den freizügigkeitsrechtlichen Verpflichtungen BGE 142 II 35, E. 3.2.

84 Oesch/Naef, 120.

85 Oesch, Grundrechte, 199 f. Vgl. dazu auch Epiney, Verbindlichkeit, 156 f.; Hruschka, Grundrechtsschutz, 159.

4. Datenschutzrechtlicher Gehalt von Art. 8 EMRK

4.1. Rechtliche Verankerung

Die EMRK ist ein völkerrechtlicher Vertrag, welcher von den Mitgliedern des Europarates im Jahr 1950 geschlossen wurde. Das Inkrafttreten erfolgte am 3.9.1953.[86] Die ursprüngliche Konvention wurde seither durch verschiedene Protokolle erweitert. Diesen kommt grundsätzlich dieselbe Wirkung zu wie der Konvention selbst. Die Konvention stellt die erste verbindliche Menschenrechtskonvention weltweit dar.[87]

Die darin verankerten Rechte sind innerstaatlich unmittelbar anwendbar. Der EGMR verfügt über die Kompetenz, für die Vertragsparteien verbindliche Urteile zu fällen. Zudem kommt dem Gericht die Möglichkeit zu, die Rechte der EMRK falls notwendig den veränderten gesellschaftlichen oder wirtschaftlichen Gegebenheiten anzupassen. Die EMRK wird insofern als «*living instrument which must be interpreted in the light of present-day conditions*»[88] verstanden. Die Richter in Strassburg haben demnach allfällige Weiterentwicklungen der Grundrechte in die bereits bestehenden Grundrechte aufzunehmen.[89] Um eine dynamische Auslegung resp. Anpassung der Grundrechte zu ermöglichen, wurde die Formulierung der EMRK absichtlich flexibel gestaltet. Der Datenschutz fand bei der Unterzeichnung der EMRK noch keine Berücksichtigung. Erst die technische Entwicklung machte dessen grundrechtliche Verankerung notwendig.[90]

Mittlerweile anerkennt der EGMR auf der Grundlage des Rechts auf Achtung des Privatlebens gemäss Art. 8 EMRK ein Recht auf Schutz personenbezogener Daten.[91] Bis in die 1980er Jahre gingen die Entscheidungsgremien des Europarats noch davon aus, der EMRK könne kein Recht auf Datenschutz entnommen werden. Dank der Interpretation der EMRK als lebendiges Instrument sind heute Art. 8 EMRK auch datenschutzrechtliche Gehalte zu entnehmen.[92]

---

86 VILLIGER, N 7 ff. mit weiteren Hinweisen zum Zustandekommen der EMRK.

87 JARASS/KMENT, § 1 N 9.

88 EGMR, Urteil v. 25.04.1978, *Tyrer v. The United Kingdom*, Beschwerde Nr. 5856/72, Rz. 31.

89 SIEMEN, 25 ff.

90 STÄMPFLI, 85.

91 Siehe dazu EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 48; PROGIN-THEUERKAUF/ZOETEWEIJ-TURHAN/TURHAN, 6.

92 MATZ, 108 f. Siehe zur Entwicklung der Rechtsprechung zu Art. 8 EMRK hinsichtlich des Schutzes personenbezogener Daten SIEMEN, 51 ff. m.w.H.

4.2. Adressatenkreis und Grundrechtsträger der EMRK

Die EMRK verpflichtet die Vertragsparteien. Die Staaten können ihrer internationalen Verantwortlichkeit in verschiedener Art und Weise nachkommen, so z.B. durch die Delegation an staatliche Behörden oder Privatpersonen. Letztlich trägt gemäss dem internationalen Recht immer der Staat als Vertragspartei der Konvention die Verantwortung für deren Einhaltung. Als Grundrechtsträger gelten alle Personen, welche der Gerichtsbarkeit der Vertragsparteien unterliegen. Auch juristische Personen können sich auf die in der EMRK verankerten Rechte berufen, solange sie mit dem Staat nicht eng verbunden sind (also z.B. wenn diese staatliche Gewalt ausüben). Juristische Personen können sich jedoch nicht auf Rechte berufen, welche ihrer Natur nach nur natürlichen Personen zustehen.[93]

4.3. Persönlicher und sachlicher Geltungsbereich

Art. 8 EMRK richtet sich primär – aber nicht ausschliesslich – an natürliche Personen und statuiert grundsätzlich das Recht auf Privatleben, das Recht auf Familienleben sowie den Schutz der Wohnung und der Korrespondenz.[94] Gemäss dem Wortlaut werden also vier Rechte gewährleistet.[95] Der datenschutzrechtliche Gehalt wird insbesondere vom Recht auf Privatleben abgeleitet und als dessen Unterkategorie behandelt.[96]

Der Begriff des Privatlebens ist im Allgemeinen sehr weit gefasst. Der EGMR hat dazu festgehalten, es erscheine weder möglich noch notwendig, eine abschliessende Definition des Begriffs Privatleben festzulegen. Der Begriff solle aber nicht auf den «*inneren Kreis*», in dem der Einzelne sein persönliches Leben nach ei-

---

93 Dabei handelt es sich z.B. um Art. 2 EMRK; Art. 3 EMRK; Art. 5 EMRK und Art. 12 EMRK. Siehe zum Ganzen GRABENWARTER, Art. 1 ECHR N 2 ff. m.w.H. Siehe insbesondere zur Gerichtsbarkeit RAIMONDO, 155 ff. m.w.H.

94 GONIN/BIGLER, Art. 8 CEDH N 1. Vgl. zu den juristischen Personen GONIN/BIGLER, Art. 8 CEDH N 11 ff.

95 Diese Rechte können sich überlappen. Die beschwerdeführende Person muss in ihrer Beschwerde nicht genauer definieren, welcher Teilgehalt von Art. 8 EMRK als verletzt angesehen wird. Siehe dazu GRABENWARTER, Art. 8 ECHR N 5.

96 PSYCHOGIOPOULOU, 33. Neben dem Recht auf Privatleben kann jedoch u.U. auch das Recht auf Schutz der Korrespondenz einschlägig sein. Siehe dazu DE HERT/GUTWIRTH, Case Law, 18. Siehe dazu auch in der Rechtsprechung (im Zusammenhang mit geheimen Überwachungsmassnahmen) EGMR, Urteil v. 15.06.1992, *Lüdi v. Switzerland*, Beschwerde Nr. 12433/86, Rz. 39; EGMR, Urteil v. 25.06.1997, *Halford v. The United Kingdom*, Beschwerde Nr. 20605/92, Rz. 44.

genem Gutdünken führe und die Aussenwelt, die nicht zu diesem Kreis gehöre, limitiert werden. Das Privatleben solle vielmehr zu einem gewissen Grad auch das Recht umfassen, Beziehungen zu anderen Menschen einzugehen und zu führen.[97] Trotz fehlender Definition des Begriffs des Privatlebens ist ein Zusammenhang mit der persönlichen Selbstbestimmung erkennbar. Der Rechtsprechung von Strassburg kann entnommen werden, dass das Privatleben verschiedene Aspekte umfasst. So z.B. soziale Aspekte (Beziehungen zu anderen Personen führen und eingehen), Geburt und Tod (Abtreibung, Bestattung) sowie auch die (telefonische) Überwachung und der Schutz der Daten.[98]

Anfänglich war für die Anwendbarkeit von Art. 8 EMRK ein Bezug der fraglichen Informationen zum Privatleben der betroffenen Person ausschlaggebend.[99] Im Fall *Amann*[100] wurde ausgeführt, dass der Begriff des Privatlebens nicht zu restriktiv ausgelegt werden solle und auch Aktivitäten professioneller oder geschäftlicher Natur umfassen könne.[101] Im Fall *Rotaru*[102] kam der EGMR zum Schluss, dass auch die Sammlung von allgemein bekannten öffentlichen Informationen den sachlichen Anwendungsbereich von Art. 8 Abs. 1 EMRK betreffen könne, wenn diese Informationen systematisch erhoben und in Datenbanken der Behörden gespeichert würden. Dies gelte umso mehr, wenn sich die Informationen auf bereits weit zurückliegende Geschehnisse beziehen.[103] Ebenfalls hat der EGMR die berechtigte Erwartungshaltung der von der Datenbearbeitung betroffenen Personen berücksichtigt, um den Bezug zum Privatleben herzustellen. Dabei handle es sich um einen wichtigen, jedoch nicht zwingend ausschlaggebenden Faktor.[104]

---

97 EGMR, Urteil v. 16.12.1992, *Niemietz v. Germany*, Beschwerde Nr. 13710/88, Rz. 29. Siehe dazu auch EGMR, Urteil v. 28.01.2003, *Peck v. The United Kingdom*, Beschwerde Nr. 44647/98, Rz. 57; EGMR, Urteil v. 04.12.2008, *S. and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 66; EGMR, Urteil v. 21.06.2011, *Shimovolos v. Russia*, Beschwerde Nr. 30194/09, Rz. 64; EGMR, Urteil v. 07.02.2012, *Hannover v. Germany* (No. 2), Beschwerde Nr. 40660/08 und 60641/08, Rz. 95.

98 GONIN/BIGLER, Art. 8 CEDH N 19 ff. m.w.H. Siehe zum Begriff des Privatlebens auch PSYCHOGIOPOULOU, 33 f.; JACOBS, et al., 407 ff.; SIEMEN, 57 ff.

99 Siehe dazu EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 48.

100 EGMR, Urteil v. 16.02.2000, *Amann v. Switzerland*, Beschwerde Nr. 27798/95.

101 EGMR, Urteil v. 16.02.2000, *Amann v. Switzerland*, Beschwerde Nr. 27798/95, Rz. 65. Siehe dazu auch PSYCHOGIOPOULOU, 50 ff. m.w.H. Es ist nicht immer eindeutig, wann Tätigkeiten einer Person ihrem Berufs- und Geschäftsleben zuzurechnen sind und wann nicht. Siehe dazu EGMR, Urteil v. 16.12.1992, *Niemietz v. Germany*, Beschwerde Nr. 13710/88, Rz. 29.

102 EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95.

103 EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 43.

104 Siehe dazu EGMR, Urteil v. 25.09.2001, *P.G. and J.H. v. The United Kingdom*, Rz. 57; EGMR, Urteil v. 17.07.2003, *Perry v. The United Kingdom*, Beschwerde Nr. 63737/00, Rz. 37. Das Kri-

Die EMRK schützt nicht alle Arten von Daten. Welche Daten durch die EMRK geschützt sind, ist aufgrund des weiten Begriffs des Privatlebens sowie der vom EGMR jeweils vorgenommenen Einzelfallbeurteilung schwierig zu bestimmen resp. vorherzusehen.[105] Insbesondere die rechtliche Qualifizierung[106] der Daten, die Art der Daten sowie die Art der Datenbearbeitung kann eine Rolle spielen.[107]

Insgesamt ist zu beobachten, dass in der Rechtsprechung des EGMR teilweise – aufgrund der Schwierigkeiten bei der Bestimmung des Schutzbereichs von Art. 8 EMRK – nicht klar zwischen der Frage nach der Anwendbarkeit von Art. 8 EMRK und des Eingriffs in den Schutzbereich dieser Bestimmung unterschieden wird.[108]

Die bisherige Rechtsprechung des EGMR zeigt auf, dass eine Ausweitung des datenschutzrechtlichen Gehalts von Art. 8 EMRK stattgefunden hat.[109] Ob aus Art. 8 EMRK (mittlerweile) ein umfassendes Selbstbestimmungsrecht über die eigenen Personendaten abgeleitet werden kann, scheint noch nicht restlos geklärt zu sein.[110] Der EGMR geht in seiner jüngeren Rechtsprechung davon aus, dass Art. 8 EMRK (zumindest) eine Form der informationellen Selbstbestimmung zu entnehmen ist.[111]

---

terium der berechtigten Erwartungshaltung stellt teilweise auch ein Kriterium dar, ob ein Eingriff in Art. 8 EMRK vorliegt. Siehe dazu VON GRAFENSTEIN, 180 ff.

105 Siehe dazu VON GRAFENSTEIN, 180 ff. m.w.H.

106 So stellen z.B. Daten betreffend die Gesundheit sog. sensitive Daten dar. Die Datenbearbeitung von solchen Daten fällt automatisch in den Anwendungsbereich von Art. 8 Abs. 1 EMRK. Siehe dazu z.B. EGMR, Urteil v. 26.01.2017, *Surikov v. Ukraine*, Beschwerde Nr. 42788/06, Rz. 75. Siehe dazu auch KONING, 25 ff.

107 Siehe dazu KONING, 25 ff., 221 m.w.H. Vgl. dazu auch PSYCHOGIOPOULOU, 52; EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 67. Siehe ausserdem zum Schutzbereich auch GRABENWARTER, Art. 8 ECHR N 10; GRABENWARTER/PABEL, § 22 N 10; EPINEY/SCHLEISS, § 3 N 9 ff. Siehe für eine Übersicht über die Rechtsprechung des EGMR im Bereich des Datenschutzes zudem das regelmässig aufdatierte «*factsheet*», abrufbar unter <https://www.echr.coe.int/documents/d/echr/FS_Data_ENG>, zuletzt besucht am 07.03.2025.

108 SIEMEN, 120.

109 Siehe zur Entwicklung der Rechtsprechung zum Datenschutz SIEMEN, 79 ff. Siehe dazu auch TZANOU, 45 ff.

110 Siehe dazu bejahend MATZ, 144 f. Siehe dazu auch GRABENWARTER, Art. 8 ECHR N 57. Zumindest im Ansatz zustimmend DE HERT/GUTWIRTH, Case Law, 15, 19 f.; NETTESHEIM, in: Europäischer Grundrechteschutz, § 10 N 54.

111 Siehe dazu EGMR, Urteil v. 27.06.2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Beschwerde Nr. 931/13, Rz. 137; EGMR, Urteil v. 28.06.2018, *M.L. and W.W. v. Germany*, Beschwerde Nr. 60798/10 und 65599/10, Rz. 87.

4.4. Positive Schutzpflichten

Der EGMR anerkennt neben den negativen Verpflichtungen von Art. 8 EMRK auch positive Verpflichtungen.[112] So wurde in verschiedenen Urteilen insbesondere ein Recht auf Zugang[113] zu den eigenen Daten, die Löschung[114] von solchen, die Berichtigung[115] von unrichtigen Daten und sogar die Notwendigkeit einer unabhängigen Aufsichtsbehörde[116] (insbesondere bei geheimen Überwachungsmassnahmen) als positive Schutzpflicht diskutiert und teilweise gewährt. Auch die (zumindest nachträgliche) Information[117] der betroffenen Person über die Datenbearbeitung kann ebenfalls eine positive Schutzpflicht darstellen.[118]

Die Anerkennung von solchen positiven Verpflichtungen erfolgte jeweils in spezifischen Einzelfällen. Der EGMR hat sich nicht dazu geäussert, inwiefern solche positiven Schutzpflichten Art. 8 EMRK generell zu entnehmen sind.[119]

4.5. Eingriffe in den Schutzbereich

Wie bereits erwähnt, grenzt der EGMR die Anwendbarkeit von Art. 8 EMRK nicht klar von der Frage ab, ob ein Eingriff in den von dieser Bestimmung ge-

112 De Hert/Gutwirth, Case Law, 17. Der EGMR unterscheidet nicht immer eindeutig zwischen den negativen und positiven Schutzpflichten. Siehe dazu von Grafenstein, 132.

113 Siehe dazu z.B. folgende Urteile: EGMR, Urteil v. 07.07.1989, *Gaskin v. The United Kingdom*, Beschwerde Nr. 10454/83, Rz. 49; EGMR, Urteil v. 24.09.2002, *M.G. v. The United Kingdom*, Beschwerde Nr. 39393/98, Rz. 28 ff.

114 Siehe dazu z.B. folgende Urteile: EGMR, Urteil v. 06.06.2006, *Segerstedt-Wiberg and others v. Sweden*, Beschwerde Nr. 62332/00, Rz. 89 ff.; EGMR, Urteil v. 18.04.2013, *M.K. v. France*, Beschwerde Nr. 19522/09, Rz. 37 ff.; EGMR, Urteil v. 18.09.2014, *Brunet c. France*, Beschwerde Nr. 21010/10, Rz. 41 ff.

115 Siehe dazu z.B. folgende Urteile EGMR, Urteil v. 18.11.2008, *Cemalettin Canli v. Turkey*, Beschwerde Nr. 22427/04, Rz. 31 ff.; EGMR, Urteil v. 27.04.2010, *Ciubotaru v. Moldova*, Beschwerde Nr. 27138/04, Rz. 51 ff. Der Berichtigungsanspruch wurde auch bei einer Änderung von Angaben in Registern nach einer geschlechtsanpassenden Operation diskutiert. Siehe dazu u.a. EGMR, Urteil v. 17.10.1986, *Rees v. The United Kingdom*, Beschwerde Nr. 9532/81, Rz. 38 ff. Siehe zu einer Übersicht über diese Rechtsprechung Siemen, 193 ff.

116 EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71, Rz. 55; EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 65 ff.; EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 59 f.

117 Siehe dazu EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71, Rz. 58 f.

118 Siehe zum Ganzen auch De Hert/Gutwirth, Case Law, 19 f. Siehe allgemein zu den positiven Schutzpflichten beim Recht auf Privatleben gemäss Art. 8 EMRK von Grafenstein, 117 f.

119 Vgl. dazu Matz, 133.

schützten datenschutzrechtlichen Gehalt vorliegt.[120] Dies hat zur Folge, dass die vom EGMR bei der Beurteilung der Anwendbarkeit resp. des Eingriffs herangezogenen Kriterien nicht klar voneinander abgegrenzt werden können.

Der Rechtsprechung ist zu entnehmen, dass im Bereich des Datenschutzes verschiedene Arten von Datenbearbeitungen einen Eingriff bewirkt haben. So etwa das Gewinnen oder das Speichern und Verwenden von Informationen, wobei der EGMR jeweils festhielt, dass es sich dabei um eigenständige Eingriffe handle.[121] Auch das systematische Sammeln, Gewinnen, Verwenden und Speichern von Daten wurde als Eingriff in das Privatleben bewertet.[122]

Im Laufe der Zeit hat der EMGR zudem den «*test of reasonable expectations*» erarbeitet, um zu entscheiden, ob ein Eingriff in das Privatleben vorliegt.[123] Dabei wird auf die berechtigten Erwartungen der betroffenen Person abgestellt und geprüft, ob diese mit der vorgenommenen Datenbearbeitung rechnen musste.[124] So musste z.B. die Beschwerdeführerin in *Halford*[125] nicht damit rechnen, dass ein ihr zu privaten Zwecken zur Verfügung gestelltes Telefon von ihrem Arbeitgeber abgehört wird.[126] Ausserdem ist auch von einem Eingriff auszugehen, wenn positive Verpflichtungen verletzt werden.[127]

---

120 Siehe dazu Kapitel II.4.3.

121 Siehe dazu u.a. EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71, Rz. 41; EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 48; EGMR, Urteil v. 25.03.1998, *Kopp v. Switzerland*, Beschwerde Nr. 13/1997/797/1000, Rz. 53; EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 46. Siehe zu einer etwas ausführlicheren Abhandlung zum Eingriff EGMR, Urteil v. 25.05.2021, *Big Brother Watch and others v. The United Kingdom*, Beschwerde Nr. 58170/13, 62322/14 und 24960/15, Rz. 324 ff. In diesem Urteil wurden verschiedene Datenbearbeitungen vom EGMR als Eingriff in Art. 8 EMRK deklariert, wobei diese Eingriffe als jeweils unterschiedlich intensiv bewertet wurden.

122 PÄTZOLD, in: Karpenstein/Mayer, Kommentar EMRK, Art. 8 EMRK N 77.

123 VON GRAFENSTEIN, 246. Siehe dazu auch WP29, Opinion purpose limitation, 7.

124 Siehe dazu z.B. EGMR, Urteil v. 15.06.1992, *Lüdi v. Switzerland*, Beschwerde Nr. 12433/86, Rz. 40; EGMR, Urteil v. 25.06.1997, *Halford v. The United Kingdom*, Beschwerde Nr. 20605/92, Rz. 53 ff.; EGMR, Urteil v. 25.09.2001, *P.G. and J.H. v. The United Kingdom*, Rz. 57 ff.; EGMR, Urteil v. 28.01.2003, *Peck v. The United Kingdom*, Beschwerde Nr. 44647/98, Rz. 62; EGMR, Urteil v. 17.07.2003, *Perry v. The United Kingdom*, Beschwerde Nr. 63737/00, Rz. 14 f., 39 ff.

125 EGMR, Urteil v. 25.06.1997, *Halford v. The United Kingdom*, Beschwerde Nr. 20605/92.

126 EGMR, Urteil v. 25.06.1997, *Halford v. The United Kingdom*, Beschwerde Nr. 20605/92, Rz. 45. Siehe für ein anderes Beispiel EGMR, Urteil v. 25.09.2001, *P.G. and J.H. v. The United Kingdom*, Rz. 57. Siehe zum *test of reasonable expectations* auch VON GRAFENSTEIN, 182 ff. m.w.H.

127 EPINEY/SCHLEISS, § 3 N 15. Siehe dazu aus der Rechtsprechung z.B. EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 48; EGMR, Urteil v. 07.07.1989, *Gaskin v. The United Kingdom*, Beschwerde Nr. 10454/83, Rz. 49; EGMR, Urteil v.

Die Schwere eines Eingriffs wird im Allgemeinen anhand von qualitativen Kriterien wie der Länge, der Dauer oder dem Ausmass des Eingriffs als auch von quantitativen Kriterien wie der Gefahr irreversibler Eingriffe oder materiellen oder psychischen Folgen bestimmt. Speziell im Kontext des Datenschutzes hängt die Schwere des Eingriffs insbesondere (auch) von der Art der gespeicherten Daten ab.[128]

Das Kriterium der Schwere des Eingriffs ist im Rahmen verschiedener Rechtfertigungskriterien zu berücksichtigen. So einerseits bei der gesetzlichen Grundlage und andererseits auch bei der Verhältnismässigkeit. Je höher die Intensität des Eingriffs, desto höher sind auch die Anforderungen an die Vorhersehbarkeit, welche als Kriterium bei der gesetzlichen Grundlage beurteilt wird.[129] Bei der Prüfung der Verhältnismässigkeit ist der den Vertragsparteien zugestandene Ermessensspielraum abgesehen von den Interessen im Einzelfall auch von der Schwere des Eingriffs abhängig.[130]

4.6. Rechtfertigung eines Eingriffs

Der (datenschutzrechtliche) Gehalt von Art. 8 EMRK gilt nicht absolut und kann deshalb unter bestimmten Voraussetzungen eingeschränkt werden. Gemäss Art. 8 Abs. 2 EMRK muss die einschränkende Massnahme in einem Gesetz vorgesehen sein, ein spezifisches legitimes Ziel verfolgen sowie in einer demokratischen Gesellschaft notwendig erscheinen, damit diese gerechtfertigt werden kann.[131] Die Bestimmung ist eng auszulegen, da sie eine Ausnahme von einem in der Konvention garantierten Recht vorsieht.[132]

Auch hinsichtlich positiver Schutzpflichten ist eine Rechtfertigung zu prüfen. Anders als bei einem Eingriff aufgrund einer negativen Verpflichtung wird bei Vorliegen einer positiven Verpflichtung nur bedingt auf die soeben aufgeführ-

04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 46; EGMR, Urteil v. 06.06.2006, *Segerstedt-Wiberg and others v. Sweden*, Beschwerde Nr. 62332/00, Rz. 99.

128 MATZ, 131. Siehe dazu z.B. EGMR, Urteil v. 04.12.2008, *S. and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 86, 120; EGMR, Urteil v. 02.09.2010, *Uzun v. Germany*, Beschwerde Nr. 35623/05, Rz. 52. Siehe zur Profilbildung als besonders einschneidender Eingriff in das Privatleben EGMR, Urteil v. 12.01.2016, *Szabó and Vissy v. Hungary*, Beschwerde Nr. 37138/14, Rz. 70.

129 Vgl. dazu GONIN/BIGLER, Art. 8 CEDH N 147; VILLIGER, N 651.

130 Vgl. dazu EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 59; EGMR, Urteil v. 25.02.1997, *Z v. Finland*, Beschwerde Nr. 22009/93, Rz. 99.

131 GONIN/BIGLER, Art. 8 CEDH N 2.

132 Siehe dazu EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 47.

ten Einschränkungsmöglichkeiten eingegangen. Vielmehr berücksichtigt der EGMR in einer generellen Abwägung die Interessen des Betroffenen sowie die öffentlichen Interessen. Ausserdem wird den Vertragsparteien im Vergleich mit negativen Verpflichtungen ein grösserer Ermessensspielraum zugestanden.[133] Der Gerichtshof äusserte sich dahingehend, dass die anwendbaren Kriterien ähnlich seien. So müssten jeweils die sich gegenüberstehenden Interessen gegeneinander abgewogen werden. Zudem verfüge der Staat jeweils über einen gewissen Ermessensspielraum.[134]

4.6.1. Gesetzliche Grundlage

Gemäss der ständigen Rechtsprechung des EGMR darf ein Eingriff in die Grundrechte nur erfolgen, wenn eine gesetzliche Grundlage im nationalen Recht vorliegt. Das betreffende Gesetz muss für die betroffene Person zudem zugänglich[135] sein. Des Weiteren muss die betroffene Person die Konsequenzen des Gesetzes vorhersehen[136] können.[137] Abgesehen davon muss der Um-

133 SIEMEN, 197 ff.

134 Siehe dazu EGMR, Urteil v. 07.02.2002, *Mikulić v. Croatia*, Beschwerde Nr. 53176/99, Rz. 58; EGMR, Urteil v. 13.02.2003, *Odièvre v. France*, Beschwerde Nr. 42326/98, Rz. 40. Siehe zum Ganzen SIEMEN, 181 ff. Siehe zu den positiven und negativen Verpflichtungen bei der Prüfung der Rechtfertigung in allgemeiner Weise JACOBS, et al., 349.

135 Bei der Zugänglichkeit kann es darum gehen, ob eine Rechtsquelle publiziert wurde oder nicht. Siehe dazu folgende Urteile EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 53; EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 54; EGMR, Urteil v. 21.06.2011, *Shimovolos v. Russia*, Beschwerde Nr. 30194/09, Rz. 69 f.

136 Z.B. wurde dies in einem Urteil bejaht, weil in den relevanten Gesetzen verständliche Begriffe verwendet wurden und zudem Einschränkungen der Befugnisse sowie ein Kontrollverfahren vorgesehen waren. Ausserdem waren die Voraussetzungen einer Weitergabe der Daten klar und detailliert umschrieben. Siehe dazu EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 55. Bei geheimen Überwachungsmassnahmen müssen die Kriterien und Umstände klar festgelegt werden, auch wenn die von solchen Massnahmen Betroffenen diese nicht vorhersehen können müssen. Siehe dazu EGMR, Urteil v. 02.08.1984, *Malone v. The United Kingdom*, Beschwerde Nr. 8691/79, Rz. 67; EGMR, Urteil v. 16.02.2000, *Amann v. Switzerland*, Beschwerde Nr. 27798/95, Rz. 56. Siehe zum Ganzen auch SIEMEN, 145 ff. m.w.H.

137 JACOBS, et al., 350. Siehe zur ständigen Rechtsprechung des EGMR u.a. EGMR, Urteil v. 26.04.1979, *The Sunday Times v. The United Kingdom*, Beschwerde Nr. 6538/74, Rz. 49; EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 50; EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 52; EGMR, Urteil v. 01.07.2008, *Liberty and others v. The United Kingdom*, Beschwerde Nr. 58243/00, Rz. 59; EGMR, Urteil v. 18.05.2010, *Kennedy v. The United Kingdom*, Beschwerde Nr. 26839/05, Rz. 151; EGMR, Urteil v. 07.07.2015, *M.N. and others v. San Marino*, Beschwerde Nr. 28005/12, Rz. 72; EGMR, Urteil v. 04.12.2015, *Roman Zakharov v. Russia*, Beschwerde Nr. 47143/06, Rz. 228.

fang eines vom Gesetz eingeräumten Ermessensspielraums klar angegeben sein.[138]

Das Erfordernis der gesetzlichen Grundlage wird im materiellen und nicht im formellen Sinn verstanden. Demnach kann auch ungeschriebenes Recht sowie Richterrecht diesem Erfordernis genügen.[139]

Im Zusammenhang mit geheimen Überwachungstätigkeiten hat der EGMR im Urteil *Marper*[140] festgehalten, dass die gesetzliche Grundlage hinreichend präzise formuliert sein müsse, damit es dem Einzelnen möglich sei – allenfalls mit entsprechender Beratung – sein Verhalten danach zu richten. Damit das innerstaatliche Recht diesen Anforderungen gerecht werde, müsse es einen ausreichenden Rechtsschutz gegen Willkür bieten und das den zuständigen Behörden zugestandene Ermessen genau festlegen.[141] Wie detailliert eine gesetzliche Grundlage ausgestaltet sein müsse, hänge wesentlich vom Inhalt des betreffenden Rechtsakts ab. Diesbezüglich seien insbesondere der Regelungsbereich des entsprechenden Aktes und dessen Adressatenkreis massgebend, wobei es zu berücksichtigen gelte, dass in einem Rechtsakt nie alle Eventualitäten abgedeckt werden könnten.[142]

Des Weiteren hielt der EGMR fest, dass es klarer und detaillierter Regeln zum Anwendungsbereich sowie zur Anwendung der fraglichen Massnahme bedürfe. Zudem müsse ein Mindestmass an Garantien festgelegt werden, welche u.a. die Dauer, die Speicherung, die Verwendung, den Zugang Dritter, die Verfahren zur Wahrung der Unversehrtheit und der Vertraulichkeit der Daten sowie die Verfahren für ihre Vernichtung betreffen, um damit angemessene und wirksame Ga-

138 EGMR, Urteil v. 25.03.1983, *Silver and others v. The United Kingdom*, Beschwerde Nr. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, Rz. 88.

139 NETTESHEIM, in: HK-EMRK, Art. 8 EMRK N 102. Siehe dazu aus der Rechtsprechung z.B. EGMR, Urteil v. 02.08.1984, *Malone v. The United Kingdom*, Beschwerde Nr. 8691/79, Rz. 66; EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 19, 52; EGMR, Urteil v. 10.11.2005, *Leyla Şahin v. Turkey*, Beschwerde Nr. 44774/98, Rz. 88. Siehe zur gesetzlichen Grundlage im Allgemeinen SIEMEN, 140 ff.

140 EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04.

141 EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 95.

142 EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 96.

rantien gegen Missbrauch bereitzustellen.[143] Diese Anforderungen gelten insbesondere für die Regelung sensitiver Daten wie DNA-Daten.[144]

Später fügte der EGMR diesen Ausführungen hinzu, dass die Notwendigkeit von solchen Sicherheitsmassnahmen umso grösser sei, wenn Daten automatisiert bearbeitet und erst recht, wenn Daten für polizeiliche Zwecke verwendet würden. Das innerstaatliche Recht solle insbesondere sicherstellen, dass die Daten für die Zwecke, für die sie gespeichert werden, sachdienlich seien und nicht darüber hinausgehen. Die Daten sollten zudem nicht länger aufbewahrt werden, als dies für den Zweck der Datenbearbeitung notwendig sei.[145] Je grösser der Anwendungsbereich der Datenerhebung und damit die Menge sowie Sensibilität der Daten, welche bearbeitet werden, desto wichtiger seien die adäquaten und effektiven Garantien in den verschiedenen Phasen der Datenbearbeitung.[146]

Ob die Sicherheitsmassnahmen im Einzelfall ausreichend sind, prüft der EGMR teilweise unter dem Kriterium der gesetzlichen Grundlage, teilweise aber auch im Rahmen der Notwendigkeit in einer demokratischen Gesellschaft.[147] Unter welchem Kriterium die Prüfung vorgenommen wird, ist inso-

143 EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 99. Dies wurde zwar bereits bei der Prüfung, ob eine ausreichende gesetzliche Grundlage vorhanden ist, ausgeführt. Ob diese Garantien *in casu* vorlagen, prüfte der EGMR aber bei der Verhältnismässigkeit. Die genannten Elemente finden sich auch schon in früheren Urteilen. Siehe dazu z.B. EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71, Rz. 50, 55; EGMR, Urteil v. 02.08.1984, *Malone v. The United Kingdom*, Beschwerde Nr. 8691/79, Rz. 69 ff.; EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 52 ff.

144 Siehe dazu EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 103.

145 EGMR, Urteil v. 17.12.2009, *Gardel v. France*, Beschwerde Nr. 16428/05, Rz. 62; EGMR, Urteil v. 17.12.2009, M.B. *c. France*, Beschwerde Nr. 22115/06, Rz. 53.

146 EGMR, Urteil v. 13.11.2012, M.M. *v. The United Kingdom*, Beschwerde Nr. 24029/07, Rz. 200. Siehe zu den ausreichenden Garantien, mit Hinweisen auf die Rechtsprechung, auch BRKAN, judicialisation and constitutionalisation, 288 f.; PSYCHOGIOPOULOU, 53 f.; KONING, 162 ff.

147 Siehe u.a. folgende Urteile betreffend die Abhandlung der ausreichenden Garantien bei der Prüfung der gesetzlichen Grundlage: EGMR, Urteil v. 24.04.1990, *Kruslin v. France*, Beschwerde Nr. 11801/85, Rz. 35; EGMR, Urteil v. 16.02.2000, *Amann v. Switzerland*, Beschwerde Nr. 27798/95, Rz. 76 f.; EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 56 ff.; EGMR, Urteil v. 24.04.2018, *Benedik v. Slovenia*, Beschwerde Nr. 62357/14, Rz. 132 f. Siehe hingegen u.a. folgende Urteile, in welchen die Garantien bei der Notwendigkeit in einer demokratischen Gesellschaft geprüft wurden: EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71, Rz. 50 ff.; EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81,

fern von untergeordneter Bedeutung, weil wenn die Sicherheitsmassnahmen als nicht ausreichend bewertet werden, in beiden Konstellationen der Eingriff nicht gerechtfertigt werden kann.

4.6.2. Spezifisches legitimes Ziel

Art. 8 Abs. 2 EMRK nennt explizit bestimmte legitime Ziele, deren Verfolgung einen Eingriff in Art. 8 EMRK rechtfertigen kann. Die nationale oder öffentliche Sicherheit[148], das wirtschaftliche Wohl des Landes, die Aufrechterhaltung der Ordnung[149], die Verhütung von Straftaten[150], der Schutz der Gesundheit oder der Moral sowie der Schutz der Rechte und Freiheiten anderer[151] stellen diese Ziele dar.[152]

Rz. 60 ff.; EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 99, 103 ff.; EGMR, Urteil v. 04.12.2015, *Roman Zakharov v. Russia*, Beschwerde Nr. 47143/06, Rz. 232. Vereinzelt hat der EGMR eine gemeinsame Prüfung der Kriterien der gesetzlichen Grundlage und der Notwendigkeit in einer demokratischen Gesellschaft vorgenommen, um die Garantien zu prüfen. Siehe dazu EGMR, Urteil v. 18.05.2010, *Kennedy v. The United Kingdom*, Beschwerde Nr. 26839/05, Rz. 155. Davon abgesehen hat der EGMR die Garantien auch schon im Zusammenhang mit Art. 13 EMRK geprüft. Siehe dazu EGMR, Urteil v. 25.03.1983, *Silver and others v. The United Kingdom*, Beschwerde Nr. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, Rz. 90. Siehe zum Ganzen auch JACOBS, et al., 416.

148 Die nationale Sicherheit wird z.B. bei staatlichen Überwachungs- und Abhörmassnahmen geltend gemacht. Siehe dazu EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 49, 59. Siehe abgesehen davon auch EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71, Rz. 48; EGMR, Urteil v. 28.01.2003, *Peck v. The United Kingdom*, Beschwerde Nr. 44647/98, Rz. 67.

149 Siehe dazu u.a. EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71, Rz. 48; EGMR, Urteil v. 02.08.1984, *Malone v. The United Kingdom*, Beschwerde Nr. 8691/79, Rz. 81; EGMR, Urteil v. 28.01.2003, *Peck v. The United Kingdom*, Beschwerde Nr. 44647/98, Rz. 67.

150 Siehe dazu z.B. EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71, Rz. 48; EGMR, Urteil v. 02.08.1984, *Malone v. The United Kingdom*, Beschwerde Nr. 8691/79, Rz. 81; EGMR, Urteil v. 28.01.2003, *Peck v. The United Kingdom*, Beschwerde Nr. 44647/98, Rz. 67; EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 100.

151 Art. 8 EMRK steht häufig Art. 10 EMRK gegenüber. Siehe dazu u.a. folgende Urteile: EGMR, Urteil v. 10.05.2011, *Mosley v. The United Kingdom*, Beschwerde Nr. 48009/08; EGMR, Urteil v. 07.02.2012, *Hannover v. Germany (No. 2)*, Beschwerde Nr. 40660/08 und 60641/08; EGMR, Urteil v. 16.07.2013, *Wegrzynowski and Smolczewski v. Poland*, Beschwerde Nr. 33846/07; EGMR, Urteil v. 16.06.2015, *Delfi AS v. Estonia*, Beschwerde Nr. 64569/09. Siehe dazu auch JACOBS, et al., 423 f.; BRKAN, judicialisation and constitutionalisation, 289 f.; PSYCHOGIOPOULOU, 35 ff.

152 GONIN/BIGLER, Art. 8 CEDH N 155 ff. m.w.H. Siehe zu diesen Begriffen auch JACOBS, et al., 354 ff.

Bislang wurden diese abschliessend aufgeführten legitimen Zielen nicht näher definiert. Die Begriffe werden jeweils grosszügig interpretiert und den nationalen Behörden wird bei der Auslegung dieser Begriffe ein grosser Ermessensspielraum eingeräumt.[153] Diese Aufzählung ist alternativer Natur, weshalb zur Rechtfertigung eines Eingriffs die Abstützung auf eines der Ziele ausreicht. Üblicherweise werden jedoch mehrere vorgebracht, um die Begründung des Eingriffs zu stärken.[154]

Die Rechtsprechung zeigt, dass sich der EGMR häufig nicht ausführlich mit der Frage auseinandersetzt, ob ein legitimes Ziel im Einzelfall vorliegt.[155] Da die legitimen Ziele sehr breit verstanden werden, dürfte dieses Kriterium in den meisten Fällen nicht problematisch erscheinen. Dem einschlägigen legitimen Ziel kommt jedoch insofern besondere Bedeutung zu, als es im Rahmen der Verhältnismässigkeitsprüfung als Bezugspunkt dient.[156]

4.6.3. Notwendigkeit in einer demokratischen Gesellschaft

Anders als bei den oben genannten Rechtfertigungskriterien, welche objektiv zu beurteilen sind, besteht die Beurteilung des in Art. 8 Abs. 2 EMRK genannten Kriteriums der Notwendigkeit in einer demokratischen Gesellschaft aus einer Abwägung sich gegenüberstehender Interessen.[157] Der EGMR verlangt für die Notwendigkeit in einer demokratischen Gesellschaft, dass die eingreifenden Massnahmen ein «*dringendes soziales Bedürfnis*»[158] bedienen und verhältnismässig sind. Dabei verfügen die Vertragsstaaten über einen gewissen Beurteilungsspielraum, welcher je nach Sachbereich und Einzelfall variieren kann.[159]

153 Siehe dazu SIEMEN, 151 f. m.w.H.

154 MATZ, 127 f.

155 In einigen Urteilen verneinte der EGMR hingegen das Vorliegen eines legitimen Ziels. Siehe dazu EGMR, Urteil v. 25.11.2008, *Biriuk v. Lithuania*, Beschwerde Nr. 23373/03, Rz. 42 ff.; EGMR, Urteil v. 06.04.2017, *Karajanov v. The former Yugoslav Republic of Macedonia*, Beschwerde Nr. 2229/15, Rz. 74 ff. Siehe dazu auch die zustimmende Stellungnahme von Richter Wildhaber, unterstützt durch die Richter Makarczyk, Türmen, Costa, Tulkens, Casadevall und Weber im Urteil EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95. In diesem zustimmenden Sondervotum wurde angezweifelt, dass ein legitimes Ziel mit der Massnahme verfolgt wurde. Es müsse zumindest ein «*reasonable und genuine link*» zwischen dem verfolgten Ziel und dem Eingriff vorliegen. Eine solche Verbindung sei vorliegend nicht ersichtlich. Siehe dazu auch SIEMEN, 170 f.

156 Vgl. dazu VILLIGER, N 649.

157 MATZ, 124 f.

158 Siehe dazu auch EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 58.

159 BREUER, in: EU-Grundrechte-HdB, § 25 N 53. Siehe dazu auch EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 102.

Der Umfang des Ermessens der Staaten bestimmt sich im Einzelfall. Im Bereich des Datenschutzes kann der Ermessensspielraum eng bemessen sein, wenn ein besonders schwerwiegender Eingriff vorliegt oder ein besonders sensitiver Bereich betroffen ist (z.B. geheime Überwachungsmassnahmen oder der Umgang mit medizinischen Daten). Aus der Rechtsprechung des EGMR ist ersichtlich, dass die von Terroristen ausgehende Gefahr grundsätzlich als sehr ernsthaft eingestuft wird. Deshalb können zur Bekämpfung von Terrorismus auch schwerwiegende Eingriffe in das Recht auf Achtung des Privatlebens verhältnismässig sein. Insgesamt zeigt sich in der Rechtsprechung des EGMR, dass den Vertragsstaaten hinsichtlich Massnahmen, welche den Schutz der nationalen Sicherheit verfolgen, ein weiter Ermessensspielraum eingeräumt wird.[160]

Im Rahmen der Notwendigkeit in einer demokratischen Gesellschaft prüft der EGMR zudem – sofern nicht bereits bei der gesetzlichen Grundlage abgehandelt – die adäquaten und effektiven Garantien, welche gegen Missbrauch von Daten vorzusehen sind.[161]

4.7. Abgrenzung zu anderen Grundrechten

Der datenschutzrechtliche Gehalt von Art. 8 EMRK ist u.a. von der Freiheit zum Empfang von Informationen gemäss Art. 10 EMRK abzugrenzen. Letztere Bestimmung verbietet es u.a. einem Staat, eine Person daran zu hindern, Informationen und Ideen zu empfangen und weiterzugeben.[162]

Ausserdem weist das aus Art. 8 EMRK abgeleitete Recht auf Zugang zu den Daten gewisse Gemeinsamkeiten mit dem Recht auf eine wirksame Beschwerde gemäss Art. 13 EMRK auf.[163] Letztere Bestimmung verlangt im Allgemeinen nicht unbedingt einen gerichtlichen Rechtsschutz. Das Beschwerdeverfahren muss jedoch effektiv und wenigstens gerichtsförmig sein. Die im Einzelfall gewährten Befugnisse resp. Verfahrensgarantien entscheiden darüber, ob eine Beschwerde als wirksam angesehen werden kann. Ausserdem wird eine gewisse Unabhängigkeit der Beschwerdeeinrichtung gegenüber der Entschei-

160 SIEMEN, 176. Siehe dazu auch EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 59. Vgl. dazu ausserdem EGMR, Urteil v. 28.10.1994, *Murray v. The United Kingdom*, Beschwerde Nr. 14310/88, Rz. 90 ff. Siehe zu einer Übersicht über die Beurteilung der Verhältnismässigkeit von einigen Urteilen betreffend Überwachungsmassnahmen PSYCHOGIOPOULOU, 55 f.

161 Siehe dazu Kapitel II.4.6.1.

162 Siehe dazu DAIBER, in: HK-EMRK, Art. 10 EMRK N 16 ff. m.w.H.

163 FRA, biometrics, 99 f.

dungsinstanz gefordert. Davon abgesehen muss dem Betroffenen das rechtliche Gehör gewährt werden. Es wird jedoch nicht explizit verlangt, dass die Beschwerdeinstanz eine rechtlich verbindliche Entscheidung zu treffen vermag. Entscheidend ist hingegen, ob die Entscheidungen der Kontrollbehörden tatsächlich von den kontrollierten Behörden beachtet werden.[164]

Des Weiteren ist auch eine Abgrenzung mit dem in Art. 6 EMRK verankerten Recht auf ein faires Verfahren vorzunehmen.[165] Diese Bestimmung stellt im Verhältnis zu Art. 13 EMRK die speziellere Bestimmung dar. Eine Verletzung von Art. 6 EMRK absorbiert folglich auch den Gehalt von Art. 13 EMRK. Art. 6 EMRK stellt bestimmte Anforderungen einerseits an das Gericht und andererseits an ein faires Verfahren.[166]

Datenschutzrechtliche Elemente finden sich demnach abgesehen von Art. 8 EMRK auch in anderen Grundrechten. Diese werden teilweise gemeinsam geltend gemacht.[167]

5. Informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV

5.1. Rechtliche Verankerung

Ausgehend vom *Volkszählurteil*[168] des deutschen Bundesverfassungsgerichts aus dem Jahre 1983 wurde das sog. Recht auf informationelle Selbstbestimmung auch in das schweizerische Recht übernommen.[169] In diesem Urteil wurde festgehalten, dass sich die Persönlichkeit der Einzelnen nur frei ent-

164 MATZ, 138 ff. m.w.H.

165 Dies betrifft nur Zivil- und Strafverfahren. Oft dürften im Zusammenhang mit dem Datenschutz jedoch verwaltungsgerichtliche Verfahren betroffen sein. Siehe dazu SIEMEN, 204 ff. m.w.H.

166 MATZ, 145 f.

167 Siehe dazu z.B. folgende Urteile: EGMR, Urteil v. 06.09.1978, *Klass and others v. Germany*, Beschwerde Nr. 5029/71; EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81; EGMR, Urteil v. 27.08.1997, *M.S. v. Sweden*, Beschwerde Nr. 74/1996/693/885; EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95. Siehe zur Thematik auch SIEMEN, 204 ff. m.w.H.

168 BVerfGE 65, 1 ff. = EuGRZ 1983, 577 ff.

169 Das BGer bezog sich im Jahr 1987 erstmals in BGE 113 Ia 1, E. 4b/bb auf das Volkszählurteil (resp. das Zensus-Urteil) des deutschen Bundesverfassungsgerichts. Im selben Jahr wurden in BGE 113 Ia 257, E. 4c) weitere Konkretisierungen vorgenommen. Damals wurde der Begriff der informationellen Selbstbestimmung noch nicht ausdrücklich verwendet.

falten könne, wenn diese vor einer unkontrollierten Bearbeitung der persönlichen Daten geschützt werden. Abgesehen von diesem Schutz sei dem Einzelnen zudem das Recht zuzugestehen, eigenständig über die Veröffentlichung sowie Verbreitung seiner Daten zu entscheiden.[170] Nachdem die informationelle Selbstbestimmung zunächst als ungeschriebenes Grundrecht anerkannt war, wurde sie in der Totalrevision der BV im Jahr 1999 als Teilgehalt der Privatsphäre explizit in Art. 13 Abs. 2 BV verankert.[171]

5.2. Adressatenkreis und Grundrechtsträger der BV

In der BV werden die Grundrechtsträger nicht in allgemeiner Weise festgelegt. Vielmehr definiert jedes Grundrecht einzeln, wer sich darauf berufen kann.[172]

Die Grundrechtsadressaten lassen sich Art. 35 Abs. 2 BV entnehmen. Demnach ist an die Grundrechte gebunden und verpflichtet, zu ihrer Verwirklichung beizutragen, wer staatliche Aufgaben wahrnimmt.[173]

5.3. Persönlicher und sachlicher Schutzbereich

Art. 13 BV sind insgesamt fünf Teilgarantien zu entnehmen: Neben der in Abs. 2 verankerten informationellen Selbstbestimmung wird in Abs. 1 das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz gewährleistet.[174] Art. 8 EMRK hat die Ausgestaltung von Art. 13 BV in massgebender Weise beeinflusst. So ist der Wortlaut von Art. 13 Abs. 1 BV nicht zufällig gewählt, sondern entspricht fast wortwörtlich Art. 8 EMRK.[175] Daher erstaunt es nicht, dass diese Schutzbereiche weitgehend identisch sind.[176] Anders als in Art. 8 EMRK wird der datenschutzrechtliche Gehalt in der BV jedoch separat, in Art. 13 Abs. 2 BV, aufgeführt.[177]

---

170 Siehe dazu BVerfGE 65, 1 (41 ff. E. 1a) = EuGRZ 1983, 577 ff. (insbesondere 588). Siehe zu diesem Urteil auch ALBERS, 151 ff.; MATZ, 95 f.; VON GRAFENSTEIN, 147.

171 Siehe dazu BLONSKI, 45 ff. m.w.H. Die BV geniesst grundsätzlich Vorrang vor dem übrigen Bundesrecht und geht somit abweichenden Bestimmungen vor, welche auf einer tieferen Stufe angesiedelt sind. Dieser Grundsatz wird jedoch durch Art. 190 BV relativiert. Siehe dazu BELSER, in: BSK BV, Einleitung N 50 ff. m.w.H.

172 KIENER/KÄLIN/WYTTENBACH, N 197.

173 BUNDESRAT, Botschaft BV 1996, 193.

174 DIGGELMANN, in: BSK BV, Art. 13 BV N 8.

175 Anstelle des Begriffs «*Korrespondenz*» in Art. 8 EMRK ist in der BV der Begriff «*Brief-, Post- und Fernmeldeverkehr*» aufgeführt.

176 Siehe dazu BGE 137 I 167, E. 3.2.

177 Vgl. dazu DIGGELMANN, in: BSK BV, Art. 13 BV N 1.

Der genaue Schutzgehalt des eigenständigen Grundrechts gemäss Art. 13 Abs. 2 BV ist umstritten. Gemäss dem Wortlaut schützt der verfassungsrechtliche Datenschutz vor Missbrauch persönlicher Daten. Die herrschende Lehre[178] sowie die Rechtsprechung[179] gehen jedoch davon aus, dass dieser Wortlaut missglückt sei und sich aus diesem Grundrecht vielmehr ein Recht auf informationelle Selbstbestimmung ableiten lasse. Der Anspruch auf informationelle Selbstbestimmung impliziere, «*dass jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden*».[180] In der Lehre wird jedoch auch die Ansicht vertreten, dass eine solche Auslegung klar dem Wortlaut widerspreche. Viele Datenbearbeitungen seien unproblematisch. Ein umfangreicherer Schutzbereich führe nicht zu einem umfassenderen Schutz.[181] Diese Argrumente sind nicht von der Hand zu weisen und haben durchaus ihre Berechtigung. Unter der Berücksichtigung des *Volkszählurteils*, welches den Ausgangspunkt für Art. 13 Abs. 2 BV darstellte, erscheint es jedoch naheliegender, dass der Gesetzgeber über den Schutz vor missbräuchlicher Datenbearbeitung hinausgehen wollte. Insofern wird der herrschenden Lehre sowie der ständigen Rechtsprechung des BGer gefolgt.

Vom Schutzbereich erfasst sind alle personenbezogenen Daten einer Person, d.h. alle Daten, die sich auf eine bestimmte oder zumindest bestimmbare Person beziehen. Dabei spielt es keine Rolle, ob die Daten korrekt oder besonders bedeutsam sind. Auch ob die Angaben der Öffentlichkeit zugänglich sind, ist irrelevant. Insbesondere Angaben betreffend die körperlichen oder psychischen Merkmale einer Person, deren politische Ansichten, ihre wirtschaftlichen sowie sozialen Verhältnisse, aber auch der Name, der Beruf, die Fingerabdrücke oder Fotos einer Person sind vom Schutzbereich des Grundrechts erfasst.[182] Bei der Beurteilung, ob personenbezogene Daten vorliegen oder nicht, wird auf die Perspektive des Datenbearbeiters abgestellt. Massgeblich

178 Siehe dazu u.a. KIENER/KÄLIN/WYTTENBACH, N 761 ff.; MÜLLER/SCHEFER, 164; DIGGELMANN, in: BSK BV, Art. 13 BV N 32 f.; FLÜCKIGER, 847 f.; SCHWEIZER/STRIEGEL, in: St. Galler Kommentar, Art. 13 Abs. 2 BV N 79 f. Vgl. dazu auch BIAGGINI, Art. 13 BV N 11.

179 Siehe dazu u.a. BGE 120 II 118, E. 3a; BGE 128 II 259, E. 3.2; BGE 129 I 232, E. 4.3.1; BGE 133 I 77, E. 5.3; BGE 138 II 346, E. 8.2; BGE 140 I 2, E. 9.1; BGE 140 I 381, E. 4.1; BGE 142 II 340, E. 4.2; BGE 145 IV 42, E. 4.2.

180 BGE 144 II 77, E. 5.2; BGE 144 II 91, E. 4.4 (jeweils mit Hinweisen auf weitere Urteile).

181 Siehe dazu u.a. BELSER, grundrechtlicher Rahmen, § 6 N 118 ff. m.w.H.; GÄCHTER/EGLI, Rz. 24 ff. m.w.H.

182 BELSER/WALDMANN, 79.

ist, ob eine Person anhand der vorhandenen Angaben – im Rahmen eines verhältnismässigen Aufwands – individualisiert werden kann.[183]

Die informationelle Selbstbestimmung umfasst zudem jeglichen Umgang mit personenbezogenen Daten – also bspw. das Erheben, Verarbeiten, Aufbewahren und Weitergeben von Daten – und gilt unbesehen des Verfahrens und der Art der Datenerhebung.[184]

5.4. Positive Schutzpflichten

Obwohl dies aus Art. 13 Abs. 2 BV nicht explizit hervorgeht, ist es unstrittig, dass die Bestimmung drei Ansprüche mit grundrechtlichem Charakter enthält. So besteht ein Anspruch auf Auskunft resp. Einsicht, ein Anspruch auf Berichtigung falscher Daten sowie ein Anspruch auf Löschung ungeeigneter resp. nicht (mehr) benötigter Daten. Der Anspruch auf Einsicht resp. Auskunft stellt dabei eine Art Grundpfeiler des Datenschutzrechts dar, da dieser die Voraussetzung für die Geltendmachung der anderen Ansprüche darstellt.[185]

Das Auskunftsrecht stellt einen wesentlichen Aspekt der informationellen Selbstbestimmung dar und steht jeder urteilsfähigen Person bedingungslos zu. Auf dieses Recht kann vorgängig nicht verzichtet werden.[186] Es bezieht sich auf eigene Daten, wobei kein spezifisches Einsichtsinteresse geltend zu machen ist. Dem Anspruch auf Auskunft können jedoch Geheimhaltungsinteressen von Dritten gegenüberstehen. In diesen Fällen ist eine Güterabwägung vorzunehmen.[187] Erweisen sich – im Rahmen der Einsichtnahme – Daten als falsch, so darf die betroffene Person deren Berichtigung verlangen. Bei widerrechtlich erhobenen Daten oder solchen, welche zu lange aufbewahrt werden, besteht ein Anspruch auf Löschung.[188]

In der Lehre wird davon abgesehen die Ansicht vertreten, dass dem Grundrecht auch ein Anspruch auf Aufsicht sowie auf eine wirksame Beschwerde zu entnehmen ist. Der Einzelne muss nämlich die Möglichkeit haben, seine Ansprüche auf dem Rechtsweg durchsetzen zu können. Da es für den Einzelnen aufgrund der zahlreichen Datenbearbeitungen zunehmend schwieriger

183 Blonski, 54.
184 Schweizer/Striegel, in: St. Galler Kommentar, Art. 13 Abs. 2 BV N 85.
185 Biaggini, Art. 13 BV N 14.
186 Siehe zum Auskunftsrecht ausführlich Schweizer/Striegel, in: St. Galler Kommentar, Art. 13 Abs. 2 BV N 101 ff.
187 Müller/Schefer, 168 f.
188 Kiener/Kälin/Wyttenbach, N 767.

ist, seine Rechte wahrzunehmen, besteht auch ein grundrechtlicher Anspruch auf staatliche Aufsicht und Kontrolle. Dieser richtet sich jedoch an den Gesetzgeber und ist nicht justiziabel.[189]

5.5. Eingriffe in den Schutzbereich

Jede staatliche Datenbearbeitung stellt einen Grundrechtseingriff dar.[190]

Eingriffe in ein Grundrecht können unterschiedlich intensiv ausfallen. Allgemeingültige Kriterien, welche bei der Beurteilung der Schwere eines Eingriffs jeweils zu berücksichtigen wären, gibt es nicht. Die Schwere eines Eingriffs ist jeweils im Einzelfall unter Berücksichtigung aller Umstände zu bestimmen, wobei sich das BGer im Allgemeinen u.a. folgender Kriterien bedient: die Intensität der Beeinträchtigung der Rechte, die Art und Dauer des Eingriffs, die Anzahl der betroffenen Personen oder die Auswirkungen für die Betroffenen.[191]

Im Bereich des Datenschutzes kann auch die Art der Daten, welche bearbeitet werden, bei der Beurteilung der Eingriffsintensität eine Rolle spielen.[192] Der Rechtsprechung des BGer ist zu entnehmen, dass die Bearbeitung von besonders schützenswerten Personendaten[193] grundsätzlich einem schwerwiegenden Eingriff gleichkommt, insbesondere wenn die Datenerfassung systematisch und ohne Kenntnis der betroffenen Personen erfolgt.[194] Auch bei der Erstellung von Persönlichkeitsprofilen, also wenn mehrere Einzeldaten ein umfangreiches Bild einer Person ergeben, nimmt das BGer regelmässig einen

189 Belser, grundrechtlicher Rahmen, § 6 N 104 f.

190 Müller/Schefer, 170.

191 Epiney, in: BSK BV, Art. 36 BV N 21. Das BGer hat jedoch festgehalten, dass der individuelle Grundrechtseingriff nicht grundsätzlich schwerer wiegt, nur weil eine grosse Anzahl von Personen betroffen ist. Siehe dazu BGE 133 I 77, E. 5.3. Siehe als Beispiel für einen schweren Eingriff BGE 143 I 253, E. 4.8. In der Lehre werden noch weitere Kriterien genannt, welche bei der Beurteilung der Schwere des Eingriffs eine Rolle spielen können. Siehe dazu Epiney/Nüesch/Rovelli, 140.

192 Siehe dazu z.B. BGE 144 I 126, E. 5.3. *In casu* wertete das BGer die Bearbeitung von sog. Randdaten «*als deutlich weniger einschneidend*» als wenn es sich um den Inhalt der Kommunikation gehandelt hätte.

193 Dazu zählen u.a. «*Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten*». Siehe dazu BGE 122 I 360, E. 5b/dd. Siehe zur Definition von besonders schützenswerten Daten auch Art. 5 lit. c DSG.

194 Siehe dazu z.B. BGE 122 I 360, E. 5c.

schweren Eingriff an.[195] Bei sog. erkennungsdienstlichen Massnahmen[196] sowie deren Aufbewahrung ist hingegen von einem leichten Eingriff auszugehen.[197]

Die Schwere eines Eingriffs spielt im Rahmen der Rechtfertigung eines Grundrechtseingriffs insbesondere bei den Anforderungen an die gesetzliche Grundlage sowie bei der Prüfung der Verhältnismässigkeit eine Rolle.[198]

5.6. Rechtfertigung eines Eingriffs

Die Voraussetzungen für die Rechtfertigung eines Eingriffs in die informationelle Selbstbestimmung ergeben sich, wie für jeden Eingriff in Grundrechte, aus Art. 36 BV. Der Eingriff bedarf einer gesetzlichen Grundlage, muss einem öffentlichen Interesse oder dem Schutz von Grundrechten Dritter dienen und verhältnismässig sein. Ausserdem darf der Kerngehalt des Grundrechts nicht angetastet werden.[199]

5.6.1. Gesetzliche Grundlage

Die BV stellt ähnliche Anforderungen an die gesetzliche Grundlage wie die EMRK. Anders als bei der EMRK kann jedoch ein Gesetz im materiellen Sinn nicht immer den Anforderungen an die gesetzliche Grundlage gerecht werden. So verlangen schwerwiegende Eingriffe in Grundrechte eine qualifizierte gesetzliche Grundlage, also ein Gesetz im formellen Sinn.[200] Die gesetzliche

195 Siehe dazu z.B. BGE 143 I 253, E. 3.2. Siehe zur Abgrenzung des Begriffs «*Persönlichkeitsprofil*» zum Begriff «*Profiling*» STENGEL/STÄUBLE m.w.H.

196 «*Als erkennungsdienstliche Massnahmen gelten Handlungen, welche staatlichen Organen, namentlich der Polizei, dabei helfen, Personen zu identifizieren. Herkömmlicherweise geschieht dies durch die Erfassung äusserer Körpermerkmale bzw. äusserlich wahrnehmbaren Merkmale einer Person wie das Erstellen von Fotografien, die Abnahme von Finger- oder Handballenabdrücken, die Signalementsaufnahme, die Körpervermessung oder die Anordnung von Schrift- oder Sprechproben. Erkennungsdienstliche Massnahmen verfolgen das doppelte Ziel, einerseits aufgrund der erfassten Merkmale nicht aufgeklärte Straftaten bestimmten Personen zuzuordnen und andererseits bei künftigen Taten eine Wiedererkennung zu ermöglichen.*» BGE 128 II 259, E. 3.4.1.

197 Siehe dazu z.B. BGE 145 IV 263, E. 3.4 (mit Hinweisen auf weitere Urteile). *In casu* ging es um die Erstellung eines DNA-Profils für allfällige künftige Straftaten.

198 EPINEY, in: BSK BV, Art. 36 BV N 21.

199 Bei der polizeilichen Generalklausel sind Einschränkungen von Grundrechten auch ohne gesetzliche Grundlage möglich. Siehe dazu Art. 36 Abs. 1 BV; EPINEY, in: BSK BV, Art. 36 BV N 40 ff. m.w.H.

200 Auf Bundesebene wird ein Bundesgesetz verlangt. Auf kantonaler Ebene ein Gesetz, welches vom kantonalen Parlament verabschiedet wurde. Auch Staatsverträge können u.a. als gesetzliche Grundlage dienen. Siehe dazu EPINEY, in: BSK BV, Art. 36 BV N 33. Das BGer

Grundlage muss zudem hinreichend bestimmt sein. So muss es dem Einzelnen möglich sein, vorherzusehen, in welchen Situationen und unter welchen Voraussetzungen ein Grundrechtseingriff zulässig ist. Die betroffenen Personen sollen ihr Verhalten nach der Rechtsnorm richten und dessen Folgen im gegebenen Fall abschätzen können.[201] Die Anforderungen an die Bestimmtheit sind anhand des Einzelfalls zu bestimmen. Grundsätzlich gilt, dass die Anforderungen steigen, je schwerer der Grundrechtseingriff ist resp. je stärker die Auswirkungen auf die Rechtsstellung des Einzelnen sind.[202]

Das BGer verweist in seiner Rechtsprechung im Bereich des Datenschutzes zudem regelmässig auf die in der EGMR-Rechtsprechung aufgeführten klaren und präzisen Regeln. Diese müssen den Anwendungsbereich und die Anwendung der in das Grundrecht eingreifenden Massnahme festlegen und gewisse Mindestanforderungen an die Datenbearbeitung (u.a. in Bezug auf die Dauer, die Speicherung, die Verwendung, den Zugang Dritter, die Verfahren zur Wahrung der Integrität und Vertraulichkeit der Daten und die Verfahren für ihre Vernichtung) vorschreiben.[203] Insbesondere ist gemäss dem BGer auch der Verwendungszweck der Daten festzulegen. Dieser dient dazu, klare Ziele und ein öffentliches Interesse der in das Grundrecht eingreifenden Massnahmen zu bestimmen sowie deren Verhältnismässigkeit zu überprüfen.[204]

Des Weiteren fordert das BGer – wie auch der EGMR – angemessene und wirksame Garantien gegen Missbrauch. Diese müssen insbesondere bei einer automatischen Datenbearbeitung und erst recht, wenn die Daten für polizeiliche Zwecke verwendet werden, vorhanden sein.[205] Diese Sicherheitsmassnahmen beurteilt das BGer – wie auch der EGMR – im Rahmen der gesetzlichen Grundlage oder im Rahmen der Verhältnismässigkeit.[206]

verlangt bei schweren Eingriffen «*in den wesentlichen Punkten eine klare unzweideutige Grundlage in einem formellen Gesetz*». Siehe dazu BGE 122 I 360, E. 5b/bb.

201 Belser, grundrechtlicher Rahmen, § 6 N 125 f.

202 Epiney, in: BSK BV, Art. 36 BV N 35 f.

203 Siehe dazu z.B. BGE 137 I 167, E. 3.2.

204 Siehe dazu BGE 146 I 11, E. 3.3.2.

205 BGE 137 I 167, E. 3.2. Vgl. dazu auch BGE 138 I 6, E. 4.3; BGE 144 I 126, E. 8.3.4; BGE 147 I 103, E. 17.5.1.

206 Siehe zur Prüfung bei der gesetzlichen Grundlage: BGE 146 I 11, E. 3.3.1. Siehe zur Prüfung bei der Verhältnismässigkeit: BGE 133 I 77, E. 5.4; BGE 138 I 6, E. 4.3; BGE 144 I 126, E. 8.3.4.

5.6.2. Öffentliches Interesse resp. Grundrechtsschutz Dritter

Ein Grundrechtseingriff muss durch ein öffentliches Interesse resp. den Grundrechtsschutz Dritter gerechtfertigt werden können.[207] Anders als in Art. 8 Abs. 2 EMRK ist der BV nicht explizit zu entnehmen, welche konkreten Interessen darunterfallen. Grundsätzlich besteht diesbezüglich ein grosser Gestaltungsspielraum. Abgesehen vom Schutz der öffentlichen Sicherheit und Ordnung sowie der öffentlichen Gesundheit – als sog. Polizeigüter – sind auch andere Interessen z.B. in wirtschaftlicher oder kultureller Hinsicht denkbar. Das öffentliche Interesse muss hinreichend konkret begründet werden.[208]

Im Bereich des Datenschutzes ist davon auszugehen, dass die Aufbewahrung von unrichtigen Daten grundsätzlich nicht im öffentlichen Interesse liegen kann.[209]

Die öffentlichen Interessen können unterschiedlich gewichtet werden. Dies wird bei der Prüfung der Verhältnismässigkeit oder auch bei der Frage, ob das festgestellte öffentliche Interesse den fraglichen Eingriff überhaupt zu rechtfertigen vermag, berücksichtigt.[210]

5.6.3. Verhältnismässigkeit

Das Erfordernis der Verhältnismässigkeit des Eingriffs umfasst die Aspekte der Geeignetheit, der Erforderlichkeit sowie der Zumutbarkeit. Demnach muss die Massnahme geeignet sein, das verfolgte öffentliche Interesse zu verwirklichen. Ausserdem muss sie das mildeste Mittel – mit vergleichbarer Wirkungsprognose – darstellen und muss für die Betroffenen zumutbar sein.[211] Die Verhältnismässigkeit wird in der Regel umso strenger geprüft, je schwerwiegender der Grundrechtseingriff ist.[212]

Die Kriterien der Erforderlichkeit sowie der Geeignetheit werden vom BGer anhand einer Analyse der entsprechenden gesetzlichen Bestimmungen beurteilt. Verlangt wird eine gewisse Plausibilität, wobei häufig auf die allgemeine Lebenserfahrung abgestellt wird und nur in wenigen Fällen Gutachten zu Rate

---

207 Art. 36 Abs. 2 BV.

208 Epiney, in: BSK BV, Art. 36 BV N 48 f. Siehe dazu auch Belser, grundrechtlicher Rahmen, § 6 N 134 ff.; Belser/Waldmann, 81. Siehe zu einer eher ausführlichen Beurteilung des öffentlichen Interesses BGE 148 I 233, E. 5.2.

209 Schweizer/Striegel, in: St. Galler Kommentar, Art. 13 Abs. 2 BV N 130.

210 Epiney, in: BSK BV, Art. 36 BV N 50.

211 Glass, 55 f.

212 Epiney, in: BSK BV, Art. 36 BV N 59.

gezogen werden.[213] Der Rechtsprechung des BGer ist zu entnehmen, dass in der Regel keine allzu hohen Hürden an die Geeignetheit einer Massnahme gestellt werden.[214] Bei der Beurteilung der Erforderlichkeit einer Massnahme ist massgebend, dass diese «*in sachlicher, räumlicher, zeitlicher und personeller Hinsicht nicht über das Notwendige hinausgehen*» darf.[215] Bei der Prüfung der Zumutbarkeit des Eingriffs stellt sich die Frage nach der Zweck-Mittel-Relation, wobei abgewogen wird, ob das eingesetzte Mittel als sachgerecht im Verhältnis zum Zweck erscheint.[216] Der Beurteilung der Zumutbarkeit kommt im Rahmen der Prüfung der Verhältnismässigkeit der Massnahme eine grosse Bedeutung zu.[217]

Zudem werden in der Verhältnismässigkeitsprüfung auch die angemessenen und wirksamen Garantien geprüft, welche auch die EGMR-Rechtsprechung fordert, sofern diese nicht bereits im Rahmen der gesetzlichen Grundlage beurteilt wurden.[218]

5.6.4. Kerngehalt

Beim Kerngehalt handelt es sich um den unantastbaren Wert eines Grundrechts, in welchen nicht eingegriffen werden darf. Der Kerngehalt erschliesst sich jeweils aus der Reichweite der einzelnen Grundrechte. Grundsätzlich handelt es sich dabei meist um einen Teilgehalt des Schutzbereichs.[219]

Das BGer hat sich bis anhin (noch) nicht zum Kerngehalt der informationellen Selbstbestimmung geäussert. Seiner Rechtsprechung sind jedoch Hinweise zu entnehmen, welche auf den Kerngehalt schliessen lassen. So wurde vom BGer die Erstellung, Speicherung sowie die (zukünftige) Verwendung eines DNA-Profils explizit nicht als Eingriff in den Kernbereich betrachtet, da solche Profile keine genetischen Informationen enthalten, weil sie auf der Grundlage der nicht-codierenden Stränge erstellt werden. Somit liege keine zwangsweise Ausforschung des genetischen Programms eines Individuums vor.[220] In einem

213 Epiney, in: BSK BV, Art. 36 BV N 58.

214 Siehe dazu z.B. BGE 144 I 126, E. 8.1. *In casu* hatte der Beschwerdeführer die Geeignetheit der Massnahme in Zweifel gezogen, da diese nicht empirisch erwiesen sei. Das BGer äusserte sich dazu dahingehend, dass eine Massnahme hinsichtlich des angestrebten Zwecks «*nicht gänzlich daran vorbei zielen*» dürfe.

215 BGE 140 I 353, E. 8.7.2.

216 Belser, grundrechtlicher Rahmen, § 6 N 143.

217 Belser/Waldmann, 81.

218 Siehe dazu Kapitel II.5.6.1.

219 Vgl. dazu Epiney, in: BSK BV, Art. 36 BV N 61 ff.

220 BGE 128 II 259, E. 3.7.

anderen Urteil hatte das BGer davon abgesehen, sich zum Kerngehalt zu äussern, da kein breiter und flächendeckender Einsatz der automatischen Fahrzeugfahndung und Verkehrsüberwachung zur Debatte stand.[221]

In der Literatur wird aufgeführt, dass der Kerngehalt verletzt sein könnte, wenn das Recht auf Zugang zu den eigenen Daten vollständig ausgeschlossen werden würde oder wenn es nicht mehr möglich wäre, sich der Überwachung im öffentlichen Raum zu entziehen. Auch wird argumentiert, dass wenn durch die Erhebung von Daten eine Person «*durchsichtig*» erscheinen würde oder wenn mit der Art und Weise der Datenerhebung gegen die Menschenwürde verstossen würde, der Kerngehalt betroffen sein könnte.[222]

5.7. Abgrenzung zu anderen Grundrechten

Das Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV wurde vom Recht auf Akteneinsicht, dem Recht auf persönliche Freiheit sowie dem Recht auf Schutz der Privatsphäre abgeleitet und muss demnach auch von diesen abgegrenzt werden.[223]

Das im Zusammenhang mit Art. 13 Abs. 2 BV gewährte Recht auf Auskunft ist gewissermassen mit dem Recht auf Akteneinsicht gemäss Art. 29 Abs. 2 BV verwandt. Während letzteres jedoch nur in einem hängigen Verfahren vor Justiz- resp. Administrativbehörden geltend gemacht werden kann, ist ersteres nicht von einem solchen Verfahren abhängig. Des Weiteren steht das Akteneinsichtsrecht jeder beteiligten Person zu und bezieht sich auf sämtliche Daten. Das in Rahmen der informationellen Selbstbestimmung gewährte Recht auf Auskunft beschränkt sich hingegen auf eigene Daten, welche bearbeitet werden.[224]

Das Verhältnis verschiedener Grundrechte im Bereich des Persönlichkeitsschutzes ist nicht klar geregelt. Dies liegt einerseits daran, dass mehrere Grundrechte den Schutz der Persönlichkeit regeln und andererseits, dass die Schutzbereiche – insbesondere von Art. 13 BV – eher umfassend geregelt sind. Neben der informationellen Selbstbestimmung können deshalb auch der Schutz der Privatsphäre gemäss Art. 13 Abs. 1 BV und/oder das Recht auf per-

221 BGE 146 I 11, E. 3.1.2.

222 Siehe dazu SCHWEIZER/STRIEGEL, in: St. Galler Kommentar, Art. 13 Abs. 2 BV N 133 m.w.H. Siehe dazu auch BELSER, grundrechtlicher Rahmen, § 6 N 156.

223 BLONSKI, 48 f.

224 BELSER, grundrechtlicher Rahmen, § 6 N 175 f.; BLONSKI, 48 f.

sönliche Freiheit gemäss Art. 10 Abs. 2 BV einschlägig sein.[225] Art. 13 Abs. 2 BV geht dabei meistens als speziellere Bestimmung vor.[226] Das Verhältnis von Art. 13 und Art. 10 Abs. 2 BV bleibt letztlich ungeklärt. So wird teilweise vertreten, dass Art. 10 Abs. 2 BV nur noch zum Zuge kommt, wenn das Grundrecht auf Privatsphäre nicht einschlägig ist. Andere hingegen sind der Ansicht, dass die Schutzbereiche der beiden Grundrechte mehrheitlich identisch sind.[227] Da die beiden Grundrechte ähnliche Rechtsgüter schützen, erscheint eine Abgrenzung nicht immer einfach.[228] Insofern kann es – auch im Zusammenhang mit dem Datenschutz – ratsam sein, sich auf beide Normen zu berufen.[229]

Ferner ist die informationelle Selbstbestimmung von der Informationsfreiheit abzugrenzen. Letztere gründet auf der freien Demokratie, wobei eine allfällige Persönlichkeitsnähe unerheblich ist.[230] Zudem schliesst die Informationsfreiheit gemäss Art. 16 Abs. 2 BV sämtliche – und nicht nur personenbezogene Angaben – ein, beschränkt sich jedoch auf öffentlich zugängliche Quellen.[231]

Bei besonders schützenswerten Daten kann zudem auch die Glaubens- und Gewissensfreiheit gemäss Art. 15 BV betroffen sein.[232]

---

225 BELSER, grundrechtlicher Rahmen, § 6 N 157 ff. m.w.H. Mit einer Datenbearbeitung kann in die psychische oder physische Integrität eingegriffen werden, z.B. durch eine Blutentnahme, Fragen zum Intim- resp. Geheimbereich oder durch die Beschlagnahme resp. Veröffentlichung persönlicher Dokumente oder Bilder. Siehe dazu BELSER, rechtliche Tragweite, 30 m.w.H.

226 Es ist jedoch zu beachten, dass die persönlichen Angaben nur unter die informationelle Selbstbestimmung fallen, sofern diese nicht vom Fernmeldegeheimnis resp. der Unverletzlichkeit der Wohnung gemäss Art. 13 Abs. 1 BV erfasst sind. Vgl. dazu MÜLLER/SCHEFER, 164 f.

227 BELSER, grundrechtlicher Rahmen, § 6 N 29.

228 Vgl. dazu BELSER, grundrechtlicher Rahmen, § 6 N 32.

229 BIAGGINI, Art. 13 BV N 2, 13 (mit Hinweisen auf die Rechtsprechung). Siehe zum Ganzen auch KIENER/KÄLIN/WYTTENBACH, N 781.

230 MÜLLER/SCHEFER, 182.

231 Vgl. dazu BELSER, grundrechtlicher Rahmen, § 6 N 178 ff.

232 BELSER, grundrechtlicher Rahmen, § 6 N 93.

6. Schutz personenbezogener Daten gemäss Art. 8 GRC

6.1. Rechtliche Verankerung

Der Datenschutz wurde erstmals in der GRC als eigenständiges Grundrecht verankert.[233] Mit Art. 8 GRC sollten die in den Mitgliedstaaten unterschiedliche Ansichten zum Datenschutz harmonisiert werden. Während der Datenschutz in einigen Mitgliedstaaten ein eigenes Recht darstellte, wurde dieser in anderen Staaten als Teil des Rechts auf Kommunikation oder des Rechts auf Privatleben verstanden. Mit der eigenständigen Bestimmung in Art. 8 GRC wurde der Schutz der Individuen gegen neue Risiken, welche durch die Bearbeitung von Daten verursacht werden, gestärkt.[234]

Art. 8 GRC ist nicht die einzige primärrechtliche Grundlage im Bereich des Datenschutzes. Der Inhalt von Art. 8 Abs. 1 und 3 GRC findet sich auch in Art. 16 AEUV. Diese Norm stellt die gesetzliche Grundlage für die EU-Gesetzgebung im Datenschutz dar.[235] Im Bereich der gemeinsamen Aussen- und Sicherheitspolitik findet sich diese Grundlage in Art. 39 EUV.[236]

EU-Grundrechte sind Teil des Primärrechts und gehen dem Sekundärrecht vor. Letzteres ist unwirksam, wenn es nicht im Einklang mit den Grundrechten steht. Deswegen ist das Sekundärrecht grundrechtskonform auszulegen. Gleiches gilt für das Tertiärrecht, also auf Ermächtigungen im Sekundärrecht gestütztes Recht.[237]

Das Verhältnis von Art. 8 GRC und dem einschlägigen Sekundärrecht ist jedoch nicht eindeutig. So wird das Sekundärrecht teilweise herangezogen, um das

---

233 Siemen, 24. Siehe zur Entstehungsgeschichte der GRC Jarass/Kment, § 1 N 16 ff. Siehe zur Rechtsprechung des EuGH im Bereich des Datenschutzes vor und nachdem die GRC verbindlich wurde Tzanou, 48 ff.

234 von Grafenstein, 175. Art. 8 GRC wurde basierend auf Art. 8 EMRK, der RL 95/46/EG (Datenschutzrichtlinie), sowie dem heutigen Art. 16 AEUV geschaffen. Dies verwundert insofern, als Art. 8 EMRK den Datenschutz nicht ausdrücklich erwähnt, die besagte Richtlinie Sekundärrecht darstellt und Art. 16 AEUV zwar Primärrecht darstellt, aber kein eigentliches Recht auf Datenschutz konstituiert. Mit der GRC wurde also nicht lediglich wiedergegeben, was bereits in anderen Quellen zu finden war. Es wurde vielmehr ein neues Grundrecht geschaffen, dessen Rahmen bereits bekannt war. Siehe dazu Tzanou, 20 f. Siehe zur Entwicklung des Datenschutzes in der EU auch Michl, 349 ff.; Naef, 20 ff.

235 Vgl. dazu auch FRA/Europarat/EDSB, Handbuch, 33 f.

236 Lock, in: Commentary EU treaties and CFR, Art. 8 GRC N 2.

237 Siehe dazu Art. 290 AEUV; Jarass/Kment, § 3 N 9.

Grundrecht zu konkretisieren. Andererseits wird das Sekundärrecht auf die Vereinbarkeit mit dem Grundrecht hin überprüft. Dies führt dazu, dass die Argumente grundrechtlicher Natur sowie diejenigen des Sekundärrechts bei der Auslegung von Richtlinien und Verordnungen häufig nicht voneinander getrennt werden. Eine Abgrenzung zwischen dem Datenschutz auf grundrechtlicher Ebene und dem Datenschutz des Sekundärrechts wird dadurch verunmöglicht. Somit bleibt oftmals unklar, wo der grundrechtliche Mindeststandard ansetzt und wo es (lediglich) um die Auslegung von sekundärrechtlichen Regelungen geht. Die primärrechtskonforme Auslegung verschwimmt so mit der sekundärrechtskonformen. Dies hat auch zur Folge, dass der Gestaltungs- sowie Änderungsspielraum des Sekundärrechts unklar bleibt.[238]

6.2. Adressatenkreis und Grundrechtsträger der GRC

Die GRC ist verbindlich für die Organe, Einrichtungen oder sonstigen Stellen der EU sowie für die Mitgliedstaaten, sofern sie EU-Recht umsetzen.[239] Das Ausmass der Verbindlichkeit von EU-Grundrechten für die Mitgliedstaaten ist ein komplexes und umstrittenes Thema. Die Rechtsprechung des EuGH zeigt, dass der Anwendungsbereich der GRC weit ausgelegt wird und sich nicht auf das Handeln der Mitgliedstaaten nach den Vorgaben des EU-Rechts beschränkt (also z.B. die Umsetzung einer Richtlinie oder die Vollziehung einer Verordnung). Auch durch das EU-Recht gewährte Handlungsspielräume fallen darunter. Dies einerseits bei der Beschränkung von Grundfreiheiten sowie andererseits bei einer durch einen Sekundärrechtsakt gewährten Handlungsmöglichkeit, welche keine Verpflichtung zu einem bestimmten Verhalten vorsieht.[240]

Die Grundrechtsträger werden, anders als der Adressatenkreis, nicht explizit in der GRC geregelt. Es handelt sich dabei primär um alle natürlichen Personen, wobei es unerheblich ist, ob es sich dabei um UnionsbürgerInnen, Drittstaatsangehörige oder Staatenlose handelt. Anders als die natürlichen Personen sind die juristischen Personen nicht generell grundrechtsberechtigt.

---

238 NETTESHEIM, in: Europäischer Grundrechteschutz, § 10 N 58. Siehe zu dieser Thematik auch BERNSDORFF, in: NomosKommentar GRC, Art. 8 GRC N 15 ff.; KONING, 39.

239 Art. 51 Abs. 1 S. 1 GRC. Siehe zum Anwendungsbereich der GRC auch LOCK, in: Commentary EU treaties and CFR, Art. 51 GRC N 1 ff. m.w.H. Eine mögliche Drittwirkung oder Horizontalwirkung ist bis anhin nicht abschliessend geklärt. Siehe allgemein zu den Adressaten JARASS/KMENT, § 4 N 1 ff. m.w.H.

240 Vgl. dazu EPINEY, Verbindlichkeit, 149 ff. m.w.H. (mit Hinweisen auf die Rechtsprechung); EPINEY/PIRKER, 236 ff. m.w.H. Siehe zum Ganzen auch RAIMONDO, 165 ff.

Hinsichtlich einzelner Grundrechte gelten jedoch auch diese als Grundrechtsträger.[241]

6.3. Persönlicher und sachlicher Schutzbereich

Auf Art. 8 GRC können sich unter bestimmten Voraussetzungen neben den natürlichen Personen auch juristische Personen berufen.[242]

Der sachliche Anwendungsbereich von Art. 8 GRC umfasst die Begriffe «*personenbezogene Daten*» und «*Verarbeitung*».[243] Geschützt werden also personenbezogene Daten. Darunter fallen Informationen, welche sich auf eine identifizierte resp. eine identifizierbare natürliche Person beziehen. Eine Person ist identifizierbar, wenn diese direkt oder indirekt – etwa durch die Zuordnung eines Namens zu physischen Merkmalen einer Person – identifiziert werden kann. Unerheblich ist, wie die Daten gespeichert werden resp. ob diese der Allgemeinheit zugänglich sind.[244]

Unter dem Begriff der Verarbeitung werden verschiedenartige Tätigkeiten mit Daten subsumiert, so bspw. das Erfassen, die Speicherung, das Abfragen, die Verwendung, die Verknüpfung, die Weitergabe, etc. Dabei muss die betroffene Person durch die Datenbearbeitung nicht zwingend einen Nachteil erleiden.[245] Der Begriff der Datenbearbeitung wird sehr weit verstanden und umfasst jeglichen Umgang mit personenbezogenen Daten unabhängig davon, ob die Bearbeitung automatisiert vorgenommen wird oder nicht.[246]

6.4. Positive Schutzpflichten

Anders als Art. 8 EMRK und Art. 13 Abs. 2 BV enthält Art. 8 GRC in den Abs. 2 und 3 ausdrücklich bestimmte Gewährleistungen.[247]

---

241 Siehe zu den Grundrechtsträgern ausführlich JARASS/KMENT, § 4 N 28 ff. m.w.H.

242 BREUER, in: EU-Grundrechte-HdB, § 25 N 25; JARASS/KMENT, § 13 N 6; BERNSDORFF, in: NomosKommentar GRC, Art. 8 GRC N 25. Siehe dazu auch EuGH, Urteil v. 09.11.2010, *Volker und Markus Schecke und Eifert*, ECLI:EU:C:2010:662, Rz. 52 f., 87.

243 BERNSDORFF, in: NomosKommentar GRC, Art. 8 GRC N 20.

244 JARASS/KMENT, § 13 N 5. Siehe zur Definition von personenbezogenen Daten auch Art. 4 Ziff. 1 DSGVO.

245 JARASS/KMENT, § 13 N 7. Siehe dazu auch BERNSDORFF, in: NomosKommentar GRC, Art. 8 GRC N 22.

246 LOCK, in: Commentary EU treaties and CFR, Art. 8 GRC N 8.

247 Vgl. zum Verhältnis der drei Absätze von Art. 8 GRC KONING, 39 f.

Art. 8 Abs. 2 GRC gewährleistet zwei Rechte: einerseits das Recht auf Auskunft der eigenen Daten und andererseits das Recht auf Berichtigung von unrichtigen Daten. Der grundrechtliche Anspruch auf Auskunft soll es ermöglichen, Kenntnis über die erhobenen resp. gespeicherten Daten zu erlangen und diese auf deren Richtigkeit überprüfen zu können.[248]

Im Urteil *Google Spain*[249] wurde zudem ein «*Recht auf Vergessenwerden*» anerkannt. *In casu* wurde eine ursprünglich rechtmässige Datenbearbeitung als unzulässig erklärt, weil diese für den anvisierten Zweck nicht mehr erforderlich war.[250] Dem Urteil ist kein absolutes Recht auf Löschung zu entnehmen. Es sollte vielmehr die unrechtmässige Datenbearbeitung verhindert werden.[251]

Des Weiteren wird gemäss Art. 8 Abs. 3 GRC verlangt, dass eine unabhängige Stelle eingerichtet wird, welche die Einhaltung der Vorschriften überwacht. Damit wird wesentlich zum Schutz der personenbezogenen Daten beigetragen.[252]

6.5. Eingriffe in den Schutzbereich

Wenn ein Grundrechtsadressat personenbezogene Daten verarbeitet, ist grundsätzlich von einem Eingriff in Art. 8 GRC auszugehen.[253]

---

248 JARASS/KMENT, § 13 N 14. Diese beiden Rechte werden im Sekundärrecht näher ausgeführt (Art. 15 und 16 DSGVO).

249 EuGH, Urteil v. 13.05.2014, *Google Spain SL v. Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317.

250 EuGH, Urteil v. 13.05.2014, *Google Spain SL v. Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317, Rz. 89 ff. *In casu* ging es jedoch um die Auslegung von der Datenschutzrichtlinie und nicht der GRC. Siehe zu diesem Urteil auch WP29, Google Spain; KRANENBORG.

251 Siehe dazu LOCK, in: Commentary EU treaties and CFR, Art. 8 GRC N 22 f. In Art. 17 DSGVO ist jedoch ausdrücklich ein Recht auf Löschung verankert, wobei in Klammer der Begriff «*Recht auf Vergessenwerden*» aufgeführt ist. Im besagten Urteil ging es aber gar nicht um eine Löschung, sondern um die Unterdrückung einer Verlinkung. Siehe zum Ganzen BREUER, in: EU-Grundrechte-HdB, § 25 N 39 ff. m.w.H.

252 Siehe dazu auch BERNSDORFF, in: NomosKommentar GRC, Art. 8 GRC N 42 m.w.H.; JOHLEN, in: Stern/Sachs-Kommentar-GRC, Art. 8 GRC N 64 m.w.H. Vgl. dazu auch EuGH, Urteil v. 06.10.2015, *Schrems*, ECLI:EU:C:2015:650, Rz. 41. Die Anforderungen an die unabhängigen Aufsichtsbehörden werden zudem in Art. 51 ff. DSGVO näher ausgeführt.

253 Vgl. dazu WOLFFGANG, in: Lenz/Borchardt, EU-Verträge Kommentar, Art. 8 GRC N 4. Es wird jedoch auch die Meinung vertreten, dass Art. 8 GRC in seiner Gesamtheit verstanden werden müsse und demnach eine Datenbearbeitung unter bestimmten Bedingungen erlaubt sei. Somit sei nicht immer zwingend von einem Grundrechtseingriff auszugehen. Siehe dazu TZANOU, 39 f. Vgl. dazu auch NAEF, 47 ff.

Die Erstellung eines Profils einer Person kann einen schweren Eingriff darstellen.[254]

Bei den positiven Schutzpflichten, also insbesondere dem Auskunfts- sowie Berichtigungsanspruch, stellt die Nichterfüllung dieser Pflichten durch die staatlichen Behörden einen Eingriff dar.[255]

6.6. Rechtfertigung von Eingriffen

Grundsätzlich statuiert Art. 52 Abs. 1 GRC eine einheitliche Schrankenregelung für die in der GRC verankerten Grundrechte. Diese wird durch die Abs. 2, 3 und 6 relativiert.[256]

Im Bereich des Schutzes der personenbezogenen Daten ist es umstritten, welche Schrankenklausel anzuwenden ist (Art. 52 Abs. 1 oder Abs. 2 oder gar Abs. 3 GRC).[257]

Gemäss Art. 52 Abs. 1 GRC wird eine Beeinträchtigung eines in der GRC geschützten Rechts oder einer Freiheit grundsätzlich als zulässig bewertet, wenn eine gesetzliche Grundlage die Eingriffsmassnahme vorsieht und der Wesensgehalt des Grundrechts gewahrt wird. Des Weiteren dürfen die einschränkenden Massnahmen nur vorgenommen werden, wenn diese unter Wahrung des Grundsatzes der Verhältnismässigkeit erforderlich sind und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen entsprechen, oder der Schutz der Rechte und Freiheiten von anderen dies erfordert.[258]

Art. 52 Abs. 2 GRC hält hingegen fest, dass die Ausübung der durch die GRC geschützten Rechte, welche in den Verträgen geregelt sind, im Rahmen der Bedingungen und Grenzen, wie diese in den Verträgen festgelegt sind, zu erfolgen hat. Da sich im Bereich des Datenschutzes neben Art. 8 GRC auch in Art. 16 AEUV eine primärrechtliche Grundlage findet, müsste eigentlich – an-

254 Siehe dazu EuGH, Urteil v. 13.05.2014, *Google Spain SL v. Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317, Rz. 80 f. Siehe dazu auch Nettesheim, in: Europäischer Grundrechteschutz, § 10 N 65. Siehe zu weiteren Beispielen für einen schweren Eingriff EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 65; EuGH, Urteil v. 21.06.2022, *Ligue des droits humains*, ECLI:EU:C:2022:491, Rz. 111.

255 Breuer, in: EU-Grundrechte-HdB, § 25 N 47.

256 Es gibt auch Grundrechte, welche nicht eingeschränkt werden können, so z.B. die Menschenwürde oder das Folterverbot. Siehe dazu Jarass/Kment, § 6 N 21.

257 Bernsdorff, in: NomosKommentar GRC, Art. 8 GRC N 24 mit Hinweisen zu weiterführender Literatur.

258 Siehe dazu Jarass/Kment, § 6 N 19 ff. mit weiteren Hinweisen zu diesen Kriterien.

stelle der allgemeinen Grundrechtsschranke gemäss Abs. 1 – die besondere Grundrechtsschranke gemäss Abs. 2 zur Anwendung gelangen.[259]

Gemäss Art. 52 Abs. 3 GRC haben die in der GRC geschützten Rechte, welche den ebenfalls in der EMRK geschützten Rechten entsprechen, die gleiche Bedeutung und Tragweite, wie gemäss der EMRK, wobei die GRC einen weiter gehenden Schutz gewähren kann. Diesbezüglich ist festzustellen, dass das unionsrechtliche Pendant zu Art. 8 EMRK nicht Art. 8 GRC, sondern Art. 7 GRC (also das Recht auf Achtung des Privat- und Familienlebens) darstellt. Art. 8 GRC stützt sich lediglich auf Art. 8 EMRK ab.[260]

Die herrschende Lehre geht davon aus, dass die allgemeine Grundrechtsschranke gemäss Art. 52 Abs. 1 GRC einschlägig ist, wobei auch die Vorgaben von Art. 8 Abs. 2 S. 1 GRC zu berücksichtigen sind (Verarbeitung von Daten «*nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage*»). Diese Ansicht teilt auch der EuGH.[261] Gemäss Art. 52 Abs. 3 S. 1 GRC sind zudem die Vorgaben von Art. 8 Abs. 2 EMRK zu beachten. Dies mag insofern erstaunen, als es zu Art. 8 GRC kein entsprechendes Pendant in der EMRK gibt. Dennoch erscheint die Beachtung von Art. 8 Abs. 2 EMRK insofern nachvollziehbar, als datenschutzrechtliche Sachverhalte im Rahmen von Art. 8 EMRK abgehandelt werden.[262] Diese Auffassung findet sich auch in der Rechtsprechung des EuGH.[263]

---

259 Dabei soll unerheblich sein, dass Art. 16 AEUV – anders als Art. 8 GRC – keine Schrankenbestimmung enthält. Das Grundrecht sei nicht schrankenlos zu gewähren, sondern es seien vielmehr die im Sekundärrecht festgelegten Datenverarbeitungsanforderungen heranzuziehen. Siehe dazu BERNSDORFF, in: NomosKommentar GRC, Art. 8 GRC N 24. Siehe dazu jedoch auch LOCK, in: Commentary EU treaties and CFR, Art. 8 GRC N 2. Dort wird die Ansicht vertreten, dass Art. 52 Abs. 2 GRC gerade nicht einschlägig sei.

260 Siehe dazu EDPS, necessity, 6; VON GRAFENSTEIN, 176 ff. m.w.H.

261 JOHLEN, in: Stern/Sachs-Kommentar-GRC, Art. 8 GRC N 40 ff. Siehe dazu auch EuGH, Urteil v. 17.10.2013, *Schwarz*, ECLI:EU:C:2013:670, Rz. 31 ff.

262 JOHLEN, in: Stern/Sachs-Kommentar-GRC, Art. 8 GRC N 43. Siehe dazu auch EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 129, wonach der EuGH festgehalten hat, dass es sich bei Art. 8 GRC um ein anderes Grundrecht als in Art. 7 GRC handelt, wofür es in der EMRK kein entsprechendes Pendant gibt. Das Verhältnis zwischen Art. 52 Abs. 1 und 3 GRC ist im Allgemeinen nicht klar. So stellt sich u.a. die Frage, ob das Kriterium des Kerngehalts auch anwendbar ist, wenn ein in der GRC geschütztes Recht auch von der EMRK geschützt wird. Siehe dazu BRKAN, prism of data privacy, 28 f. m.w.H. Vgl. dazu auch COLELLA, restriction, 199 f.

263 So z.B. in EuGH, Urteil v. 09.11.2010, *Volker und Markus Schecke und Eifert*, ECLI:EU:C:2010:662, Rz. 48 ff.

Da die Kriterien gemäss Art. 8 Abs. 2 EMRK bereits oben erläutert wurden, werden im Folgenden die Kriterien gemäss Art. 52 Abs. 1 GRC näher vorgestellt.[264] Zudem wird auch auf die zusätzlichen Kriterien in Art. 8 Abs. 1 S. 1 GRC eingegangen.

6.6.1. Gesetzliche Grundlage

Die gesetzliche Grundlage kann sich im Unionsrecht finden, wobei grundsätzlich alle verbindlichen Rechtsakte nach Art. 288 AEUV in Frage kommen. Auch nationale Rechtsvorschriften sind als gesetzliche Grundlage möglich, sofern EU-Grundrechte Mitgliedstaaten verpflichten.[265]

Die gesetzliche Grundlage muss im Allgemeinen genügend bestimmt sein, so dass der Betroffene – im Sinne der Vorhersehbarkeit – die Folgen seines Verhaltens abzuschätzen vermag.[266] Zudem muss die gesetzliche Grundlage auch hinreichend zugänglich sein.[267]

Im Bereich des Datenschutzes verlangt der EuGH – wie auch der EGMR und das BGer – hinsichtlich der fraglichen Massnahmen klare und präzise Regeln, mit welchen die Tragweite sowie die Anwendung der Massnahme festgelegt werden.[268] Es sind Mindestanforderungen festzulegen, damit ausreichende Garantien gegen Missbrauch zur Verfügung stehen.[269] Anders als (teilweise) der EGMR beurteilt der EuGH diese Kriterien nicht im Rahmen der Prüfung der gesetzlichen Grundlage, sondern bei der Prüfung der Verhältnismässigkeit.[270]

6.6.2. Wesensgehalt

Die Wesensgehaltsgarantie umfasst den festen Kernbereich eines Grundrechts. Diese wesentlichen Eigenheiten der Grundrechte dürfen nicht angetastet werden.[271]

---

264 In der Lehre werden dazu verschiedene Prüfschemata aufgeführt. Diese unterscheiden sich in der Reihenfolge der Kriterien resp. der Bezeichnung derselben. Vorliegend wird dem vom EDSB verwendeten Prüfschema gefolgt. Siehe dazu EDPS, proportionality, 6 f.

265 JARASS/KMENT, § 6 N 27 ff.

266 JARASS/KMENT, § 6 N 30.

267 LOCK, in: Commentary EU treaties and CFR, Art. 52 GRC N 6.

268 JARASS/KMENT, § 13 N 10.

269 BREUER, in: EU-Grundrechte-HdB, § 25 N 51.

270 Siehe dazu BREUER, in: EU-Grundrechte-HdB, § 25 N 51. Siehe dazu z.B. EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 54 ff.

271 Vgl. dazu JARASS/KMENT, § 6 N 44. Siehe eingehend zur Entwicklung resp. Bedeutung des Wesensgehalts in der GRC sowie auch zur Abgrenzung zur Verhältnismässigkeit BRKAN,

Der Wesensgehalt von Art. 8 GRC wurde bis anhin (noch) nicht genau definiert.[272] In der Rechtsprechung des EuGH finden sich jedoch einige Hinweise dazu.

Im Urteil *Digital Rights*[273] hat sich der EuGH erstmals zum Wesensgehalt von Art. 8 GRC geäussert. In diesem Urteil beurteilte der EuGH die Gültigkeit der RL 2006/24/EG, welche die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste bzw. öffentlicher Kommunikationsnetze dazu verpflichtete, bestimmte Arten von Daten, die sog. Verkehrs- und Standortdaten, auf Vorrat zu speichern, um sie den nationalen Behörden zwecks Bekämpfung von schweren Straftaten zur Verfügung stellen zu können. Im Zusammenhang mit dem Wesensgehalt von Art. 8 GRC führte das Gericht aus, dass dieser *in casu* nicht angetastet werde, da die in Frage stehende EU-Richtlinie eine Bestimmung zum Datenschutz und zur Datensicherheit enthalte. Gemäss dieser hätten die Anbieter der öffentlich zugänglichen elektronischen Kommunikationsdienste resp. Betreiber eines öffentlichen Kommunikationsnetzes bestimmte Grundsätze des Datenschutzes resp. der Datensicherheit einzuhalten. Mit diesen Grundsätzen hätten die Mitgliedstaaten sicherzustellen, dass geeignete technische und organisatorische Massnahmen getroffen werden, «*um die Daten gegen zufällige oder unrechtmässige Zerstörung sowie zufälligen Verlust oder zufällige Änderung zu schützen*».[274] Im Ergebnis müssen diese Ausführungen so verstanden werden, dass der Kern von Art. 8 GRC darin besteht, dass minimale Sicherheitsmassnahmen gegen Missbrauch vorhanden sind. Die Anforderung an den Wesensgehalt wird somit sehr tief angesetzt. Dies ist kritisch zu betrachten. Denn dies führt dazu, dass der Wesensgehalt nie verletzt ist, wenn ein Minimum an Sicherheitsmassnahmen vorhanden ist. Ausserdem stellt sich die Frage, in welchen Fällen eine Datenbearbeitung nicht verhältnismässig ist und wann eine Verletzung des Wesensgehalts vorliegt.[275] Im gleichen Urteil wurde zudem festgehalten, dass auch der Wesensgehalt von

prism of data privacy. Vgl. zur Abgrenzung des Kerngehalts und der Verhältnismässigkeit auch BRKAN, essence, 867 ff. Siehe zum Verständnis des Wesensgehalts in den Mitgliedstaaten BRKAN, essence, 865 ff.

272 Zum Kerngehalt eines Grundrechts wird auch die Ansicht vertreten, dass es beinahe unmöglich sei, diesen abstrakt festzulegen. Der Kerngehalt müsse jeweils unter Berücksichtigung der Umstände im Einzelfall in konkreten Fall bestimmt werden. Zudem sei es möglich, dass ein Grundrecht mehrere Kerngehalte habe. Siehe dazu BRKAN, prism of data privacy, 29.

273 EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238.

274 Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 40. Siehe dazu auch BRKAN, essence, 871 ff.

275 Siehe dazu BRKAN, essence, 878 f.

Art. 7 GRC, dem Recht auf Achtung des Privat- und Familienlebens, nicht angetastet werde, da mit der in Frage stehenden Vorratsdatenspeicherung nicht die Kenntnisnahme des Inhalts der elektronischen Kommunikation gestattet werde.[276] Diesem Urteil ist zu entnehmen, dass im Zusammenhang mit einer Datenbearbeitung neben Art. 8 GRC auch Art. 7 GRC eine Rolle spielen kann. Auf das Verhältnis dieser beiden Bestimmungen wird nachfolgend noch genauer eingegangen.[277]

In *Tele2*[278] befasste sich der EuGH erneut mit der Vorratsdatenspeicherung und bezog abermals Stellung zum Wesensgehalt von Art. 7 GRC sowie von Art. 8 GRC. Das Gericht stellte fest, dass aus den gespeicherten Daten geschlossen werden könne, wer mit welcher Person wie lange und von welchem Ort aus über welchen Kanal kommuniziert habe. Davon abgesehen gehe aus den Daten auch hervor, wie regelmässig eine Person mit einer anderen während eines bestimmten Zeitraums in Kontakt gestanden habe. Das Zusammenfügen der Daten einer Person, welche von der Vorratsdatenspeicherung betroffen sei, ermögliche sehr genaue Rückschlüsse auf das Privatleben dieser Person, da diese u.a. Gewohnheiten des täglichen Lebens, das Bewegungsprofil sowie Hinweise zum sozialen Umfeld der Person offenbarten. Diese Angaben ermöglichten die Erstellung eines Profils, welches unter Berücksichtigung von Art. 7 GRC «*eine genauso sensible Information darstellt wie der Inhalt der Kommunikation selbst*». Dennoch stellte das Gericht im Anschluss fest, dass der Wesensgehalt von Art. 7 *und* 8 GRC nicht angetastet werde, da die Vorratsdatenspeicherung nicht den Inhalt der Kommunikation betreffe.[279] Damit dehnte der EuGH seine in *Digital Rights* vertretene Ansicht zu Art. 7 GRC, wonach keine Verletzung des Wesensgehalts vorliege, weil die Vorratsdatenspeicherung nicht den Inhalt der Kommunikation betreffe, ausdrücklich auch auf Art. 8 GRC aus.[280] Der EuGH löst sich damit also von seiner im Urteil *Digital Rights* vertretenen Ansicht zum Kerngehalt von Art. 8 GRC und zeigt auf, dass

276 EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 39. Siehe dazu kritisch Brkan, essence, 871 ff. In einem anderen Urteil wurde von einem Eingriff in den Kerngehalt von Art. 7 GRC ausgegangen, da die fragliche Gesetzgebung den Behörden erlaubte, im grossen Stil auf den Inhalt der Kommunikation zuzugreifen. Siehe dazu EuGH, Urteil v. 06.10.2015, *Schrems*, ECLI:EU:C:2015:650, Rz. 94. Siehe zu diesem Urteil auch (teilweise kritisch) Epiney, Überwachung, 1509; Brkan, prism of data privacy, 16 ff.; Brkan, essence, 874 ff.

277 Siehe dazu Kapitel II.6.7.

278 EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970.

279 EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 98 ff.

280 Siehe dazu EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 101.

eine Massnahme gleichzeitig in zwei Grundrechte eingreifen kann.[281] Die Ausführungen in *Tele2* machen deutlich, dass es dem EuGH nicht leicht fällt, die Grundrechte gemäss Art. 7 und 8 GRC auseinanderzuhalten.[282]

Auch dem *Gutachten 1/15*[283] des EuGH sind Hinweise zum Wesensgehalt von Art. 8 GRC zu entnehmen, wobei eine Verletzung desselben letztlich verneint wurde. In diesem vom Europäischen Parlament beantragten Gutachten beurteilte der EuGH das geplante Abkommen zwischen Kanada und der EU, in welchem die Übermittlung und Verarbeitung von Fluggastdatensätzen (sog. PNR-Daten) geregelt war.[284] Der EuGH legte in diesem Gutachten dar, dass auch wenn PNR-Daten sehr spezifische Informationen bezüglich des Privatlebens einer Person betreffen, diese auf bestimmte Aspekte des Privatlebens, nämlich Flugreisen zwischen Kanada und EU, beschränkt seien. Im Abkommen werde die Nutzung der Daten – auf bestimmte Zwecke – beschränkt und es würden Regeln vorgesehen, um die Sicherheit, die Vertraulichkeit sowie die Integrität der Daten zu gewährleisten und diese Daten vor unrechtmässiger Bearbeitung zu schützen.[285] Der Aspekt zu den Regeln, welche die Sicherheit, die Vertraulichkeit sowie die Integrität der Daten gewährleisten sollen, zielt in eine ähnliche Richtung wie die Ausführungen im Urteil *Digital Rights* zum Kerngehalt von Art. 8 GRC. Davon abgesehen nimmt der EuGH noch einen anderen Aspekt auf, nämlich die Zweckbestimmung. Dieses Erfordernis geht explizit aus Art. 8 Abs. 2 GRC hervor. Der EuGH nimmt darauf jedoch nicht Bezug. Dies könnte zur Annahme verleiten, dass der Wesensgehalt automatisch betroffen ist, sobald ein in Art. 8 GRC aufgeführtes Element verletzt ist. Dies hätte jedoch zur Folge, dass ein Eingriff in Art. 8 GRC relativ häufig eine Verletzung des Kerngehalts darstellen dürfte. Dies wäre wohl nicht mit Art. 52 Abs. 1 GRC vereinbar.[286]

Abgesehen von der Rechtsprechung finden sich auch in der Lehre Ausführungen zum Wesensgehalt von Art. 8 GRC. So wird z.B. die Ansicht vertreten, dass die in Art. 8 GRC enthaltenen datenschutzrechtlichen Prinzipien den Ausgangspunkt für die Bestimmung des Wesensgehalts darstellen sollten.[287] Da-

281 Siehe dazu BRKAN, essence, 879. Die Autorin vertritt darin zudem die Meinung, dass die Unterscheidung zwischen dem Inhalt und den Randdaten der Kommunikation weder für die Bestimmung des Kerngehalts der Privatsphäre noch des Datenschutzes ein geeignetes Kriterium darstellt.

282 BRKAN, essence, 878.

283 EUGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592.

284 Siehe zu den Hintergründen von diesem Abkommen EUGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 14 ff.

285 EUGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 150.

286 Siehe dazu BRKAN, essence, 879 ff.

287 Siehe dazu TZANOU, 42 ff. m.w.H.

von abgesehen wird auch die Meinung vertreten, dass das im Sekundärrecht verankerte Prinzip der Zweckbestimmung zum Wesensgehalt von Art. 8 GRC gehört.[288]

Insgesamt ergibt sich weder aus der Rechtsprechung des EuGH noch aus der Lehre eindeutig, worin der Wesensgehalt von Art. 8 GRC besteht. Es scheint, als ob der Wesensgehalt von Art. 8 GRC anhand von grundlegenden Prinzipien definiert wird, welche beachtet werden müssen, um den Wesensgehalt zu respektieren. Der Wesensgehalt umfasst ein Minimum an Garantien, welche eingesetzt werden müssen, um die personenbezogenen Daten effektiv zu schützen. Gemäss der Rechtsprechung des EuGH umfassen diese Garantien zumindest die Wahrung der Integrität und der Vertraulichkeit der personenbezogenen Daten sowie die Festlegung des Zwecks der Datenbearbeitung.[289]

6.6.3. Zulässiger Beeinträchtigungsgrund

Als zulässige Beeinträchtigungsgründe gelten die «*von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen*» sowie der «*Schutz der Rechte und Freiheiten anderer*».[290] Bei den dem Gemeinwohl dienenden Zielsetzungen handelt es sich um die in Art. 3 EUV aufgeführten allgemeinen Ziele der EU, wie z.B. die Förderung des Friedens oder die soziale Gerechtigkeit.[291] Steht der Schutz personenbezogener Daten einem anderen Recht oder einer anderen Freiheit entgegen, so hat das Gericht eine Interessenabwägung vorzunehmen.[292]

Wie auch der EGMR befasst sich auch der EuGH häufig nicht ausführlich mit dem Begriff der legitimen Ziele. Insbesondere dann nicht, wenn eine Massnahme als erforderlich zur Erreichung eines solchen Ziels angesehen wird.[293]

Die Festlegung der im Einzelfall einschlägigen, dem Gemeinwohl dienenden Zielsetzung ist jedoch wichtig, da die Notwendigkeit der Einschränkung danach beurteilt wird. Nur so kann bestimmt werden, ob die in das Grundrecht eingreifende Massnahme erforderlich ist. Die Zielsetzung, die Notwendigkeit

---

288 Dem Prinzip der Zweckbestimmung, welches u.a. Art. 5 Abs. 1 Bst. b DSGVO zu entnehmen ist, werden zwei verschiedene Gehalte zugewiesen («*purpose specification requirement*» und «*non-incompatibility requirement*»). Es besteht Uneinigkeit darüber, ob beide Aspekte zum Kerngehalt gehören. Siehe dazu KONING, 124 ff. m.w.H.

289 Vgl. dazu KONING, 124 ff.

290 Art. 52 Abs. 1 S. 2 GRC.

291 FRA/EUROPARAT/EDSB, Handbuch, 57. Siehe dazu auch NAEF, 53 m.w.H.

292 Siehe dazu FRA/EUROPARAT/EDSB, Handbuch, 62 ff.

293 KONING, 160 ff. Siehe zum EGMR Kapitel II.4.6.2.

und die Verhältnismässigkeit der Einschränkung sind demnach eng miteinander verbunden.[294] Im Bereich des Datenschutzes kann der für die Datenbearbeitung festgelegte Zweck Hinweise liefern, worin das legitime Ziel einer Massnahme besteht.[295]

6.6.4. Verhältnismässigkeit

Nach ständiger Rechtsprechung verlangt der EuGH bezüglich der Verhältnismässigkeit, «*dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist*».[296]

Im Rahmen der Geeignetheit wird geprüft, ob die in Frage stehende Massnahme geeignet ist, das anvisierte Ziel tatsächlich zu erreichen.[297] Die Förderung der Erreichung eines Ziels wird dabei bereits als ausreichend betrachtet. Ferner ist es bei mehreren Zielen auch ausreichend, wenn die Geeignetheit der Massnahme mindestens zur Förderung eines Ziels bejaht werden kann.[298] Die Rechtsprechung des EuGH zeigt, dass an die Geeignetheit einer Massnahme oftmals keine allzu hohen Anforderungen gestellt werden.[299]

Bei der Erforderlichkeit geht es um eine faktenbasierte Bewertung der Geeignetheit einer Massnahme hinsichtlich der verfolgten Ziele und der Frage, ob im Einzelfall weniger einschneidende Massnahmen zur Verfügung stehen.[300]

---

294 FRA/Europarat/EDSB, Handbuch, 58.

295 Koning, 118.

296 EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 46 mit Hinweisen auf weitere Urteile.

297 Vgl. dazu Art. 52 Abs. 1 S. 2 GRC.

298 Jarass/Kment, § 6 N 35.

299 So wurde bspw. im Urteil *Digital Rights* die Geeignetheit der Vorratsspeicherung bejaht, da diese den nationalen Behörden zusätzliche Möglichkeiten biete und somit ein nützliches Mittel für strafrechtliche Ermittlungen darstelle. Auch dass es andere elektronische Kommunikationsweisen gebe, welche nicht von der RL 2006/24/EG erfasst seien oder die anonyme Kommunikation ermöglichten, vermöge daran nichts zu ändern. Die Eignung werde dadurch lediglich eingeschränkt, begründe jedoch nicht die gänzliche Ungeeignetheit der Massnahme. Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 49 f. Ebenfalls wurde die Geeignetheit in *Schwarz vs. Bochum* bejaht. Dem Einwand des Beschwerdeführers, wonach eine Fehlerquote vorhanden sei, hielt das Gericht entgegen, dass die Massnahme nicht völlig zuverlässig sein müsse. Eine erhebliche Verminderung der Akzeptanz von unbefugten Personen reiche aus. Siehe dazu EuGH, Urteil v. 17.10.2013, *Schwarz*, ECLI:EU:C:2013:670, Rz. 41 ff.

300 EDPS, proportionality, 10 f.

Massnahmen dürfen nur so weit greifen, wie sie für die Zielerreichung oder -förderung notwendig sind. Es darf also kein – in sachlicher und zeitlicher Hinsicht – milderes Mittel zur Verfügung stehen.[301] Das Problem, welches mit der Massnahme behoben werden soll, muss umschrieben werden. Ausserdem muss dargelegt werden, wie das Problem mit der Massnahme angegangen werden kann und warum bereits bestehende oder weniger einschneidende Massnahmen ungenügend sind.[302]

Bei der Prüfung der von der Rechtsprechung geforderten Kriterien ist zu berücksichtigen, dass der Gestaltungsspielraum des Unionsgesetzgebers aufgrund von verschiedenen Kriterien eingeschränkt sein kann. Dazu zählen u.a. der betroffene Bereich, die Natur des betroffenen Rechts, die Art und Schwere des Eingriffs sowie dessen Zweck.[303]

Bei der Beurteilung der Verhältnismässigkeit im Bereich des Datenschutzes prüft der EuGH, ob die in Frage stehende Regelung klare und präzise Regeln hinsichtlich der Tragweite und der Anwendung der fraglichen Massnahme vorsieht sowie, ob Mindestgarantien festgelegt wurden, die den von der Datenbearbeitung betroffenen Personen eine ausreichende Garantie für einen wirksamen Missbrauchsschutz dieser personenbezogenen Daten gewährleisten.[304] Aus der Regelung hat insbesondere hervorzugehen, unter welchen Umständen sowie welchen Voraussetzungen eine Massnahme, welche eine Bearbeitung von personenbezogenen Daten vorsieht, vorgenommen werden darf, so dass der Eingriff auf das absolut Notwendige beschränkt wird. Diese Garantien sind umso wichtiger, wenn eine automatisierte Bearbeitung von personenbezogenen Daten vorgenommen wird, vor allem wenn eine grosse Gefahr eines missbräuchlichen Zugangs zu diesen besteht.[305] Solche Garantien können z.B. in der Stärkung der Aufsichtsbehörden oder der Rechte der betroffenen Personen bestehen. Ebenfalls können Sanktionen bei der missbräuchlichen Verarbeitung von Daten vorgesehen werden.[306] Überdies hat auch das Kriterium der Schwere eines Eingriffs Auswirkungen auf die Anforderungen an

301 Diese Beurteilung hängt oftmals stark von den Umständen des Einzelfalles ab. Siehe dazu JARASS/KMENT, § 6 N 38.

302 EDPS, necessity, 8.

303 EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 47.

304 Siehe dazu Kapitel II.6.6.1.

305 EuGH, Urteil v. 05.04.2022, *Commissioner of An Garda Síochána*, ECLI:EU:C:2022:258, Rz. 54 (mit Hinweisen zu weiteren Urteilen). Vgl. dazu auch EPINEY, Überwachung, 1511; EDPS, proportionality, 10 f.

306 BROUWER, purpose limitation, 294.

die Garantien. Je schwerer der Eingriff, desto höhere Anforderungen sind an die Garantien zu stellen.[307]

6.6.5. Zusätzliche Anforderungen gemäss Art. 8 Abs. 2 S. 1 GRC

Wie bereits oben erläutert, sind abgesehen von den Rechtfertigungskriterien gemäss Art. 51 Abs. 1 GRC auch die zusätzlichen Anforderungen von Art. 8 Abs. 2 S. 1 GRC zu prüfen.[308] Dabei handelt es sich um die folgenden drei Kriterien.

Erstens verlangt der Wortlaut von Art. 8 Abs. 2 S. 1 GRC, dass Daten nur nach Treu und Glauben verarbeitet werden dürfen. Diesbezüglich wird argumentiert, dass dieses Kriterium dem Einsatz von verborgenen Geräten entgegenstehe.[309] Ausserdem wird die Ansicht vertreten, dass es bei rechtswidrigen Zwecken an diesem Erfordernis fehle.[310] Davon abgesehen findet sich in der Lehre auch der Hinweis, dass mit diesem Grundsatz Transparenz gewährleistet werden soll. Daraus fliesse die Verpflichtung des für die Datenbearbeitung Verantwortlichen, die Betroffenen über die Bearbeitung ihrer Daten zu informieren. Auch sei damit eine Auffangfunktion für Fälle verbunden, welche zwar grundsätzlich den Datenschutzvorgaben entsprechen, aber den vernünftigen Erwartungen der betroffenen Person entgegenlaufen.[311]

Zweitens wurde das Erfordernis einer gesetzlichen Grundlage ebenfalls explizit in Art. 8 Abs. 2 S. 1 GRC verankert. Daraus ergeben sich jedoch keine über die vorstehenden Ausführungen hinausgehenden Verpflichtungen.[312]

Drittens ist ausdrücklich festgehalten, dass die Datenbearbeitung nur für festgelegte Zwecke erfolgen darf. Die Festlegung des Zwecks verbietet eine ziellose Datenerhebung.[313] Der Zweck einer Datenbearbeitung ist im Vorhinein festzulegen und verpflichtet den für die Datenbearbeitung Verantwortlichen, die Daten nicht in einer Weise weiterzuverarbeiten, welche diesem Zweck zuwiderläuft.[314] Eine Datenbearbeitung, welche nicht mit dem ursprünglich festgelegten Zweck vereinbar ist, stellt einen Eingriff in den Datenschutz dar.[315]

---

307 Lock, in: Commentary EU treaties and CFR, Art. 8 GRC N 11.
308 Siehe dazu Kapitel II.6.6.
309 Jarass/Kment, § 13 N 12. Vgl. dazu auch Naef, 39 f.
310 Jarass, Art. 8 GRC N 11 m.w.H.
311 Marsch, in: Ehlers-Kommentar-EuGR, § 4.2.2 N 26.
312 Siehe zum Ganzen Colella, restriction, 233 f. m.w.H.
313 Naef, 40.
314 Marsch, in: Ehlers-Kommentar-EuGR, § 4.2.2 N 25.
315 Naef, 40.

Die Festlegung des Zwecks misst sich am Grundsatz der Verhältnismässigkeit.[316] Zu den Kriterien, welche bei der Festlegung des Zwecks zu berücksichtigen sind, äussert sich der EuGH nicht.[317] Die Anforderungen an den Zweck sind deshalb sehr vage.[318] Der Zweck ist im Rahmen der gesamten Prüfung der Rechtfertigung eines Eingriffs von Bedeutung, insbesondere auch hinsichtlich der Beurteilung der Sicherheitsmassnahmen.[319] Diese Sicherheitsmassnahmen, welche einen unrechtmässigen Zugang zu den Daten verhindern sollen, tragen dazu bei, dass dem Prinzip der Zweckbindung entsprochen wird. Die Erstellung von Protokollen betreffend die Datenbearbeitung oder die räumliche sowie elektronische Zugangskontrolle können beispielswiese effektive Sicherheitsmassnahmen darstellen.[320]

6.7. Abgrenzung zu anderen Grundrechten

Art. 8 GRC hat einen engen Bezug zu dem in Art. 7 GRC verankerten Recht auf Achtung des Privat- und Familienlebens.[321] Das Verhältnis zwischen diesen beiden Grundrechten ist jedoch unklar. So wird einerseits in der Lehre die Meinung vertreten, dass Art. 8 GRC als *lex specialis* zu betrachten sei.[322] Andere Lehrmeinungen gehen hingegen von Idealkonkurrenz aus. Dass der EuGH in seiner Rechtsprechung die beiden Bestimmungen häufig gemeinsam anwendet, ist als Indiz für Idealkonkurrenz zu deuten.[323] Das Verhältnis

316 Breuer, in: EU-Grundrechte-HdB, § 25 N 35.

317 von Grafenstein, 232 ff.

318 von Grafenstein, 354.

319 Koning, 130.

320 FRA, biometrics, 72. Siehe zum sog. Grundsatz der Zweckbindung Art. 5 Abs. 1 Bst. b DSGVO. Demnach dürfen die Daten nur für «*festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden*».

321 Siehe dazu Bernsdorff, in: NomosKommentar GRC, Art. 8 GRC N 13 m.w.H. Siehe dazu auch EuGH, Urteil v. 24.11.2011, *ASNEF*, ECLI:EU:C:2011:777, Rz. 41; EuGH, Urteil v. 09.11.2010, *Volker und Markus Schecke und Eifert*, ECLI:EU:C:2010:662, Rz. 47.

322 Siehe dazu Michl, 351 f. mit Hinweisen auf die einschlägige Literatur. Siehe dazu auch Lock, in: Commentary EU treaties and CFR, Art. 8 GRC N 3; Bernsdorff, in: NomosKommentar GRC, Art. 8 GRC N 13; Johlen, in: Stern/Sachs-Kommentar-GRC, Art. 8 GRC N 24.

323 Im Urteil *Digital Rights* scheint es, als ob sich der EuGH auf Art. 7 GRC stützt, wenn es um die direkten Auswirkungen der Datenbearbeitung auf das Privatleben der betroffenen Person geht. Hingegen wird bei der Prüfung der Sicherheitsmassnahmen auf Art. 8 GRC verwiesen. Siehe dazu von Grafenstein, 201 ff. Siehe aus der Rechtsprechung zudem u.a. EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 29; EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 100; EuGH, Urteil v. 05.04.2022, *Commissioner of An Garda Síochána*, ECLI:EU:C:2022:258, Rz. 43; EuGH, Urteil v. 21.06.2022, *Ligue des droits humains*, ECLI:EU:C:2022:491, Rz. 94 f.

zwischen Art. 7 und 8 GRC wird in der Rechtsprechung jedoch nicht näher diskutiert.[324]

Teilweise vermischt der EuGH diese beiden Grundrechte, indem er ausführt, dass davon auszugehen sei, «*dass sich die in den Art. 7 und 8 der Charta anerkannte Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft*».[325] In einem anderen Urteil hielt das Gericht jedoch fest, dass es sich um zwei verschiedene Grundrechte handle.[326]

Grundsätzlich ist festzustellen, dass die beiden Rechte einen unterschiedlichen Anwendungsbereich haben. Das Recht auf Schutz personenbezogener Daten gemäss Art. 8 GRC ist immer dann anwendbar, wenn personenbezogene Daten bearbeitet werden. Solche Informationen fallen nicht immer in den Anwendungsbereich des Rechts auf Achtung des Privatlebens im Sinne von Art. 7 GRC. Der Schutz personenbezogener Daten ist folglich umfassender als das Recht auf Achtung des Privatlebens. Jedoch kann eine Verarbeitung personenbezogener Daten auch mit einer Verletzung des Rechts auf Privatleben einhergehen. Eine Verletzung des Rechts auf Privatleben muss nicht belegt werden, damit die Datenschutzvorschriften anwendbar sind. Das Recht auf Privatsphäre ist immer dann betroffen, wenn das Privatleben einer Person beeinträchtigt wird.[327] Die beiden Schutzbereiche überlappen sich also teilweise. So ist bei Art. 8 GRC nicht zwingend ein Bezug zur Privatsphäre erforderlich, bei Art. 7 GRC hingegen schon. Diese Bestimmung schützt die Privatsphäre hingegen viel umfassender als Art. 8 GRC, da sie nicht auf informationelle Aspekte beschränkt ist. Ausserdem wird mit Art. 8 GRC die Errichtung eines Schutzregimes anvisiert. Dieses Verständnis der Schutzbereiche von Art. 7 und 8 GRC lässt ebenfalls auf Idealkonkurrenz schliessen.[328] Sofern also personenbezogene Daten betroffen sind, welche einen Bezug zum Privatleben haben, sind beide Grundrechte kumulativ anwendbar. Fehlt ein Bezug zum Privatleben ist lediglich Art. 8 GRC einschlägig.[329]

---

324 Siehe zum Ganzen NETTESHEIM, in: Europäischer Grundrechteschutz, § 10 N 52. Zum Teil werden für die in der Rechtsprechung vorgenommene Abgrenzung von Art. 7 und 8 GRC verschiedene Kategorien unterschieden. Siehe dazu BRKAN, Judge-made law, 13 ff. m.w.H.

325 EuGH, Urteil v. 09.11.2010, *Volker und Markus Schecke und Eifert*, ECLI:EU:C:2010:662, Rz. 52. Dies wird später auch aufgenommen in EuGH, Urteil v. 24.11.2011, *ASNEF*, ECLI:EU:C:2011:777, Rz. 42.

326 Siehe dazu EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 129.

327 Vgl. dazu FRA/EUROPARAT/EDSB, Handbuch, 23 f. Siehe dazu auch KOKOTT/SOBOTTA, 225 f.

328 NETTESHEIM, in: Europäischer Grundrechteschutz, § 10 N 53. Vgl. zum Verhältnis zwischen Art. 7 und 8 GRC auch VAVOULA, Immigration and Privacy, 37 ff.

329 JARASS/KMENT, § 13 N 3.

Abgesehen davon steht Art. 8 GRC in einem Spannungsverhältnis zum Recht auf Zugang zu Dokumenten gemäss Art. 42 GRC. Bei diesen beiden Grundrechten handelt es sich um konkurrierende Rechte. Beide sind in der zivilen, demokratischen Informationsgesellschaft notwendige Grundbedingungen.[330] Ebenso besteht ein solches Spannungsverhältnis zwischen Art. 8 GRC und dem Recht der Freiheit der Meinungsäusserung sowie zum Recht Informationen zu empfangen gemäss Art. 11 GRC.[331] Werden die von Art. 8 GRC garantierten Ansprüche den betroffenen Personen nicht zugestanden, so ist zugleich auch das Grundrecht auf wirksamen gerichtlichen Rechtsschutz gemäss Art. 47 GRC betroffen.[332]

7. Gemeinsamkeiten und Unterschiede der Grundrechte

In den folgenden Ausführungen werden die Gemeinsamkeiten und Unterschiede der oben dargestellten Grundrechte herausgearbeitet.

Vorweg ist festzuhalten, dass der Gehalt der EMRK den Mindestschutz darstellt, welcher sowohl für die Schweiz als auch die Mitgliedstaaten verbindlich ist. Die BV als auch die GRC können einen weitergehenden Schutz gewährleisten. Der Rechtsprechung des BGer sowie des EuGH ist zu entnehmen, dass im Bereich des Datenschutzes vielfach auf die Rechtsprechung der Strassburger Organe verwiesen wird. Dementsprechend weist der datenschutzrechtliche Gehalt dieser drei Grundrechtsinstrumente viele Gemeinsamkeiten auf.[333]

330 Siehe dazu BERNSDORFF, in: NomosKommentar GRC, Art. 8 GRC N 13. Dort wird zudem auch aufgeführt, dass bei berufsbezogenen Daten sowie Geschäftsinformationen die Art. 15-17 GRC betroffen sein können.

331 LOCK, in: Commentary EU treaties and CFR, Art. 8 GRC N 3. In *Digital Rights* wurde Art. 11 GRC zwar vorgebracht, aber letztlich nicht geprüft. Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 70. Siehe zu Art. 11 GRC LOCK, in: Commentary EU treaties and CFR, Art. 11 GRC N 2 ff.

332 BREUER, in: EU-Grundrechte-HdB, § 25 N 37.

333 Trotz der vielen Gemeinsamkeiten des datenschutzrechtlichen Gehalts der Grundrechtsinstrumente zeigt die Rechtsprechung, dass verschiedene Gerichte ähnliche Sachverhalte teilweise unterschiedlich bewerten. So teilen bspw. der EGMR und der EuGH im Bereich der Massenüberwachung nicht dieselbe Auffassung. Während der EGMR diese grundsätzlich als zulässig erachtet, nimmt der EuGH eine gegenteilige Sicht ein. Siehe dazu LOCK, in: Commentary EU Treaties and CFR, Art. 8 N 17. Siehe zur Vorratsdatenspeicherung MATTER, 261 ff. Die Rechtsprechung des EuGH zur Vorratsdatenspeicherung zeigt, dass dieser den Datenschutz generell hoch gewichtet. Siehe dazu BERNSDORFF, in: NomosKommentar GRC, Art. 8 N 40.

7.1. Schutzbereich und Eingriff

Eine erste Gemeinsamkeit der drei Grundrechtsinstrumente im Bereich des Datenschutzes findet sich beim persönlichen Schutzbereich. So können sich primär natürliche Personen auf den grundrechtlich geschützten Datenschutz berufen, wobei unter bestimmten Voraussetzungen auch juristische Personen erfasst sind.[334]

Der sachliche Schutzbereich gemäss Art. 13 Abs. 2 BV als auch gemäss Art. 8 GRC umfasst jede Art der Bearbeitung von personenbezogenen Daten. Zudem liegt ein Eingriff im Sinne dieser Bestimmungen immer dann vor, wenn die Grundrechtsadressaten solche Daten bearbeiten. Im Zusammenhang mit Art. 13 Abs. 2 BV wird der Begriff der informationellen Selbstbestimmung verwendet. Dieser Begriff taucht auch in der jüngeren Rechtsprechung des EGMR zu Art. 8 EMRK auf.[335] Obwohl die datenschutzrechtlichen Gewährleistungen der EMRK stetig ausgeweitet wurden und eine Tendenz in Richtung eines Rechts auf informationelle Selbstbestimmung erkennbar ist, nimmt der EGMR stets eine Einzelfallbeurteilung vor. Dabei beurteilt er jeweils unter Berücksichtigung der konkreten Umstände, ob der Anwendungsbereich von Art. 8 EMRK eröffnet ist und ob ein Eingriff vorliegt, wobei die in der Prüfung des EGMR angewendeten Kriterien nicht immer nachvollziehbar erscheinen. Dies führt dazu, dass der EGMR bei der Beurteilung der Besonderheiten des Einzelfalles und der Bejahung resp. Verneinung des Anwendungsbereichs von Art. 8 EMRK relativ frei ist. Der EuGH sowie auch das BGer sind hingegen an die Definition der personenbezogenen Daten gebunden. Dies hat zur Konsequenz, dass wenn solche von einem Grundrechtsadressat bearbeitet werden, die Anwendungsbereiche von Art. 8 GRC (sowie ggf. Art. 7 GRC) resp. Art. 13 Abs. 2 BV stets eröffnet sind.[336]

7.2. Positive Schutzpflichten

Die drei Grundrechtsinstrumente sehen zudem, neben der Abwehrfunktion der Grundrechte, auch gewisse positive Schutzpflichten im Bereich des Datenschutzes vor. Diese sind in Art. 8 EMRK sowie Art. 13 Abs. 2 BV (im Einzelfall) implizit anerkannt und gehen explizit aus dem Wortlaut von Art. 8 GRC hervor.

---

334 Siehe dazu Kapitel II.4.3; II.5.3 sowie II.6.3.
335 Siehe dazu Kapitel II.4.3; II.5.3 sowie II.6.3.
336 Vgl. dazu VON GRAFENSTEIN, 195 ff.

Im Zentrum stehen dabei die den von einer Datenbearbeitung betroffenen Personen zugestandenen Rechte auf Auskunft, Berichtigung und Löschung. Das Recht auf Auskunft über die eigenen Daten stellt den Grundpfeiler dieser Rechte dar.[337]

7.3. Rechtfertigungskriterien

Eine weitere Gemeinsamkeit dieser Grundrechte besteht darin, dass der Schutz der personenbezogenen Daten, welcher von den drei Grundrechtsinstrumenten gewährt wird, nicht absolut gilt. So können Eingriffe in den Schutzbereich unter bestimmten Voraussetzungen gerechtfertigt werden. Während in Art. 8 EMRK die jeweiligen Voraussetzungen einer Rechtfertigung in derselben Bestimmung festgehalten sind, enthält die BV eine allgemeine Bestimmung für die Einschränkung von Grundrechten. Auch in der GRC findet sich eine solche allgemeine Bestimmung. Zudem sind in der GRC die zusätzlichen Kriterien von Art. 8 Abs. 2 S. 1 GRC zu berücksichtigen. Insgesamt unterscheiden sich die Rechtfertigungskriterien der drei Grundrechtsinstrumente zwar teilweise in ihrer Wortwahl resp. in der Prüfreihenfolge. Inhaltlich betrachtet, werden jedoch jeweils dieselben oder zumindest ähnliche Kriterien geprüft.[338]

So muss stets eine gesetzliche Grundlage vorliegen, welche zugänglich und genügend bzw. hinreichend bestimmt sein muss, so dass die Auswirkungen derselben für die betroffenen Personen vorhersehbar sind. Abgesehen von dieser allgemeinen Anforderung an die gesetzliche Grundlage werden gemäss der Rechtsprechung des EGMR, des EuGH sowie des BGer im Bereich des Datenschutzes klare und präzise Regeln hinsichtlich der Datenbearbeitung gefordert, welche die Datenbearbeitung näher ausführen. Ebenso müssen adäquate und effiziente Sicherheitsmassnahmen vorgesehen werden, welche die betroffenen Personen vor einer missbräuchlichen Verwendung der Daten zu schützen vermögen. Diese Kriterien werden von den verschiedenen Gerichten nicht immer beim Kriterium der gesetzlichen Grundlage geprüft. Zum Teil werden diese auch erst bei der Prüfung der Verhältnismässigkeit diskutiert.[339]

---

337 Siehe zu den Einzelheiten Kapitel II.4.4; II.5.4 sowie II.6.4.

338 Vgl. dazu FRA, Opinion IOP, 8 f., wonach Art. 8 Abs. 2 EMRK ähnliche Voraussetzungen wie Art. 52 Abs. 1 GRC verlangt. Siehe dazu auch COLELLA, restriction, 199 f., wonach eine grosse Mehrheit in der Lehre davon ausgeht, dass die Rechtfertigungskriterien der GRC sowie der EMRK gleichwertig sind. Siehe dazu auch BGE 144 I 126, E. 5.1, wonach das BGer Art. 36 BV als die Art. 8 Abs. 2 EMRK entsprechende Bestimmung bezeichnet.

339 Siehe dazu Kapitel II.4.6.1; II.5.6.1 sowie II.6.6.1.

Des Weiteren muss mit der Datenbearbeitung ein im öffentlichen Interesse liegendes Ziel resp. der Schutz von Grundrechten Dritter verfolgt werden. Während diese spezifischen legitimen Ziele in Art. 8 Abs. 2 EMRK abschliessend definiert sind, findet sich weder in der BV noch in GRC eine entsprechende Auflistung. Da die in der EMRK gewählten Begriffe sehr weit ausgelegt werden können, dürften sich die im Rahmen der BV resp. der GRC zulässigen öffentlichen Interessen wohl – zumindest grösstenteils – unter die Begriffe der EMRK subsumieren lassen.[340]

Letztlich wird bei allen drei Grundrechten eine Verhältnismässigkeitsprüfung vorgenommen. Diesbezüglich bedienen sich die BV und die GRC gewisser Unterkategorien, wie u.a. der Geeignetheit resp. der Erforderlichkeit der fraglichen Massnahme. Der EGMR verwendet solche Unterkategorien hingegen nicht explizit. Der Rechtsprechung des Strassburger Gerichts ist jedoch zu entnehmen, dass diese Unterkategorien implizit bei der Verhältnismässigkeitsprüfung herangezogen werden.[341] Die Verhältnismässigkeitsprüfung dient dazu, die sich gegenüberstehenden Interessen gegeneinander abzuwägen. Letztlich geht es um die Frage, ob die Vorteile der Massnahme die Nachteile derselben überwiegen, wobei Nachteile und Risiken einer Massnahme mit angemessenen Garantien gemindert werden können.[342]

Des Weiteren wird im Rahmen von Art. 13 Abs. 2 BV sowie Art. 8 GRC als eigenes Kriterium geprüft, ob im Rahmen der in Frage stehenden Massnahme der Kern des Grundrechts angetastet wird. Der Kerngehalt wurde bis anhin weder für Art. 13 Abs. 2 BV noch Art. 8 GRC klar definiert. Der einschlägigen Rechtsprechung sind jedoch Hinweise zu entnehmen, worin der Wesensgehalt bestehen könnte. Die EMRK hingegen sieht explizit kein äquivalentes Prüfkriterium vor.[343]

340 Siehe dazu Kapitel II.4.6.2; II.5.6.2 sowie II.6.6.3. Siehe zum Verhältnis zwischen der EMRK und der GRC Breuer, in: EU-Grundrechte-HdB, § 25 N 52.

341 Pätzold, in: Karpenstein/Mayer, Kommentar EMRK, Art. 8 EMRK N 97.

342 Siehe dazu Kapitel II.4.6.3; II.5.6.3 sowie II.6.6.4. Vgl. dazu auch FRA/Europarat/EDSB, Handbuch, 55.

343 Siehe dazu Kapitel II.5.6.4 sowie II.6.6.2. Es wird die Ansicht vertreten, dass auch der Rechtsprechung von Strassburg eine Verletzung des Kerns von Grundrechten nicht fremd ist. Dabei wird jedoch kein konsistenter Ansatz verfolgt. Siehe dazu Brkan, essence, 870. Siehe dazu auch Brkan, prism of data privacy, 10 f., 23 ff. m.w.H.

7.4. Besonderes Kriterium: der Zweck

Wie bereits aufgeführt, sind in Art. 8 Abs. 2 S. 1 GRC weitere Kriterien genannt, welche im Bereich des Datenschutzes abgesehen von den allgemeinen Kriterien gemäss Art. 52 GRC zu berücksichtigen sind. Die Kriterien, wonach die Datenbearbeitung nach Treu und Glauben zu erfolgen hat und sich diese (sofern sie nicht auf der Grundlage einer Einwilligung erfolgt) auf eine gesetzlich geregelte legitime Grundlage abstützen muss, finden sich so nicht explizit in der BV oder der EMRK. Wie bereits dargelegt, kommt diesen Elementen aber auch nur begrenzt eine eigenständige Bedeutung zu.[344]

Davon abgesehen ist der GRC auch zu entnehmen, dass der Zweck einer Datenbearbeitung festzulegen ist. Auf die Funktion dieses Kriteriums wurde bereits eingegangen.[345] Diese Ausführungen werden im Folgenden noch ergänzt. Insbesondere wird auch der Frage nachgegangen, ob im Zusammenhang mit dem datenschutzrechtlichen Gehalt von Art. 8 EMRK sowie der informationellen Selbstbestimmung gemäss Art. 13 Abs. 2 BV dem Zweck einer Datenbearbeitung auch eine Bedeutung zukommt.

7.4.1. Relevanz für Art. 8 GRC

Das Erfordernis der Festlegung des Zwecks findet sich ausdrücklich in Art. 8 Abs. 2 S. 1 GRC.[346] Es stellt eine besondere Ausprägung der Vorhersehbarkeit im Datenschutzrecht dar.[347] Der Zweck einer Datenbearbeitung ist bei der gesamten Prüfung der Rechtfertigung eines Eingriffs in Art. 8 GRC zu berücksichtigen.[348] Insofern erfüllt der Zweck einer Datenbearbeitung eine ähnliche

344 Siehe dazu Kapitel II.6.6.5.

345 Siehe dazu Kapitel II.6.6.5.

346 Im EU-Sekundärrecht ist das sog. Prinzip der Zweckbindung verankert. Demnach dürfen personenbezogene Daten nur «*für festgelegte, eindeutige und legitime Zwecke erhoben*» werden. Des Weiteren dürfen diese Daten grundsätzlich «*nicht einer mit diesen Zwecken nicht zu vereinbarenden Weise*» (weiter)verarbeitet werden, wobei Ausnahmen vorgesehen sind (Art. 5 Abs. 1 Bst. b und Abs. 4 DSGVO sowie Art. 4 Abs. 1 Bst. b und Abs. 2 RL 2016/680). Dem Prinzip der Zweckbestimmung lassen sich zwei Elemente entnehmen. Einerseits muss der Zweck einer Datenbearbeitung festgelegt werden. Andererseits darf eine Weiterverarbeitung der Daten grundsätzlich nicht zu einem neuen Zweck vorgenommen werden, welcher mit dem ursprünglichen Zweck nicht vereinbar ist. Siehe dazu ausführlich Koning, 57 ff. m.w.H. Siehe zur Entwicklung des Prinzips der Zweckbestimmung auch in anderen Rechtsinstrumenten Forgó/Hänold/Schütze, 22 ff. m.w.H.

347 Schlussanträge der Generalanwältin Kokott Juliane, Urteil v. 18.07.2007, *Promusicae*, ECLI:EU:C:2007:454, Rz. 53.

348 Siehe dazu Kapitel II.6.6.5.

Funktion wie das öffentliche Interesse einer Massnahme. Denn auch dieses Prüfkriterium stellt einen Bezugspunkt in der gesamten Prüfung der Rechtfertigung eines Eingriffs dar.[349] Trotz dieser ähnlichen Funktion sind die Zweckbestimmung und das öffentliche Interesse voneinander abzugrenzen.

Bei der Festlegung des Zwecks handelt es sich um eine Spezialität des Datenschutzrechts. Der Zweck beschreibt gewissermassen die Zielsetzung einer (einzelnen) Datenbearbeitung. Das öffentliche Interesse hingegen ist ein allgemeines Kriterium, welches nicht nur im Bereich des Datenschutzes bei der Prüfung der Rechtfertigung eines Eingriffs in ein Grundrecht zu berücksichtigen ist. Es bezieht sich auf die in ein Grundrecht eingreifende Massnahme. Der Zweck einer Datenbearbeitung fällt also detaillierter aus als das öffentliche Interesse einer in ein Grundrecht eingreifenden Massnahme.[350] Der Zweck kann jedoch auf das öffentliche Interesse hindeuten.[351]

Aus der Rechtsprechung des EuGH geht zudem hervor, dass eine Datenbearbeitung, welche zu einem anderen als dem ursprünglich festgelegten Zweck erfolgt, eine neue Gefährdungslage darstellt, welche ebenfalls gerechtfertigt werden muss.[352] Im folgenden Kapitel wird sich zeigen, dass bei verschiedenen Informationssystemen bereits solche Zweckerweiterungen vorgenommen wurden. So handelt es sich z.B. bei der Zugriffsgewährung der nationalen Strafverfolgungsbehörden sowie der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) zu Eurodac-Daten um eine Weiterbearbeitung von Daten zu einem anderen Zweck.[353]

---

349 Siehe dazu KONING, 130.

350 Vgl. dazu EDPS, necessity, 10.

351 KONING, 130. Siehe dazu auch BGE 146 I 11, E. 3.3.2, wonach in der gesetzlichen Grundlage der Verwendungszweck nicht klar definiert worden sei und dies es verunmöglicht habe, «*klare Ziele und ein öffentliches Interesse an entsprechenden Überwachungsmassnahmen zu bestimmen oder deren Verhältnismässigkeit zu überprüfen*». Die Abgrenzung zwischen dem Zweck und dem öffentlichen Interesse wurde bei der Interoperabilität nicht immer konsequent vorgenommen. So wurde bspw. in der Folgenabschätzung beim öffentlichen Interesse der Interoperabilitätskomponenten eher auf deren Zweck eingegangen. Siehe dazu EUROPEAN COMMISSION, Impact assessment IOP Part 1, 37 ff.

352 BREUER, in: EU-Grundrechte-HdB, § 25 N 35. Vgl. dazu auch EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 35; EUGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 142 f. Der EuGH nimmt in seiner Rechtsprechung zur GRC nicht ausdrücklich auf das zweite Element des dem EU-Sekundärrecht zu entnehmenden Prinzips der Zweckbindung Bezug. Siehe dazu KONING, 139 ff. m.w.H.

353 BROUWER, purpose limitation, 282 f. Die Notwendigkeit sowie Verhältnismässigkeit dieses Zugangs wurde verschiedentlich in Frage gestellt. Siehe dazu z.B. FRA, Opinion Eurodac 2016, 40 ff. Als weitere Beispiele von Zweckerweiterungen werden die RL 2006/24/EG sowie die PNR-Daten genannt. Siehe dazu WP29, Opinion purpose limitation, 67 ff.

7.4.2. Relevanz für Art. 8 EMRK

Anders als in Art. 8 Abs. 2 GRC findet sich in Art. 8 EMRK kein expliziter Verweis auf das Erfordernis der Festlegung des Zwecks einer Datenbearbeitung.[354] Insofern stellt der Zweck kein ausdrückliches Kriterium im Rahmen der Prüfung einer Rechtfertigung eines Eingriffs in den datenschutzrechtlichen Gehalt von Art. 8 EMRK dar. Dennoch wird der Ausgangspunkt der Entwicklung des Prinzips der Zweckbestimmung darin angesehen, dass die Strassburger Organe bestimmte Anforderungen an die gesetzliche Grundlage entwickelt haben, welche den Eingriff begrenzen sollen.[355] Damit wird die Datenbearbeitung nämlich näher definiert. Anhand der Festlegung der Bedingungen einer Datenbearbeitung kann auch auf den Zweck einer Datenbearbeitung geschlossen werden, sofern dieser nicht explizit in der gesetzlichen Grundlage selbst wiedergegeben wird. So können z.B. die Art der erhobenen Daten oder auch der Umstand, von welchen Personen Daten erhoben werden resp. wer die Daten bearbeiten darf, Hinweise hinsichtlich des Zwecks der Datenbearbeitung liefern.[356]

Vereinzelt nimmt der EGMR direkt Bezug auf den Zweck der Datenbearbeitung. So führte der EGMR z.B. in *Gardel*[357] aus, dass die bearbeiteten Daten einschlägig und im Vergleich mit dem Zweck nicht übermässig erscheinen dürften. Zudem dürften die Daten nicht länger aufbewahrt werden als für den Zweck notwendig.[358] Auch wenn der Zweck der Datenbearbeitung in der Rechtsprechung des EGMR häufig keine explizite Rolle hat, so fliesst dieses Erfordernis dennoch bei der Beurteilung der Rechtfertigung eines Eingriffs in den datenschutzrechtlichen Gehalt von Art. 8 EMRK ein.[359]

---

354 Der Konvention 108 des Europarats ist hingegen das Prinzip der Zweckbestimmung zu entnehmen. Gemäss diesem müssen personenbezogene Daten, welche automatisch verarbeitet werden, für festgelegte und rechtmässige Zweck gespeichert werden und dürfen nicht so verwendet werden, dass eine Unvereinbarkeit mit diesem Zweck bestehen würde. Siehe dazu SIEMEN, 136. Dieses Prinzip enthält also auch – wie das Prinzip der Zweckbestimmung des EU-Sekundärrechts – zwei Elemente.

355 FORGÓ/HÄNOLD/SCHÜTZE, 22.

356 Vgl. dazu auch KONING, 119 f.

357 EGMR, Urteil v. 17.12.2009, *Gardel v. France*, Beschwerde Nr. 16428/05.

358 EGMR, Urteil v. 17.12.2009, *Gardel v. France*, Beschwerde Nr. 16428/05, Rz. 62. Siehe zur Erwähnung des Zwecks in der Rechtsprechung des EGMR auch EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 103.

359 Siehe dazu KONING, 130.

Bei einer Weiterbearbeitung von Daten geht der EGMR von einem zusätzlichen Eingriff aus.[360] Ein solcher ist ebenfalls rechtfertigungsbedürftig. Insbesondere das Erfordernis einer gesetzlichen Grundlage ist zu prüfen.[361] Der EGMR prüft die Nähe des Zwecks der ursprünglichen Datenbearbeitung und dem Zweck der Weiterbearbeitung unter dem Kriterium der Vorhersehbarkeit.[362]

Die Rechtsprechung des EGMR zeigt, dass dem Zweck einer Datenbearbeitung insbesondere beim «*test of reasonable expectations*» eine entscheidende Rolle zukommen kann.[363] Diesen Test nimmt das Gericht bei der Frage, ob ein Eingriff in Art. 8 EMRK vorliegt, vor.[364]

7.4.3. Relevanz für Art. 13 Abs. 2 BV

Wie in der EMRK, fehlt auch in der BV ein expliziter Verweis auf das Erfordernis der Festlegung des Zwecks einer Datenbearbeitung.[365] Die Rechtsprechung des BGer zeigt jedoch, dass das Gericht im Rahmen von verschiedenen Rechtfertigungskriterien Bezug auf den Zweck genommen hat. So hat das BGer in einem Entscheid zum damals noch ungeschriebenen Verfassungsrecht der persönlichen Freiheit ausgeführt, dass die *in casu* vorgenommene systematische Erhebung besonders sensibler Daten für die Betroffenen nicht voraussehbar gewesen sei. Es wäre eine klare gesetzliche Grundlage notwendig gewesen, welche u.a. klar geregelt hätte, «*unter welchen Voraussetzungen und zu welchem Zweck*» eine Registrierung vorgenommen werden dürfe.[366]

---

360 EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 48. Siehe dazu u.a. auch EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 46; EGMR, Urteil v. 29.06.2006, *Weber and Saravia v. Germany*, Beschwerde Nr. 54934/00, Rz. 79.

361 Vgl. dazu VILLIGER, N 672.

362 Siehe dazu KONING, 145 ff. mit Verweis auf Beispiele aus der Rechtsprechung.

363 Siehe dazu VON GRAFENSTEIN, 182 ff. m.w.H. Der EuGH benutzt den vom EGMR entwickelten «*test of reasonable expectations*» bis anhin nicht. Der EU-Gesetzgeber hat jedoch stattdessen im Sekundärrecht das Prinzip der Zweckbestimmung vorgesehen. Die Elemente dieses Prinzips sind eng mit den berechtigten Erwartungen der von der Datenbearbeitung betroffenen Person verbunden. Siehe dazu VON GRAFENSTEIN, 360.

364 Siehe dazu Kapitel II.4.5.

365 Das Prinzip der Zweckbestimmung ist in der Schweiz jedoch ausdrücklich auf Gesetzesstufe verankert. Gemäss Art. 6 Abs. 3 DSG dürfen personenbezogene Daten nur für einen bestimmten Zweck beschafft werden, welcher für die betroffenen Personen erkennbar ist. Die Datenbearbeitung darf nur derart erfolgen, dass diese mit dem Zwecke vereinbar ist.

366 BGE 122 I 360, E. 5d. In BGE 148 I 233, E. 4.5.4 wird ebenfalls bei der Prüfung der gesetzlichen Grundlage auf den Datenbearbeitungszweck eingegangen.

In einem anderen Urteil äusserte sich das BGer dahingehend, dass der Zweck einer Datenbearbeitung den Ausgangspunkt darstelle, um zu prüfen, ob die Dauer einer Aufbewahrung von Daten verhältnismässig sei.[367] Bei der Beurteilung der Verpflichtung der Fernmeldeanbieter, gewisse Randdaten zu speichern, damit diese ggf. von Strafverfolgungsbehörden eingesehen werden können, erwähnte das BGer den Zweck der Datenbearbeitung beim öffentlichen Interesse.[368] Im selben Urteil nimmt das BGer bei der Prüfung der Sicherheitsmassnahmen nochmals Bezug auf den Zweck der Datenbearbeitung und führt aus, dass dieser für die Betroffenen bereits bei der Erhebung der Daten erkennbar gewesen sei.[369] Abgesehen davon geht auch aus dem regelmässig vom BGer verwendeten Beschrieb der informationellen Selbstbestimmung die Bedeutung des Zwecks der Datenbearbeitung hervor. Demnach muss die betroffene Person «*gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können*», «*ob und zu welchem Zweck diese Informationen über sie bearbeitet werden*».[370]

Auch das BGer hatte sich bereits mit einer Weiterbearbeitung von Daten zu befassen. Das Gericht stellte dabei fest, dass die *in casu* vorgenommene Weitergabe von gesundheitsbezogenen Daten nicht dem ursprünglichen Zweck entspreche. Die Weitergabe wurde als eigenständiger Eingriff in die informationelle Selbstbestimmung bewertet, weshalb im Anschluss die Rechtfertigungskriterien gemäss Art. 36 BV geprüft wurden.[371]

7.5. Abgrenzung zu anderen Grundrechten

Der Datenschutz weist teilweise Ähnlichkeiten mit dem Schutzgehalt von anderen Grundrechten auf und ist deshalb von diesen abzugrenzen. Darunter fallen insbesondere andere Rechte der Privatsphäre sowie die grund- und menschenrechtlichen Rechtsschutzgarantien.[372]

Die enge Verbundenheit zwischen dem Datenschutz und der Privatsphäre zeigt sich anschaulich am Beispiel von Art. 7 und Art. 8 GRC. Der Rechtsprechung des EuGH ist zu entnehmen, dass diese beiden Grundrechte häufig

367 BGE 133 I 77, E. 5. Siehe dazu auch BGE 146 I 11, E. 3.3.2, wonach sich die Speicherung der erhobenen Daten am Verwendungszweck zu orientieren habe. Siehe zur Bezugnahme auf den Zweck bei der Verhältnismässigkeitsprüfung BGE 147 I 346, E. 5.5.

368 BGE 144 I 126, E. 7.

369 BGE 144 I 126, E. 8.3.6.

370 BGE 144 I 126, E. 4.1 (mit weiteren Hinweisen auf die Rechtsprechung).

371 Siehe dazu BGE 148 I 233, E. 3 ff.

372 Siehe dazu Kapitel II.4.7; II.5.7 sowie II.6.7. Vgl. dazu SCHWEIZER, wirksame Beschwerde, 72.

gemeinsam geprüft werden, wenn es um die Bearbeitung von personenbezogenen Daten geht. Weil diese beiden Grundrechte nicht klar voneinander abgegrenzt werden können, kann deshalb Art. 7 GRC für die weiteren Ausführungen in der vorliegenden Arbeit nicht gänzlich unberücksichtigt bleiben.

8. Fazit

Aus dem vorliegenden Kapitel geht hervor, dass der Gehalt der EMRK den Mindestschutz darstellt, welcher sowohl für die Schweiz als auch die Mitgliedstaaten verbindlich ist. Die BV als auch die GRC können einen weitergehenden Schutz gewährleisten. Der Rechtsprechung des BGer sowie des EuGH ist zu entnehmen, dass im Bereich des Datenschutzes vielfach auf die Rechtsprechung der Strassburger Organe verwiesen wird. Dementsprechend ist es nicht überraschend, dass der datenschutzrechtliche Gehalt dieser drei Grundrechtsinstrumente viele Gemeinsamkeiten aufweist. Zudem sind auch die Anforderungen an die Rechtfertigung eines Eingriffs in die Grundrechte gemäss Art. 8 EMRK, Art. 13 Abs. 2 BV sowie Art. 8 GRC vergleichbar.

Eine Besonderheit ist das spezielle Verhältnis von Art. 8 GRC und Art. 7 GRC. Aufgrund der engen Verbundenheit dieser beiden Grundrechte erscheint es angezeigt, dass im datenschutzrechtlichen Kontext Art. 7 GRC ebenfalls berücksichtigt wird.

Die vorstehenden Ausführungen haben ausserdem gezeigt, dass dem Zweck einer Datenbearbeitung im Datenschutzrecht eine zentrale Bedeutung zukommt. Dieses Erfordernis, wonach jede Datenbearbeitung einen festgelegten Zweck verfolgen muss, ist in Art. 8 Abs. 2 GRC explizit festgehalten. Auch ohne ausdrückliche Nennung in der BV und der EMRK geht aus der Rechtsprechung des BGer sowie des EGMR hervor, dass dem Zweck einer Datenbearbeitung auch im Zusammenhang mit Art. 13 Abs. 2 BV resp. Art. 8 EMRK eine besondere Rolle bei der gesamten Prüfung der Rechtfertigung eines Eingriffs zukommen kann. Der Zweck einer Datenbearbeitung dient – ähnlich wie das Kriterium des öffentlichen Interesses – als Bezugspunkt bei der Beurteilung der Rechtfertigung eines Eingriffs in den grundrechtlich geschützten Datenschutz. Dennoch sind diese beiden Kriterien voneinander zu unterscheiden.

Abgesehen davon hat sich auch gezeigt, dass eine Weiterbearbeitung von Daten zu einem anderen Zweck, eine sog. Zweckerweiterung, nicht *per se* unzulässig ist. Vielmehr deutet die Rechtsprechung des EuGH, des EGMR sowie des BGer darauf hin, dass eine Zweckerweiterung als neuer Eingriff zu werten ist,

welcher ebenfalls – also wie die Datenbearbeitung zum ursprünglich festgelegten Zweck – rechtfertigungsbedürftig ist.

III. EU-Informationssysteme

1. Einleitung

Das folgende Kapitel dient der Darstellung der von der Interoperabilität betroffenen Informationssysteme. Auf die Erklärung des Konzepts der Interoperabilität wird (vorerst) bewusst verzichtet. Diese folgt im anschliessenden Kapitel. Damit die Ausgestaltung und der Umfang der geplanten Interoperabilität besser nachvollzogen werden können, erscheint es sinnvoll, zuerst die von der Interoperabilität betroffenen Informationssysteme zu kennen. Deshalb wird im Folgenden u.a. erläutert, vor welchem Hintergrund die von der Interoperabilität betroffenen Informationssysteme entstanden sind, welchen Zweck sie erfüllen, wie sie funktionieren, welche Daten in diesen Systemen gespeichert werden und wer auf diese Daten zugreifen darf. Diese Darstellung hat jedoch nicht das Ziel, diese Systeme (aus datenschutzrechtlicher Perspektive) kritisch zu würdigen.[373] Die vorliegende Untersuchung beschäftigt sich ausschliesslich mit der anvisierten Verknüpfung dieser Systeme, weshalb die Bewertung der einzelnen Systeme nicht vom Gegenstand derselben erfasst ist.[374]

Durch die Interoperabilität sollen insbesondere sechs Informationssysteme aus den Bereichen Grenzmanagement, Migration und Sicherheit miteinander verknüpft werden. Es handelt sich dabei um das Schengener Informationssystem (SIS), das Visa-Informationssystem (VIS), die Eurodac-Datenbank, das Einreise- und Ausreisesystem (EES), das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) sowie das Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN).[375]

---

373 Es gibt durchaus verschiedene Aspekte, welche aus datenschutzrechtlicher Perspektive näher beleuchtet werden könnten. So z.B. die teilweise sehr lange Speicherfrist bei der Eurodac-Datenbank (Kapitel III.5.4), die auf das nationale Recht abstellende Speicherfrist bei ECRIS-TCN (Kapitel III.9.4), der automatisierte Abgleich in anderen Datenbanken bei ETIAS (Kapitel III.8.4) oder die sehr grosszügige Möglichkeit, ECRIS-TCN-Daten für ganz unterschiedliche Zwecke zu verwenden (Kapitel III.9.1).

374 Siehe dazu Kapitel I.2.

375 Siehe dazu Kapitel IV.5.2.

Abgesehen von diesen sechs Informationssystemen sollen auch zwei Interpol-Datenbanken[376] sowie die Europol-Daten[377] partiell in die Interoperabilität eingebunden werden.[378] Da diese nicht vollumfänglich in die Interoperabilität integriert werden, wird im Folgenden darauf verzichtet, näher auf diese Datenbanken resp. die Europol-Daten einzugehen.[379]

Der Darstellung der genannten Informationssysteme werden einige allgemeine Ausführungen zur Schengener und Dubliner Zusammenarbeit resp. zur Assoziierung der Schweiz an Schengen und Dublin vorangestellt. Diese sind notwendig, da die Umsetzung der Interoperabilität in der Schweiz im Fokus der vorliegenden Untersuchung steht und die Assoziierung der Schweiz an Schengen und Dublin das Fundament der Beteiligung der Schweiz an diesem EU-Projekt darstellt. Das Kapitel schliesst mit einem Fazit, in welchem u.a. die Gemeinsamkeiten und Unterschiede der Informationssysteme beleuchtet werden.

2. Schengener und Dubliner Zusammenarbeit

2.1. Schengener Zusammenarbeit

Als im Jahr 1985 Belgien, Luxemburg, die Niederlande, Deutschland und Frankreich das Schengener Übereinkommen (SÜ) im gleichnamigen luxemburgi-

376 Dabei handelt es sich um die Interpol-Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten («*Travel Documents Associated with Notices*», TDAWN) sowie um die Interpol-Datenbank für gestohlene und verlorene Reisedokumente («*Stolen and Lost Travel Documents*», SLTD).

377 Bei den Europol-Daten handelt es sich um diejenigen Daten, welche zu bestimmten Zwecken von Europol verarbeitet werden dürfen. Siehe dazu Art. 4 Ziff. 16 EU-IOP-VO. Die Europol-Daten können von den Mitgliedstaaten sowie auch von Europol für Abfragen und Analysen bezüglich schwerer Kriminalität und Terrorismus verwendet werden. Siehe dazu EUROPEAN COMMISSION, Impact assessment IOP Part 2, 26 f. Bei Europol werden keine Datenbanken definiert. Es wird vielmehr ein technologieneutraler Ansatz in Bezug auf das Datenmanagement und die Datenverarbeitung verfolgt. Demnach stehen die Zwecke der Datenbearbeitung im Zentrum. Siehe dazu <https://www.europol.europa.eu/processing-of-personal-data>, zuletzt besucht am 07.03.2025. Insofern wird deshalb der Begriff Europol-*Daten* verwendet.

378 Art. 3 Abs. 1 und Art. 6 Abs. 1 EU-IOP-VO; BUNDESRAT, Botschaft IOP, 8000 f.

379 Zudem stellen sich teilweise Fragen, welche die anderen sechs Datenbanken nicht betreffen. Siehe z.B. zu spezifischen Fragen zu den Interpol-Datenbanken FRA, Opinion IOP, 19 f.; SFH, Vernehmlassungsantwort, 11.

schen Ort unterzeichneten, wurde der Schengen-Raum geschaffen.[380] Diese fünf Staaten beschlossen im Rahmen dieses multilateralen Vertrags, die Kontrollen an ihren Binnengrenzen – also den Grenzen zwischen den Vertragsparteien[381] – schrittweise abzuschaffen. Der Schutz der Aussengrenzen – also den Grenzen mit denjenigen Staaten, welche nicht an Schengen partizipieren[382] – wurde dabei nicht konkret geregelt. Es wurde jedoch eine verstärkte Zusammenarbeit in der Bekämpfung des illegalen Handels von Betäubungsmitteln und Waffen sowie der illegalen Einreise angestrebt. Im Jahr 1990 wurde für die Umsetzung des SÜ schliesslich das Schengener Durchführungsübereinkommen (SDÜ) abgeschlossen.[383]

Mit dem SDÜ wurden insbesondere die systematischen Identitätskontrollen an den Binnengrenzen abgeschafft, um so den Personenverkehr zwischen den Schengen-Staaten zu erleichtern. Damit die Sicherheit dennoch gewährleistet werden konnte, wurden verschiedene Ausgleichsmassnahmen ergriffen. So wurden u.a. die Kontrollen an den Schengen-Aussengrenzen verstärkt. Des Weiteren wurde eine gemeinsame Visapolitik für kurzfristige Aufenthalte geschaffen, die polizeiliche Kooperation und justizielle Zusammenarbeit in Strafsachen – insbesondere durch die Entwicklung des SIS – verbessert, die Gesetzgebung im Bereich der Waffen und Betäubungsmittel vereinheitlicht und es wurde ein Datenschutz-Mindeststandard definiert.[384]

Mit dem Inkrafttreten des im Jahr 1997 unterzeichneten Vertrags von Amsterdam wurden die zu Schengen gehörenden Rechtsakte und Massnahmen, der sog. Schengen-Besitzstand resp. Schengen-*Acquis*, in die EU-Rechtsordnung

380 Bereits davor existierte das Saarbrücker Regierungsübereinkommen. Dieser zwischen Frankreich und Deutschland geschlossene völkerrechtliche Vertrag sah den Abbau von Binnengrenzkontrollen vor und beinhaltete auch Ausgleichs- und Begleitmassnahmen zur Vermeidung von Sicherheitseinbussen. Nach dem Beitritt von weiteren Staaten wurde schliesslich das SÜ abgeschlossen, welches als längerfristiges Ziel den kompletten Abbau von Binnengrenzkontrollen vorsah. Vgl. dazu GOOD, 9 ff.

381 Bei den Binnengrenzen handelt es sich gemäss Art. 1 SDÜ um gemeinsame Landgrenzen der Vertragsparteien, Flughäfen für Binnenflüge zwischen den Vertragsparteien sowie Seehäfen, welche direkte und regelmässige Fährverbindungen zwischen den Vertragsparteien anbieten.

382 Gemäss Art. 1 SDÜ handelt es sich bei den Aussengrenzen um «*die Land- und Seegrenzen sowie die Flug- und Seehäfen der Vertragsparteien, soweit sie nicht Binnengrenzen sind*».

383 Die Schengener Zusammenarbeit entstand somit ausserhalb der damaligen Europäischen Wirtschaftsgemeinschaft (EWG). Der EWG fehlten zum damaligen Zeitpunkt die entsprechenden Kompetenzen für den Abschluss eines solchen Vertrages. Zudem wollten sich zu jenem Zeitpunkt nicht alle Mitgliedstaaten an der Schengener Zusammenarbeit beteiligen. Siehe dazu KOLLER, 910 f.; STÄMPFLI, 6 f.; MOHLER, Stresstest, 8 f.

384 CORNU, 211.

überführt.[385] Dazu musste hinsichtlich jeder Bestimmung resp. jedes Beschlusses des Schengen-Besitzstands eine Rechtsgrundlage bestimmt werden.[386] So wurden z.B. die Bereiche Grenzkontrollen und Visa in den ersten Pfeiler der damaligen Pfeilerstruktur der EU migriert, die polizeiliche Kooperation sowie die justizielle Zusammenarbeit in Strafsachen in den dritten.[387]

Mit den im Jahr 2007 abgeschlossenen Verträgen von Lissabon über die Europäische Union (EUV) und die Arbeitsweise der Europäischen Union (AEUV) wurde die Pfeilerstruktur der Europäischen Union aufgehoben. Des Weiteren erlangte die Union Rechtspersönlichkeit.[388] Die in den Schengen-Bereich fallenden Gebiete betreffend Grenzkontrollen, Einwanderung und justizielle sowie polizeiliche Zusammenarbeit finden sich seither zusammengefasst unter dem Titel «*Der Raum der Sicherheit, der Freiheit und des Rechts*»[389] im AEUV.[390]

Der Schengen-Raum besteht neben den Mitgliedstaaten auch aus den assoziierten Staaten Norwegen, Liechtenstein, Island sowie der Schweiz. Einzelne Mitgliedstaaten beteiligen sich jedoch lediglich partiell an der Schengener Zusammenarbeit resp. verfügen über eine Sonderstellung.[391]

385 Diese Integration stützte sich dabei auf das sog. Schengen-Protokoll. Siehe dazu Stämpfli, 24 f. Vgl. zum Stand des Schengen-Besitzstands im Zeitpunkt des Inkrafttretens des Vertrags von Amsterdam Art. 1 Abs. 2 Beschluss 1999/435/EG. Siehe zur Definition des Schengen-*Acquis* auch Wagner, 12 ff.

386 Vgl. dazu den Beschluss 1999/436/EG. Siehe dazu auch Epiney, Schengen, Dublin, 303 f.

387 Bundesrat, Botschaft Bilaterale II, 6067 ff. Siehe zur Integration des Schengen-Besitzstands in den Rechtsrahmen der Union auch Cornu, 212 ff. m.w.H.; Wagner m.w.H.; Stämpfli, 25 ff. m.w.H.

388 Vgl. dazu Art. 47 EUV.

389 Der «*Raum der Freiheit*» soll die Bewegungsfreiheit der UnionsbürgerInnen (inkl. Drittstaatsangehörige mit einem rechtmässigen Aufenthaltsstatus) gewährleisten. Des Weiteren soll eine gemeinsame Asyl- und Einwanderungspolitik betrieben und die Aussengrenzen einer verstärkten Kontrolle unterzogen werden. Der «*Raum der Sicherheit*» soll durch die effiziente Bekämpfung von internationaler Kriminalität herbeigeführt werden. Der «*Raum des Rechts*» soll einen besseren Zugang zum Recht bei grenzüberschreitenden Rechtsstreitigkeiten erzielen. So soll für die BürgerInnen der Zugang zur Justiz in jedem Mitgliedstaat gleich ausgestaltet sein sowie die gegenseitige Anerkennung von gerichtlichen Urteilen im Zivil- sowie auch Strafrecht vereinfacht werden. Vgl. dazu Koller, 912 f.

390 Vgl. dazu Titel V AEUV. Mohler, Stresstest, 11; Wüger, 69 f.

391 Siehe dazu Cornu, 214 ff. m.w.H. Eine Karte, welche den Schengen-Raum abbildet, findet sich auf der Webseite des BJ, abrufbar unter <https://www.bj.admin.ch/bj/de/home/sicherheit/schengen-dublin.html>, zuletzt besucht am 07.03.2025.

2.2. Dubliner Zusammenarbeit

Die Dubliner Zusammenarbeit entstand – ebenso wie die Schengener Zusammenarbeit – ausserhalb der EU-Rechtsordnung. Der völkerrechtliche Vertrag, das Dubliner Übereinkommen (DÜ), wurde im Jahr 1990 nur wenige Tage vor dem SDÜ von den damals zwölf EG-Staaten[392] unterzeichnet, trat jedoch erst am 1. September 1997 in Kraft. Ursprünglich hätte der Inhalt des DÜ einen Teil des SDÜ darstellen sollen.[393] Dies zeigt die enge Verbundenheit von Schengen und Dublin auf. Da sich die Vertragsparteien jedoch im Asylbereich für ein separates Abkommen aussprachen, entstand schliesslich das DÜ.[394] Der Einbezug des Asylrechts in das EU-Recht gestaltete sich anfänglich insbesondere deshalb schwierig, da die Mitgliedstaaten sehr unterschiedliche Gesetzgebungen in diesem Gebiet aufwiesen. Erst mit dem im Jahr 1997 unterzeichneten Vertrag von Amsterdam konnten schliesslich Grundsätze für eine gemeinsame europäische Asylpolitik festgelegt werden.[395]

Mit dem DÜ wurden drei Ziele verfolgt. Erstens sollte der Asylantrag eines Drittstaatsangehörigen nur von einem einzigen Dublin-Staat beurteilt werden. Zweitens sollte die Zuständigkeit der Mitgliedstaaten durch klare Zuständigkeitsregeln gewährleistet werden, womit das Weiterschieben von Asylsuchenden verunmöglicht werden sollte. Drittens sollte verhindert werden, dass eine Person mehrere Asylgesuche in mehreren Dublin-Staaten stellen kann.[396]

Das DÜ wurde vorerst im ersten Pfeiler der Union untergebracht. Im Jahr 2003 wurde das Abkommen als Verordnung, die Verordnung (EG) Nr. 343/2003 (Dublin-II-VO), in das Gemeinschaftsrecht überführt.[397] Am 1. Januar 2014 trat schliesslich die Verordnung (EU) Nr. 604/2013 (Dublin-III-VO), eine Weiterentwicklung der Dublin-II-VO, in Kraft.[398] Am 14. Mai 2024 wurde vom Rat das sog. Asyl- und Migrationspaket angenommen. Damit wurden verschiedene Rechtsakte verabschiedet, welche u.a. die Dublin-III-VO (sowie auch die Euro-

392 Belgien, Dänemark, Deutschland, Griechenland, Spanien, Frankreich, Italien, Luxemburg, Niederlande, Portugal, Irland und Grossbritannien. KOEHLER, 26. Das Vereinigte Königreich sowie Irland haben das Abkommen nicht ratifiziert. Vgl. dazu MOHLER, Stresstest, 10.

393 Art. 28 ff. SDÜ enthalten Kriterien zur Zuständigkeitsverteilung der Asylgesuche. Diese wurden jedoch zwecks Kollisionsvermeidung mit dem DÜ für unanwendbar erklärt. Vgl. dazu PROGIN-THEUERKAUF/EGBUNA-JOSS, 29 f.

394 PROGIN-THEUERKAUF/EGBUNA-JOSS, 30; BUNDESRAT, Botschaft Bilaterale II, 6069 f.; KOLLER, 911.

395 BUNDESRAT, Botschaft Bilaterale II, 6112 f.

396 JORNS, 1589 f.

397 PROGIN-THEUERKAUF/EGBUNA-JOSS, 30.

398 KOEHLER, 41.

dac-VO) revidieren werden. Die Anwendung dieser Verordnungen steht noch bevor.[399]

Die derzeit noch gültige Dublin-III-VO beinhaltet einen Katalog von festgelegten Kriterien, anhand welchen der Dublin-Staat bestimmt wird, welcher für die Prüfung eines Asylgesuchs einer Person zuständig ist.[400] Es handelt sich dabei um ein reines Zuständigkeitsverteilungssystem.[401] Damit soll letztlich eine ausgewogene Verteilung der asylsuchenden Personen auf die Dublin-Staaten herbeigeführt werden.[402] Ist eine Vertragspartei der Ansicht, dass ein in ihrem Hoheitsgebiet gestelltes Asylgesuch gemäss dem Kriterienkatalog nicht in ihre Zuständigkeit fällt, so kann diese dem vermeintlich zuständigen Dublin-Staat ein Aufnahmegesuch zustellen. Wurde das Gesuch einer asylsuchenden Person bereits in einem anderen Dublin-Staat geprüft, so kann der Dublin-Staat, in welchem ein zweites Mal um Schutz ersucht wurde, denjenigen Dublin-Staat um Übernahme ersuchen, in welchem erstmals ein Gesuch gestellt worden ist.[403]

Die Anwendung der Dubliner Zuständigkeitskriterien gestaltete sich anfänglich insbesondere deshalb schwierig, weil die Dublin-Staaten kaum den Beweis für das Zuständigkeitskriterium, insbesondere den Ort der Einreise in einen Dublin-Staat, zu erbringen vermochten. Zur Verbesserung des Dublin-Systems trug schliesslich die im Jahr 2000 eingeführte Eurodac-Datenbank bei.[404]

Der Bereich Asyl ist – wie auch die in die Schengener Zusammenarbeit fallenden Bereiche – im Titel V des AEUV geregelt.[405] Gestützt auf diese primärrechtliche Grundlage wurde das Gemeinsame Europäische Asylsystem (GEAS) geschaffen. Dieses soll sicherstellen, dass die Schutzsuchenden innerhalb der EU den gleichen gesetzlichen Normen unterworfen sind. Relevant in diesem Zusammenhang sind vor allem die Dublin-III-VO, die RL 2013/32/EU (Asylverfahrensrichtlinie), die RL 2011/95/EU (Qualifikationsrichtlinie), die RL 2013/33/EU (Aufnahmerichtlinie) sowie die Verordnung (EU) 603/2013 (Eurodac-

399 Siehe dazu Kapitel III.5.7.

400 Siehe dazu Caroni, et al., § 6 N 367 ff. m.w.H. Siehe zu den Kriterien Art. 7 ff. Dublin-III-VO. Aufgrund der geografischen Lage profitiert die Schweiz vom Dublin-System, da grundsätzlich derjenige Staat für die Prüfung eines Asylgesuchs zuständig ist, über dessen Grenze die Einreise in den Dublin-Raum erfolgte. Siehe dazu Spescha, et al., 439.

401 Progin-Theuerkauf/Egbuna-Joss, 126.

402 Bundesrat, Botschaft Bilaterale II, 5968.

403 Bundesrat, Botschaft Bilaterale II, 6114 ff.

404 Gloor Scheidegger, 138; Bundesrat, Botschaft Bilaterale II, 6111. Auf die Eurodac-Datenbank wird in Kapitel III.5 ausführlich eingegangen.

405 Vgl. dazu Art. 78 AEUV.

VO). Während die Qualifikationsrichtlinie definiert, welche Personen als Flüchtlinge anzuerkennen sind resp. welchen Personen subsidiärer Schutz zukommen soll, befasst sich die Aufnahmerichtlinie mit den Mindeststandards asylsuchender Personen während des Asylverfahrens. Dieses Verfahren hat zudem den Anforderungen der Asylverfahrensrichtlinie zu entsprechen.[406] Die Eurodac-VO regelt die Einzelheiten zum Anwendungsbereich der gleichnamigen Datenbank. Nicht alle Richtlinien des GEAS sind Teil des Dublin-Systems.[407] Dieses besteht lediglich aus der Dublin-III-VO sowie der Eurodac-VO.[408]

An der Dubliner Zusammenarbeit beteiligen sich neben den Mitgliedstaaten auch die assoziierten Staaten Norwegen, Island, Liechtenstein sowie die Schweiz. Wie bei der Schengener Zusammenarbeit haben gewisse Mitgliedstaaten eine Sonderstellung.[409]

3. Assoziierung der Schweiz an Schengen und Dublin

3.1. Geschichtlicher Hintergrund

Die Assoziierung der Schweiz an Schengen und Dublin erfolgte im Rahmen der im Jahr 2004 abgeschlossenen Bilateralen II.[410] Da der Inhalt von Dublin ursprünglich als Ausgleichsmassnahme der Schengener Zusammenarbeit vorgesehen war und deshalb Schengen und Dublin untrennbar miteinander verbunden sind, war eine Assoziierung der Schweiz an nur einen Teil nicht möglich. Die beiden Assoziierungen konnten zudem nur gemeinsam in Kraft treten.[411]

406 Siehe m.w.H. zum GEAS Caroni, et al., § 6 N 345 ff.

407 Progin-Theuerkauf/Egbuna-Joss, 186 f.

408 Europäische Kommission, Vorschlag Eurodac Neufassung 2016, 2.

409 Eine Karte, welche den Dublin-Raum abbildet, findet sich auf der Webseite des BJ, abrufbar unter <https://www.bj.admin.ch/bj/de/home/sicherheit/schengen-dublin.html>, zuletzt besucht am 07.03.2025.

410 Stämpfli, 35. Bereits davor hatten die Schweiz und die EU zahlreiche bilaterale Abkommen abgeschlossen. Siehe dazu Oesch, Grundrechte, 176 ff. m.w.H. Siehe zu den Bilateralen I und II Epiney/Metz/Pirker, 101 ff. m.w.H.; Pirker/Epiney, 41 ff. m.w.H.; Baumgartner, et al., 422 ff. m.w.H. Siehe zu den Entwicklungen hinsichtlich der «*Bilateralen III*» Epiney, Rechtsschutz. Siehe zu den bilateralen Abkommen auch Oesch, Europarecht, N 961 ff.

411 Art. 15 Abs. 4 SAA; Art. 14 Abs. 2 DAA; Bundesrat, Botschaft Bilaterale II, 6124.

Mit der Assoziierung der Schweiz an Schengen und Dublin wurde – anders als mit anderen Abkommen zwischen der Schweiz und der EU – eine «*Teilintegration*» der Schweiz in das entsprechende EU-Recht beabsichtigt.[412]

Mit der Schengen/Dublin-Assoziierung wirkte die Schweiz einer Isolierung im Bereich der Sicherheitspolitik in Europa entgegen. Es bestanden zwar davor schon bilaterale Verträge mit den umliegenden Staaten, welche sicherheitspolitische Aspekte regelten. Diese konnten jedoch kaum erweitert werden, da die diesbezüglichen Kompetenzen von den Mitgliedstaaten an die EU übertragen worden waren. Ausserdem bestand von den Mitgliedstaaten wenig Interesse neben dem Schengen- und Dublin-System ein paralleles Konstrukt mit der Schweiz aufzubauen.[413]

3.2. Assoziierungsabkommen

Zwecks Assoziierung der Schweiz an Schengen und Dublin wurden zwei separate Abkommen zwischen der Schweiz und der EU bzw. der EG abgeschlossen: das Schengen-Assoziierungsabkommen (SAA) und das Dublin-Assoziierungsabkommen (DAA). Diese beiden Abkommen wurden durch weitere Rechtsakte ergänzt, um einerseits den Besonderheiten von bestimmten Mitgliedstaaten Rechnung zu tragen und andererseits die anderen assoziierten Staaten einzuschliessen.[414] Im Rahmen der Schengen-Assoziierung enthält der Briefwechsel zur Komitologie zudem die Verpflichtung der EU, die Beteiligung der Schweiz bei den Arbeiten der Ausschüsse separat zu regeln. Diese Ausschüsse unterstützen die Kommission bei der Ausübung ihrer Durchführungsbefugnisse.[415] Die Einzelheiten der Beteiligungsrechte in diesen Ausschüssen in Bezug auf die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands sind der Komitologievereinbarung zu entnehmen.[416]

---

412 SCHWEIZER, europäisches Recht, 38. Bei den bilateralen Abkommen I und II handelt es sich grundsätzlich um klassische völkerrechtliche Verträge, welche auf eine parallele Rechtslage abzielen, jedoch keine Integration in den EU-*Acquis* vorsehen. Die Ausnahmen davon sind das Luftverkehrsabkommen sowie Schengen/Dublin. Siehe dazu PIRKER/EPINEY, 41.

413 BUNDESRAT, Botschaft Bilaterale II, 6179. Zur Abgrenzung der Schengener Zusammenarbeit von den anderen polizeilichen Instrumenten Interpol, Europol sowie den bilateralen Polizeikooperationsabkommen siehe BUNDESRAT, Botschaft Bilaterale II, 6093 ff.; BREITENMOSER/DRÜCK, 360 ff.

414 Dänemark beteiligt sich auf völkerrechtlicher Ebene an Schengen und Dublin, weshalb ein separates Abkommen abgeschlossen werden musste. Bei den anderen assoziierten Staaten handelte es sich um Norwegen und Island. Später kam auch Liechtenstein dazu.

415 BUNDESRAT, Botschaft Bilaterale II, 6121 f.

416 Die Komitologieausschüsse bestehen grundsätzlich aus VertreterInnen der Mitgliedstaaten. Ihnen kommt bei der Erarbeitung von Durchführungsmassnahmen eine beratende resp. kontrollierende Funktion zu. Fallen diese in den Schengen-Besitzstand kann sich die

Die schweizerische Assoziierung an Schengen besteht also aus sechs und diejenige an Dublin aus vier Verträgen. Grundsätzlich ist die Assoziierung der Schweiz an Schengen und Dublin derjenigen von Norwegen und Island nachgebildet.[417] Dennoch enthält die schweizerische Assoziierung einige Besonderheiten.[418]

Mit dem SAA verpflichtete sich die Schweiz den gesamten zum damaligen Zeitpunkt vorhandenen Schengen-Rechtsbestand zu übernehmen.[419] Gemäss dem DAA war die Übernahme hingegen auf ausgewählte Bereiche des EU-Asylrechts beschränkt. Dabei handelte es sich um vier Rechtsakte: Die Dublin-II-VO, die Verordnung (EG) Nr. 2725/2000 (altEurodac-VO) sowie die jeweiligen Durchführungsbestimmungen.[420] Daraus folgt, dass die Schweiz im Asylbereich materiellrechtlich nicht an EU-Recht gebunden ist, da die Richtlinien des GEAS – wie oben bereits erläutert – nicht Teil des Dublin-Systems sind.[421]

3.3. Übernahme und Umsetzung von Weiterentwicklungen des Schengen/Dublin-Besitzstands

Die Schengen/Dublin-Assoziierung der Schweiz sieht eine dynamische Übernahmeverpflichtung vor.[422] Die Schweiz hat demnach die jeweiligen Weiterentwicklungen von dem im Zeitpunkt der Unterzeichnung vorhandenen Schengen/Dublin-Besitzstand zu übernehmen und ggf. ins nationale Recht umzusetzen. Ob die Schweiz den Inhalt einer Weiterentwicklung akzeptiert

Schweiz ebenfalls daran beteiligen. Bei Dublin kann die Schweiz lediglich indirekt Einfluss nehmen (Art. 2 Abs. 6 DAA). Siehe zum Ganzen Oesch/Neier m.w.H.

417 Vgl. dazu Epiney, Schengen, Dublin, 304 ff.

418 So ist bspw. die Umsetzungsfrist von zwei Jahren für die Schweiz deutlich höher als diejenige von Island mit maximal vier Wochen und Norwegen mit maximal sechs Wochen. Vgl. dazu Bundesrat, Botschaft Bilaterale II, 6001 f.

419 Vgl. dazu Art. 2 Abs. 1 und 2 SAA.

420 Vgl. dazu Art. 1 Abs. 1 DAA; Tobler, Homogenität, 214. Gemäss Art. 1 Abs. 4 DAA sind zudem die einschlägigen Bestimmungen der Datenschutzrichtlinie von der Schweiz entsprechend umzusetzen und anzuwenden.

421 Progin-Theuerkauf/Egbuna-Joss, 186 f. Siehe zu einer Bewertung des Dublin-Systems vor dessen Einführung in der Schweiz Bolz.

422 Tobler, IT-Agentur, 2. Andere bilaterale Abkommen zwischen der Schweiz und der EU sind hinsichtlich der (allfälligen) Übernahme von EU-Recht anders ausgestaltet. So kann sich z.B. die Übernahme von EU-Recht auf im Zeitpunkt der Vertragsunterzeichnung geltendes Recht beschränken. Siehe dazu Epiney/Pirker, 45 ff. m.w.H. Vgl. dazu auch Epiney/Metz/Pirker, 182 ff.

und eine Umsetzung im innerstaatlichen Recht stattfindet, entscheidet sie jedoch autonom.[423]

Eine Weiterentwicklung des Schengen/Dublin-Besitzstands kann einerseits darin bestehen, dass ein in den Anhängen A und B des SAA resp. in Art. 1 Abs. 1 DAA aufgeführter Rechtsakt ergänzt oder verändert wird. Andererseits wird auch ein auf Grundlage eines dieser aufgeführten Rechtsakte neu geschaffener Rechtsakt als Weiterentwicklung verstanden. Ausschlaggebend sind somit die Inhalte des Besitzstands.[424] Während der Besitzstand von Schengen mittlerweile kaum zu überblicken ist, ist derjenige von Dublin übersichtlicher.[425]

Die Kommission entscheidet in der Regel schon im Entwurfsstadium eines neuen EU-Rechtsaktes über eine allfällige Schengen- resp. Dublin-Relevanz. Häufig wird dabei auf die Rechtsgrundlage des Aktes abgestellt. Stellt ein neu erlassener EU-Rechtsakt eine Schengen/Dublin-Weiterentwicklung dar, ist dieser entsprechend zu kennzeichnen.[426] Die Einflussnahme der Schweiz bezüglich der Frage, ob ein Rechtsakt eine Weiterentwicklung des Schengen/Dublin-Besitzstands darstellt, ist sehr begrenzt. Sie kann zwar versuchen, ihre Ansicht im Rahmen ihrer Beteiligungsrechte vorzubringen. Letztlich obliegt der Entscheid jedoch der EU.[427]

Wird ein neuer Rechtsakt oder eine Massnahme auf EU-Ebene angenommen, welcher resp. welche zum Schengen/Dublin-Besitzstand zählt, notifiziert der Rat oder die Kommission diesen resp. diese unverzüglich der Schweiz. Die Schweiz hat sich in der Folge dahingehend zu äussern, ob sie den Inhalt des Rechtsakts resp. der Massnahme akzeptiert und sie diesen in ihre innerstaatliche Rechtsordnung übernimmt. Soweit der betroffene Rechtsakt rechtlich

423 Art. 2 Abs. 3 und Art. 7 Abs. 2 Bst. a SAA; Art. 1 Abs. 3 und Art. 4 Abs. 2 DAA. Vgl. dazu auch Breitenmoser/Jutzeler, 30; Stämpfli, 71; Gruber, 488 ff.

424 Bundesrat, Botschaft Bilaterale II, 6071; Oesch, bilaterale Abkommen, 644; Good, 56 ff. m.w.H.

425 In der Systematischen Rechtssammlung des Bundes wird lediglich der Notenaustausch von Weiterentwicklungen des Schengen/Dublin-Besitzstands aufgeführt. Diese Publikationspraxis kann einen Überblick über das geltende Recht erschweren. Vgl. dazu Good, 172 ff.; Wüger, 72 ff.; Schweizer, wirksame Beschwerde, 46 ff.; Mohler, Herausforderung, 5 ff. Ein im Internet aufgeführtes Verzeichnis verschafft jedoch einen Überblick über die jeweiligen Weiterentwicklungen, wobei der relevante EU-Rechtsakt anhand der Verlinkung auf die Fundstelle auf EUR-lex aufgefunden werden kann. Vgl. dazu <https://www.bj.admin.ch/bj/de/home/sicherheit/schengen-dublin/rechtsgrundlagen.html>, zuletzt besucht am 07.03.2025.

426 So wird jeweils in den Erwägungsgründen eines Rechtsaktes auf die Schengen/Dublin-Relevanz hingewiesen. Siehe dazu z.B. betreffend die Schweiz ErwG. 77 IOP-Polizei-VO.

427 Tobler, Homogenität, 214 f.; Good, 74.

verbindlicher Natur ist, stellt diese als Antwortnote bekannte Mitteilung der Schweiz zusammen mit der Notifizierung des Rates resp. der Kommission einen Notenaustausch dar, welcher aus schweizerischer Perspektive als völkerrechtlicher Vertrag zu qualifizieren ist.[428] Der ursprünglich europarechtliche Rechtsakt wird dadurch zu einem völkerrechtlichen Vertrag.[429]

Die Übernahme einer Weiterentwicklung durch die Schweiz muss von der allfällig notwendigen Umsetzung derselben im nationalen Recht unterschieden werden. Eine innerstaatliche Umsetzung ist vorzunehmen, sofern die Weiterentwicklung nicht direkt anwendbar ist.[430] Direkt anwendbare Normen, welche die Rechtsstellung von Personen unmittelbar regeln, können von den rechtsanwendenden Behörden unmittelbar angewendet werden. Nicht direkt anwendbare Normen bedürfen hingegen einer Konkretisierung im nationalen Recht. Die innerstaatliche Umsetzung kann entweder auf Gesetzesstufe oder unterhalb der Stufe des formellen Gesetzesrechts erfolgen.[431]

Im EU-Recht kann die Klassifizierung eines Rechtsakts als Verordnung oder Richtlinie eine Hilfe bei der Beurteilung darstellen, ob eine Norm direkt anwendbar ist oder nicht. Die Richtlinie bezweckt eine Rechtsharmonisierung, welche Raum für gewisse Unterschiede lässt. Sie richtet sich an die Mitgliedstaaten und ist nicht direkt anwendbar und nur hinsichtlich des verfolgten Ziels verbindlich. Die Verordnung hingegen strebt eine Rechtsvereinheitlichung an, ist an alle Personen in der EU sowie die Mitgliedstaaten gerichtet und direkt anwendbar. Da mit der Assoziierung der Schweiz an Schengen und Dublin eine parallele Rechtsordnung angestrebt wird, gilt diese Europarechtsdogmatik auch für die Schweiz, es sei denn, dass gegenteilige Absprachen getroffen worden sind.[432]

---

428 Die Notifizierung durch die Schweiz folgt unterschiedlichen Modellen. Siehe dazu GRUBER, 496 ff. Siehe zur innerstaatlichen Abschlusskompetenz von solchen Verträgen zudem BUNDESRAT, Botschaft Bilaterale II, 6131.

429 Siehe zum Ganzen Art. 7 SAA; Art. 4 DAA; BUNDESRAT, Botschaft Dublin-III-VO/Eurodac-VO, 2683 f.; BUNDESRAT, Botschaft SIS 2007, 8599 f.; GOOD, 167 ff. m.w.H.

430 BUNDESRAT, Botschaft Bilaterale II, 6132 f.; CORNU, 234 ff. Siehe zum zweistufigen Übernahmeverfahren gemäss dem SAA GRUBER, 491 ff.

431 Bezüglich der Geltung von Völkerrecht folgt die Schweiz dem monistischen System. Demnach erlangt das Völkerrecht unmittelbar innerstaatliche Geltung und stellt einen Teil der nationalen Rechtsordnung dar. Siehe zum Ganzen BUNDESRAT, Botschaft Bilaterale II, 6132 f. m.w.H.

432 GOOD, 193 ff.; STÄMPFLI, 35 f.

3.4. Beteiligungsrechte der Schweiz

Im Vergleich zu den Bilateralen I wurden der Schweiz im Bereich von Schengen und Dublin mehr Mitwirkungsmöglichkeiten zugestanden. So kann sich die Schweiz im Rahmen ihrer Beteiligungsrechte in verschiedenen Ausschüssen zu neuem Schengen/Dublin-Recht einbringen.[433] Das Stimmrecht bei der Verabschiedung neuer Schengen/Dublin-Rechtsakte und Massnahmen ist jedoch den Mitgliedstaaten vorbehalten. Diese Tatsache wird insoweit relativiert, als normalerweise versucht wird, einen Konsens zu erreichen.[434]

Die Schweiz ist zudem berechtigt, bezüglich der Auslegung von Schengen/Dublin-Besitzstand im Rahmen von entsprechenden Vorabentscheidungsverfahren beim EuGH Schriftsätze einzureichen oder schriftliche Erklärungen abzugeben.[435]

3.5. Einheitliche Anwendung und Auslegung des Schengen/Dublin-Besitzstands

Das Ziel der Schengen/Dublin-Assoziierung ist eine möglichst einheitliche Anwendung und Auslegung des Schengen/Dublin-Besitzstands. Der Gemischte Ausschuss verfolgt deshalb die Entwicklung der einschlägigen Rechtsprechung des EuGH sowie der zuständigen schweizerischen Gerichte.[436] Es ist demnach eine gegenseitige Berücksichtigung vorgesehen. Eine direkte, ausdrückliche Übernahmeverpflichtung der Rechtsprechung des EuGH durch die Schweiz ist in den Schengen/Dublin-Assoziierungsabkommen hingegen nicht vorgesehen.[437]

---

433 Vgl. dazu im Einzelnen Art. 2 DAA; Art. 6 SAA. Bei Schengen kann sich die Schweiz zudem als Beobachter an der Arbeit der Komitologieausschüsse beteiligen. Die Einzelheiten dazu sind in der Komitologievereinbarung geregelt. Bei Dublin hingegen ist keine formelle Beteiligung an den Komitologieausschüssen vorgesehen. Vgl. dazu OESCH, bilaterale Abkommen, 643 f. Siehe zum Ganzen auch BUNDESRAT, Botschaft Bilaterale II, 6129 f.; GOOD, 111 ff. m.w.H. Siehe zur Komitologie im Bereich Schengen und Dublin zudem GUTZWILLER, 247 ff. Siehe zur Aufgabenaufteilung in der Verwaltung des Bundes sowie der Kantone hinsichtlich der Partizipationsrechte der Schweiz bei Schengen GRUBER, 484 ff.

434 BUNDESRAT, Botschaft Bilaterale II, 5968 f., 6129, 6178; PROGIN-THEUERKAUF/EGBUNA-JOSS, 187 ff. m.w.H.; GOOD, 129 ff. m.w.H. Vgl. dazu auch GRUBER, 481 ff.; GUTZWILLER, 257.

435 Art. 5 Abs. 2 DAA; Art. 8 Abs. 2 SAA. Eine Liste der Vorabentscheidungsverfahren, welche der Schweiz notifiziert worden sind, ist abrufbar unter <https://www.bj.admin.ch/bj/de/home/sicherheit/schengen-dublin/uebersichten.html>, zuletzt besucht am 07.03.2025. Siehe auch OESCH, EuGH, Rz. 85 ff.

436 Art. 8 Abs. 1 SAA; Art. 5 Abs. 1 DAA.

437 Obwohl keine explizite Pflicht zur Berücksichtigung der Rechtsprechung des EuGH vorgesehen ist, sprechen verschiedene Gründe dafür, dass die Auslegung von Schengen/Dublin

Die schweizerischen Behörden und Gerichte bleiben also hinsichtlich der Anwendung und Auslegung des Schengen/Dublin-Besitzstands kompetent. Es ist jedoch im Interesse von allen Beteiligten, wenn die Regeln von Schengen und Dublin möglichst gleich angewendet und ausgelegt werden.[438]

3.6. Beendigungsmechanismus

Der Schengen/Dublin-Besitzstand besteht aus einem Geflecht von Rechtsakten und Massnahmen, welche häufig eng verbunden sind. Die Weiterentwicklungen sind deshalb von allen Schengen-Staaten zu übernehmen und gleichzeitig anzuwenden. Die Schengen/Dublin-Assoziierung sieht einen Beendigungsmechanismus vor, welche die Anwendung dieses Prinzips garantieren soll.[439]

Im SAA sowie im DAA wird geregelt, in welchen Situationen der Beendigungsmechanismus eingeleitet wird. Für den Fall, dass die Schweiz einen neuen Schengen/Dublin-Rechtsakt nicht akzeptieren will, wird das SAA als beendet angesehen resp. gilt das DAA als ausgesetzt, es sei denn der Gemischte Ausschuss beschliesst im Rahmen einer Frist von 90 Tagen etwas anderes. Läuft die Frist unbenutzt ab, so gelten die Abkommen nach Ablauf einer weiteren Frist von 90 Tagen als beendet.[440]

Davon abgesehen können auch wesentliche Abweichungen in der Rechtsprechung zwischen dem EuGH sowie den schweizerischen Gerichten betreffend die Anwendung des Schengen/Dublin-Besitzstands zum Einleiten des Beendigungsmechanismus führen. Ist der Gemischte Ausschuss nämlich innerhalb von zwei Monaten nach der Kenntnisnahme einer solchen wesentlichen Abweichung nicht in der Lage, eine einheitliche Anwendung und Auslegung zu gewährleisten, versucht der Gemischte Ausschuss diesen Streit – sowie auch

Besitzstand in Konformität mit der (vergangenen wie auch zukünftigen) Rechtsprechung des EuGH erfolgen sollte: Beide Assoziierungsabkommen bezwecken die Schweiz umfassend in den Schengen/Dublin-Besitzstand zu integrieren. Zudem besteht die Pflicht zur Übernahme von EU-Recht im Zeitpunkt der Unterzeichnung sowie auch der zukünftigen Entwicklungen. Schliesslich ist auch vorgesehen, dass der Beendigungsmechanismus eingeleitet werden kann, sofern in der Schweiz eine wesentliche Abweichung der Rechtsprechung resp. der Auslegung vorliegt. Dies zeigt, dass die parallele Auslegung ein sehr wichtiges Ziel dieser beiden Abkommen ist. Siehe dazu PIRKER/EPINEY, 52; EPINEY/METZ/PIRKER, 175 ff. m.w.H.

438 CORNU, 241.

439 CORNU, 238 f.

440 Siehe dazu Art. 7 Abs. 4 SAA; Art. 4 Abs. 6 und 7 DAA.

bei Streitigkeiten betreffend die Anwendung (resp. Auslegung) des SAA und des DAA – beizulegen. Innert einer Frist von 90 Tagen, gerechnet ab dem Zeitpunkt der Annahme der Tagesordnung, kann im Gemischten Ausschuss die weitere Anwendung bzw. Geltung des Abkommens beschlossen werden. Kann der Streit auch nach einer weiteren Frist von 30 resp. 90 Tagen nicht beigelegt werden, so wird das SAA sechs Monate danach als beendet angesehen.[441]

Im SAA und im DAA ist zudem vorgesehen, dass diese Abkommen nur angewendet werden, sofern das jeweils andere Abkommen angewendet wird. Wird ein Abkommen gekündigt, teilt das andere jeweils das gleiche Schicksal.[442]

4. Schengener Informationssystem

4.1. Entstehung

Das SIS wurde als Ausgleichsmassnahme im Zuge des Abbaus der Grenzkontrollen mit der Unterzeichnung des SDÜ im Jahr 1990 eingeführt und 1995 in Betrieb genommen. Es handelt sich um eine Datenbank, welche verschiedene Personen- und Sachfahndungen enthält.[443] Als gemeinsames Fahndungssystem stellt das SIS ein wichtiges Instrument der Schengener Polizeizusammenarbeit dar. Hautsächlich kann damit nach Straftätern gefahndet werden, welche nach der Festnahme ausgeliefert werden sollen.[444]

Das SIS war ursprünglich für maximal 18 Staaten ausgelegt. Da immer mehr Staaten in die EU aufgenommen wurden, kam das Informationssystem in technischer Hinsicht an seine Grenzen. Deswegen wurde eine neue Generation – das SIS II – geplant, welches im Jahr 2007 hätte in Betrieb genommen werden sollen.[445] Da sich die Einführung des SIS II aufgrund technischer Schwierigkei-

441 Siehe dazu Art. 9 Abs. 2 sowie Art. 10 SAA; Art. 6 Abs. 2 sowie Art. 7 DAA. Siehe zum Ganzen auch Epiney/Meier/Theuerkauf, 39; Bundesrat, Botschaft Bilaterale II, 6125 f.; Tobler, Homogenität, 214 f. Betreffend mangelhafter Übernahme siehe Good, 181 ff. Die Schweiz kann die Übernahme einer Weiterentwicklung verweigern, wenn diese die Schweiz – in Abänderung zu Art. 51 SDÜ – zur Leistung von Rechtshilfe für Durchsuchungen und Beschlagnahmen bei Abgabehinterziehung im Bereich der direkten Steuern verpflichten würde. Dies ist in Art. 7 Abs. 5 SAA vorgesehen. Siehe dazu Gruber, 491.

442 Art. 14 DAA; Art. 16 Abs. 2 DAA; Art. 15 Abs. 4 SAA; Art. 17 Abs. 2 SAA.

443 Siehe dazu Art. 92 ff. SDÜ; Art. 2 Abs. 1 SIS-Polizei-VO; Art. 2 Abs. 1 SIS-Grenze-VO; Art. 1 SIS-Rückkehr-VO; Stämpfli, 45; Progin-Theuerkauf/Zoeteweij-Turhan/Turhan, 9; Epiney, Herausforderungen, 17 ff.; Riepl, 236.

444 Bundesrat, Botschaft Bilaterale II, 6082.

445 Bundesrat, Botschaft Bilaterale II, 6081; Bundesrat, Botschaft SIS 2007, 8593.

ten verzögerte, wurde eine Übergangslösung – das SISone4all – entwickelt, um die Grenzöffnung der neuen Mitgliedstaaten per Ende 2007 zu ermöglichen.[446] Letztlich konnte das SIS II am 9. April 2013 in Betrieb genommen werden.[447]

Aufgrund der Evaluierung des SIS II im Jahr 2016 durch die Kommission wurde zwar der grosse Erfolg der Datenbank – insbesondere auch aufgrund der hohen Nutzung durch die beteiligten Staaten – ersichtlich. Es zeigte sich jedoch auch, dass Verbesserungen hinsichtlich der Wirksamkeit sowie der Effizienz des Systems nötig waren.[448] Daher wurden drei neue Rechtsakte erarbeitet, welche das System weiterentwickeln und stärken sollten. Diese Rechtsakte beziehen sich auf die Bereiche Grenzmanagement, polizeiliche und justizielle Zusammenarbeit in Strafsachen sowie Rückführung illegaler Drittstaatsangehöriger[449]. Während die VO 2018/1860 (SIS-Rückkehr-VO) und die VO 2018/1861 (SIS-Grenze-VO) die Anwendung des SIS im Bereich der Migrationskontrolle regeln, stellt die VO 2018/1862 (SIS-Polizei-VO) die rechtliche Grundlage für die Nutzung der Datenbank für die Strafverfolgung dar.[450] Diese drei Verordnungen sind zwar bereits Ende 2018 in Kraft getreten. Die Inbetriebnahme der Weiterentwicklungen des Systems erfolgte jedoch erst per 7. März 2023.[451]

Seit dieser Änderung der gesetzlichen Grundlagen wird das Informationssystem nicht mehr spezifisch SIS II genannt. Im Folgenden wird deshalb die Bezeichnung SIS verwendet. Der Begriff SIS II kommt nur zur Anwendung, sofern genau diese Version des SIS gemeint ist.

Das SIS ist gemischter Natur, weil es sowohl im Bereich der Immigration (vor allem im Bereich von Visa und Aufenthaltsbewilligungen) als auch im Bereich der Strafverfolgung (Überprüfung von Personen an den Aussengrenzen oder im Hoheitsgebiet durch die Polizei-, Zoll- und Grenzkontrollbehörden) eingesetzt wird.[452]

---

446 Bundesrat, Botschaft SIS 2007, 8593; Good, 87; Stämpfli, 60 ff.

447 Progin-Theuerkauf/Zoeteweij-Turhan/Turhan, 11 ff. Siehe Parkin zu einer kritischen Beurteilung der Entstehung des SIS II.

448 EDSB, SIS recast, 5. Siehe zur Evaluierung Europäische Kommission, Bericht Evaluierung SIS II.

449 Als Drittstaatsangehörige gelten Personen, welche keine UnionsbürgerInnen sind. Davon ausgenommen sind Personen, welche aufgrund eines entsprechenden Abkommens ebenfalls über ein gleichwertiges Recht auf Freizügigkeit verfügen. Siehe dazu Art. 3 Ziff. 4 SIS-Grenze-VO.

450 Cassani, et al., 452 f. Siehe zur Entwicklung des rechtlichen Rahmens des SIS Mitsilegas/Vavoula, 491 ff.

451 Siehe dazu Durchführungsbeschluss 2023/201.

452 Vavoula, Right to Private Life, 232 f.; Vavoula, EU immigration databases, 218 ff.

4.2. Betrieb und Aufsicht

Das SIS besteht aus einem zentralen System. Dieses enthält die Datenbank enthaltene technische Unterstützungseinheit sowie eine einheitliche nationale Schnittstelle. Daneben existiert in den Schengen-Staaten jeweils ein nationales System, welches aus den nationalen Datensystemen besteht und die wiederum mit dem zentralen SIS kommunizieren. Über die nationalen Systeme, für welche die jeweiligen Schengen-Staaten für die Errichtung, Wartung, Weiterentwicklung, etc. zuständig sind, werden die Ausschreibungen an das SIS übermittelt. Ebenfalls erfolgt die Eingabe, die Aktualisierung, die Löschung sowie die Abfrage von SIS-Daten über das jeweilige nationale System. Dieses kann eine nationale Kopie umfassen, welche eine vollständige oder eine Teilkopie der SIS-Datenbank enthält.[453] Des Weiteren ermöglicht eine Kommunikationsinfrastruktur u.a. den Datenaustausch.[454]

Für den Betrieb des zentralen SIS ist die Europäische Agentur für das Betriebsmanagement von IT-Grosssystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA)[455] zuständig.[456]

Abgesehen von diesem eigentlichen SIS-Netzwerk bezeichnen die Schengen-Staaten jeweils eine N.SIS-Stelle sowie ein SIRENE-Büro. Während erstere u.a. für den einwandfreien Betrieb des nationalen Systems verantwortlich ist, gewährleistet letzteres den Austausch sowie die Verfügbarkeit aller Zusatzinformationen.[457] Der SIS-Datenbank kann nämlich lediglich entnommen werden, ob ein entsprechender Eintrag vorhanden ist. Weitere Angaben müssen beim zuständigen SIRENE-Büro eingefordert werden. Die SIRENE-Büros verfügen

---

453 Im SIS der ersten Generation sowie im SISone4all war noch keine Möglichkeit einer nationalen Kopie vorgesehen. Damals waren die nationalen Systeme direkt mit der zentralen Datenbank verknüpft. Es erscheint fraglich, weshalb die Möglichkeit der nationalen Kopie eingeführt wurde. Es sind weder technische Vorteile ersichtlich, noch wird dadurch das Verfahren vereinfacht. Auch ergibt sich dadurch keine bessere Qualität der Datensätze. Vielmehr muss stets eine Aktualisierung vorgenommen werden, um die Korrektheit der Daten sicherzustellen. Eine Vervielfältigung der SIS-Daten sollte so klein wie möglich gehalten werden. Es besteht zudem die Gefahr, dass nicht befugte Behörden durch die nationalen Kopien Einsicht in SIS-Daten erhalten. Siehe dazu Stämpfli, 301 ff.

454 Siehe zu den Einzelheiten Art. 4 und 6 SIS-Grenze-VO; Art. 4 und 6 SIS-Polizei-VO.

455 Die IT-Agentur eu-LISA wurde im Jahr 2012 errichtet und ist insbesondere für die Gewährleistung des Betriebs der Informationssysteme zuständig. Sie trägt die Verantwortung für die Sicherheit der Systeme sowie der darin gespeicherten Daten. Vgl. dazu Progin-Theuerkauf/Zoeteweij-Turhan/Turhan, 8.

456 Art. 15 Abs. 1 SIS-Polizei-VO; Art. 15 Abs. 1 SIS-Grenze-VO.

457 Art. 7 Abs. 1 und 2 SIS-Grenze-VO; Art. 7 Abs. 1 und 2 SIS-Polizei-VO. Siehe zur Definition der Zusatzinformationen Art. 3 Ziff. 2 SIS-Grenze-VO.

über einen 24-Stunden-Bereitschaftsdienst.[458] Der Austausch von Zusatzinformationen soll es erlauben, bei einem Treffer[459] im SIS, die erforderlichen Massnahmen zu ergreifen.[460] Das SIRENE-Büro fungiert somit als Kontaktstelle für andere SIRENE-Büros, wobei die Kommunikation über ein verschlüsseltes virtuelles Netz erfolgt.[461]

Das SIS untersteht einer Aufsicht. So hat jeder Schengen-Staat eine nationale Aufsichtsbehörde zu benennen, welche die Datenverarbeitung von SIS-Daten im jeweiligen Hoheitsgebiet überwacht. Über die Verwaltungsbehörde eu-LISA übt der Europäische Datenschutzbeauftragte (EDSB)[462] die Aufsicht aus. Zwecks koordinierter Überwachung arbeiten die nationalen Aufsichtsbehörden und der EDSB zusammen.[463]

4.3. Beteiligung der Schweiz

Die Schweiz beteiligt sich aufgrund der Schengen-Assoziierung am SIS. Der effektive Anschluss erfolgte im Jahr 2008.[464] Bei der Unterzeichnung des SAA ging die Schweiz noch davon aus, dass sie sich direkt am SIS II beteiligen würde. Da sich die technische Umsetzung des SIS II jedoch verzögerte, entschied der Bundesrat, sich vorerst der Übergangslösung SISone4all anzuschliessen, bis das SIS II einsatzbereit war.[465]

Die Schweiz betreibt eine nationale Kopie der im zentralen System der EU gespeicherten Daten.[466] Der Zugriff auf dieses sog. N-SIS erfolgt via verschiedene nationale Informationssysteme.[467] Soweit erforderlich dürfen Daten aus

458 GOOD, 88; STÄMPFLI, 46 ff. Siehe dazu auch Art. 8 SIS-Grenze-VO und Art. 8 SIS-Polizei-VO.
459 Zur Definition siehe Art. 3 Ziff. 8 SIS-Grenze-VO; Art. 3 Ziff. 7 SIS-Polizei-VO.
460 Art. 7 Abs. 2 SIS-Grenze-VO; Art. 7 Abs. 2 SIS-Polizei-VO.
461 Anhang Ziff. 1.10.3. SIRENE-Handbuch.
462 Der EDSB ist für die Überwachung der Datenbearbeitungen durch die Kommission und andere EU-Institutionen zuständig. Des Weiteren kommt dem EDSB eine Beratungsfunktion gegenüber der Kommission, dem Rat sowie dem Parlament hinsichtlich neuer Gesetzgebung zu, welche den Datenschutz betrifft. Eine weitere Aufgabe des EDSB besteht in der Koordination mit anderen Datenschutz-Behörden, insbesondere mit nationalen Behörden, um die Einheitlichkeit des Datenschutzes zu gewährleisten. Siehe dazu HUSTINX, 16.
463 Siehe dazu Art. 55-57 SIS-Grenze-VO; Art. 69-71 SIS-Polizei-VO.
464 STÄMPFLI, 74 ff. m.w.H.
465 BUNDESRAT, Botschaft SIS 2007, 8593 ff.; GOOD, 87.
466 Vgl. dazu Art. 4 Abs. 1 N-SIS-Verordnung.
467 Vgl. dazu Art. 4 Abs. 5 N-SIS-Verordnung.

diesen Systemen automatisch in das N-SIS überführt werden. Die Bearbeitung von SIS-Daten erfolgt ebenfalls über das N-SIS.[468]

Ergibt eine Abfrage einen Treffer, so kontaktiert die abfragende Behörde das SIRENE-Büro. Das SIRENE-Büro holt auf Ersuchen der abfragenden Behörde beim SIRENE-Büro des ausschreibenden Staates Zusatzinformationen ein, welche der abfragenden Behörde mitgeteilt werden. Anschliessend berät das SIRENE-Büro die abfragende Behörde hinsichtlich der zu treffenden Massnahmen.[469] Erfolgt ein Treffer einer von der Schweiz vorgenommenen Ausschreibung im Ausland, so kontaktiert das SIRENE-Büro der Schweiz die ausschreibende Behörde und bespricht mit dieser die zu treffenden Massnahmen. Das SIRENE-Büro kann bei Bedarf von der ausschreibenden Behörde auch Zusatzinformationen einfordern, welche dem SIRENE-Büro desjenigen Schengen-Staates zur Verfügung gestellt wird, in dem der Treffer erfolgt ist.[470]

In der Schweiz wird das SIRENE-Büro vom Bundesamt für Polizei (fedpol) geführt. Abgesehen davon betreibt fedpol unter Mitwirkung anderer Behörden des Bundes resp. der Kantone auch das nationale System N-SIS und trägt dafür die Verantwortung.[471]

Die Aufsicht über die Datenverarbeitung von SIS-Daten in der Schweiz wird insbesondere vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) wahrgenommen.[472] Dieser koordiniert seine Aufsichtstätigkeit mit den kantonalen Datenschutzbehörden. Für diese Zusammenarbeit wurde die Koordinationsgruppe Schengen geschaffen. In dieser Gruppe werden Informationen ausgetauscht, die Aufsicht koordiniert sowie gegenseitige Unterstützungsleistungen erbracht. Der EDÖB arbeitet abgesehen davon mit dem EDSB zusammen.[473]

Für die Umsetzung der SIS-Grenze-VO, der SIS-Polizei-VO sowie der SIS-Rückkehr-VO mussten in der Schweiz im nationalen Recht einige Anpassungen auf Gesetzes- sowie auch auf Verordnungsstufe vorgenommen werden.[474]

---

468 Vgl. dazu Art. 4 N-SIS-Verordnung; Art. 16 Abs. 7 und 8 BPI; Stämpfli, 46.

469 Art. 18 N-SIS-Verordnung.

470 Art. 19 N-SIS-Verordnung.

471 Art. 3 und Art. 8 N-SIS-Verordnung; Art. 16 BPI.

472 Siehe zur Funktion und zu den Tätigkeiten des EDÖB im Allgemeinen Art. 43 ff. DSG.

473 Art. 55 N-SIS-Verordnung. Vgl. dazu auch Gloor Scheidegger, 135 f.

474 Vgl. zu den Einzelheiten Bundesrat, Botschaft SIS 2020; SEM, Erläuternder Bericht SIS Recast. Siehe dazu auch Bundesbeschluss vom 18. Dezember 2020.

4.4. Gespeicherte Daten

4.4.1. Ausschreibungskategorien

Die SIS-Datenbank enthält Ausschreibungen von Personen sowie von bestimmten Sachen.[475] Diese Ausschreibungen werden von den Schengen-Staaten in das SIS eingegeben.[476] Grundsätzlich ist der ausschreibende Staat für die Richtigkeit sowie die Aktualität der in der SIS-Datenbank gespeicherten Daten sowie für die Rechtmässigkeit der Eingabe in die Datenbank verantwortlich. Nur dieser Staat ist jeweils berechtigt, eine Änderung, Ergänzung, Berichtigung, Aktualisierung oder Löschung der gespeicherten Daten vorzunehmen.[477]

Bevor eine Ausschreibung in das SIS aufgenommen oder eine Verlängerung vorgenommen wird, hat der ausschreibende Schengen-Staat stets eine Verhältnismässigkeitsprüfung vorzunehmen. Bei Personen oder Sachen, welche im Zusammenhang mit terroristischen Straftaten stehen, wird grundsätzlich davon ausgegangen, dass die Verhältnismässigkeit vorliegt.[478] Ausschreibungen im SIS können von den Schengen-Staaten zudem – unabhängig von der Art der Ausschreibung – miteinander verknüpft werden.[479]

Da die Ausschreibungen von Sachen für die Fragestellung der vorliegenden Untersuchung nicht relevant sind, beschränken sich die nachfolgenden Ausführungen auf die Ausschreibungen von Personen. Diese lassen sich in verschiedene Kategorien unterteilen. Bezüglich jeder Ausschreibungskategorie müssen jeweils bestimmte Voraussetzungen vorliegen.[480] So können Personen zur Einreise- oder Aufenthaltsverweigerung[481], zum Zwecke der Übergabe- oder Ausliefe-

475 Art. 1 SIS-Rückkehr-VO; Art. 2 Abs. 1 SIS-Grenze-VO; Art. 2 Abs. 1 SIS-Polizei-VO.

476 Europol kann den Schengen-Staaten Drittstaatsangehörige zur sog. Informationsausschreibung vorschlagen. Siehe dazu Art. 4 Abs. 1 Bst. t VO 2016/794; Art. 37a f. SIS-Polizei-VO. Bis anhin wurde Europol nur Lesezugriff auf die Ausschreibungen im SIS gewährt. Siehe dazu Mitsilegas/Vavoula, 502. In der Schweiz sind verschiedene Behörden zur Erfüllung ihrer Aufgaben berechtigt, eine Ausschreibung für die Verbreitung im SIS zu melden. Siehe dazu Art. 6 N-SIS-Verordnung.

477 Art. 59 Abs. 1 und 3 SIS-Polizei-VO; Art. 44 Abs. 1 und 3 SIS-Grenze-VO.

478 Art. 21 SIS-Grenze-VO; Art. 21 SIS-Polizei-VO.

479 Art. 48 SIS-Grenze-VO; Art. 63 SIS-Polizei-VO; Bundesrat, Botschaft SIS 2020, 3503.

480 Bei einigen Ausschreibungskategorien muss z.B. eine Entscheidung eines nationalen Gerichts resp. einer Verwaltungsbehörde vorliegen. Siehe dazu z.B. Art. 24 Abs. 1 SIS-Grenze-VO (Ausschreibungen zur Einreise- oder Aufenthaltsverweigerung); Art. 32 Abs. 4 SIS-Polizei-VO (Ausschreibungen von schutzbedürftigen Personen, die am Reisen gehindert werden müssen); Art. 3 Abs. 1 SIS-Rückkehr-VO (Ausschreibungen zur Rückkehr).

481 Siehe zu den Einzelheiten Art. 20 ff. SIS-Grenze-VO.

rungshaft[482] oder für verdeckte oder gezielte Kontrollen resp. Ermittlungsanfragen[483] ausgeschrieben werden. Des Weiteren können Personen, welche vermisst[484] oder die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht[485] werden, in der Datenbank zur Ausschreibung aufgenommen werden.

Mit der SIS-Polizei-VO sowie der SIS-Rückkehr-VO sind zudem weitere Ausschreibungskategorien geschaffen worden. So sind nun auch Ausschreibungen von schutzbedürftigen Personen vorgesehen, welche am Reisen gehindert werden müssen. In diese Kategorie fallen bspw. Kinder resp. Jugendliche, welche in bewaffnete Gruppen rekrutiert wurden oder potenzielle Opfer von Menschenhandel darstellen.[486] Zudem wurden auch Ausschreibungen von unbekannten gesuchten Personen zwecks Identifizierung nach Massgabe des nationalen Rechts möglich. Bei solchen Ausschreibungen können vollständige oder unvollständige Fingerabdruck- oder Handflächenabdrücke, welche an Tatorten von terroristischen oder sonstigen schweren Straftaten vorgefunden wurden, in der Datenbank gespeichert werden, sofern diese mit hoher Wahrscheinlichkeit dem Täter zuzuordnen sind.[487] Ausserdem können Drittstaatsangehörige, gegen welche eine Rückkehrentscheidung ergangen ist, in der Datenbank ausgeschrieben werden.[488]

Im SIS waren Ende 2023 knapp 1,4 Millionen Personenausschreibungen gespeichert. Damit stellen die Personenausschreibungen rund 1,5 % aller im SIS gespeicherten Ausschreibungen dar. Die restlichen Ausschreibungen beziehen sich auf Sachen.[489] Im Vergleich mit Ende 2022 ist das ein Wachstum um 38 %. Es ist jedoch zu berücksichtigen, dass zwischenzeitlich neue Arten von Personenausschreibungen eingeführt wurden.[490]

4.4.2. Datenkategorien

Die Datenkategorien, welche im SIS gespeichert werden, wurden im Rahmen der SIS-Grenze-VO, der SIS-Polizei-VO sowie der SIS-Rückkehr-VO erneut

482 Siehe zu den Einzelheiten Art. 26 ff. SIS-Polizei-VO.

483 Diesbezüglich sind auch Sachfahndungsausschreibungen möglich. Siehe dazu Art. 36 f. SIS-Polizei-VO.

484 Siehe zu den Einzelheiten Art. 32 f. SIS-Polizei-VO.

485 Siehe zu den Einzelheiten Art. 34 f. SIS-Polizei-VO.

486 Siehe zu den Einzelheiten Art. 32 f. SIS-Polizei-VO.

487 Siehe zu den Einzelheiten Art. 40 f. SIS-Polizei-VO.

488 So z.B., wenn die Person bis zur Abschiebung in Haft genommen wird. Siehe dazu Art. 3 SIS-Rückkehr-VO.

489 EU-LISA, SIS report 2023, 13 ff.

490 EU-LISA, SIS report 2023, 18 m.w.H.

erweitert.[491] Es handelt sich mittlerweile um einen umfangreichen Katalog alphanumerischer und biometrischer Daten.[492]

Einige dieser Daten stellen den Mindestdatensatz dar, welcher für die Eingabe einer Ausschreibung erforderlich ist. Dieser Mindestdatensatz kann mit weiteren festgelegten Daten ergänzt werden. Grundsätzlich umfasst der Mindestdatensatz die Angabe des Nachnamens, des Geburtsdatums, des Ausschreibungsgrunds sowie die im Falle eines Treffers zu ergreifende Massnahme.[493] Gemäss der SIS-Grenze-VO sowie der SIS-Rückkehr-VO besteht der Mindestdatensatz noch aus weiteren Angaben.[494]

Davon – und von weiteren Angaben zur Person – abgesehen, kann bspw. in eine Personenausschreibung eingegeben werden, ob die betreffende Person bewaffnet, selbstmordgefährdet oder eine Gefahr für die öffentliche Sicherheit darstellt. Teilweise können auch besondere, objektive, unveränderliche körperliche Merkmale der betroffenen Person in das SIS eingegeben werden. Des Weiteren können Lichtbilder, Gesichtsbilder[495], daktyloskopische Daten[496] und teilweise auch DNA-Profile[497] erfasst werden.[498]

---

491 BUNDESRAT, Botschaft SIS 2020, 3490, 3497 f. Bereits im Vergleich mit dem SIS der ersten Generation enthielt das SIS II neue Datenkategorien bezüglich Personenausschreibungen. Siehe dazu BUNDESRAT, Botschaft Bilaterale II, 6081; BUNDESRAT, Botschaft SIS 2007, 8593.

492 Siehe zu den Einzelheiten der Daten, welche im SIS gespeichert werden können Art. 4 Abs. 1 SIS-Rückkehr-VO; Art. 20 Abs. 2 SIS-Grenze-VO; Art. 20 Abs. 2 SIS-Polizei-VO.

493 Davon ausgenommen ist die Ausschreibungskategorie gemäss Art. 40 SIS-Polizei-VO (Ausschreibungen zu unbekannten gesuchten Personen zwecks Identifizierung nach Massgabe des nationalen Rechts). Vgl. dazu Art. 22 Abs. 1 SIS-Polizei-VO.

494 Siehe dazu Art. 22 Abs. 1 SIS-Grenze-VO; Art. 4 Abs. 2 SIS-Rückkehr-VO.

495 Gemäss Art. 3 Ziff. 14 SIS-Polizei-VO handelt es sich bei einem Gesichtsbild um «*eine digitale Aufnahme des Gesichts, in ausreichender Bildauflösung und Qualität für den automatisierten biometrischen Abgleich*».

496 Darunter fallen Fingerabdrücke und Handflächenabdrücke. Siehe dazu Art. 3 Ziff. 13 SIS-Polizei-VO; Art. 3 Ziff. 14 SIS-Grenze-VO.

497 Gemäss Art. 3 Ziff. 15 SIS-Polizei-VO handelt es sich bei einem DNA-Profil um «*einen Buchstaben- beziehungsweise Zahlencode, der eine Reihe von Identifikationsmerkmalen des nichtcodierenden Teils einer analysierten menschlichen DNA-Probe, d.h. der speziellen Molekularstruktur an den verschiedenen DNA-Loci, abbildet*». Die DNA als zweistrangige Doppelhelix enthält sowohl codierende wie auch nicht codierende Abschnitte, wobei nur erstere die genetischen Informationen enthalten. Das DNA-Profil zeichnet sich durch eine hohe Einzigartigkeit aus, da nur eineiige Zwillinge über ein identisches DNA-Profil verfügen. Deshalb wird das DNA-Profil als ein sicheres und zuverlässiges Erkennungsmerkmal angesehen. Siehe dazu BLONSKI, 31 ff. m.w.H.

498 Siehe zu den Einzelheiten der Daten, welche im SIS gespeichert werden können Art. 4 Abs. 1 SIS-Rückkehr-VO; Art. 20 Abs. 2 SIS-Grenze-VO; Art. 20 Abs. 3 SIS-Polizei-VO.

Die im SIS gespeicherten Personenausschreibungen sollen grundsätzlich nicht länger als für den verfolgten Zweck erforderlich gespeichert werden. Die Schengen-Staaten haben deshalb die Erforderlichkeit der Beibehaltung der Ausschreibung in einem Zeitraum von einem, drei resp. fünf Jahren zu überprüfen. Nach Ablauf dieser Prüffrist ist die Ausschreibung automatisch zu löschen. Vorbehalten bleibt eine Verlängerung durch den ausschreibenden Schengen-Staat.[499] Die Löschung von Ausschreibungen ist zudem bei Vorliegen von bestimmten Ereignissen vorgesehen, so z.B., wenn die zuständige Behörde die Entscheidung, welche die Grundlage für die Ausschreibung darstellte, zurückgezogen oder für nichtig erklärt hat.[500]

4.5. Zugriffsberechtigung

Ähnlich wie bei den Ausschreibungs- sowie den Datenkategorien ist auch bei den Zugriffsberechtigungen auf SIS-Daten eine stetige Erweiterung zu beobachten. Anfänglich waren Zugriffsberechtigungen für nationale Behörden vorgesehen, welche in der Registrierung sowie der Kontrolle von Personen tätig waren. Später wurde der Zugriff auch den Visum- und Asylbehörden gewährt. Danach erhielten die nationalen Grenzkontroll-, die Migrations-, die Polizei-, Zoll-, Justiz- und Fahrzeugregisterbehörden sowie Europol[501] und die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust)[502] Zugriff auf die SIS-Daten.[503] Dadurch wurde der Kreis der Zugriffsberechtigten insoweit erweitert, als nicht mehr nur diejenigen Behörden zugriffsberechtigt sind, welche die aufgrund einer Ausschreibung zu ergreifenden Massnahmen auszuführen haben, sondern auch solche, welche die

499 Art. 39 SIS-Grenze-VO; Art. 53 f. SIS-Polizei-VO.

500 Siehe dazu im Allgemeinen Art. 55 SIS-Polizei-VO; Art. 40 SIS-Grenze-VO; Art. 14 SIS-Rückkehr-VO.

501 Bei Europol handelt es sich um die Strafverfolgungsbehörde der EU. Sie hilft bei der Abwehr sowie Untersuchung von bestimmten Straftaten, sofern mindestens zwei Mitgliedstaaten involviert sind. Siehe dazu FRA/Europarat/EDSB, Handbuch, 356 ff. m.w.H.

502 Seit 2018 stellt Eurojust eine Agentur dar, welche die Koordinierung sowie Zusammenarbeit zwischen den nationalen für die Ermittlung und Verfolgung von schwerer Kriminalität zuständigen Behörden unterstützt und verstärkt, sofern mindestens zwei Mitgliedstaaten involviert sind oder eine gemeinsame Verfolgung angezeigt erscheint. Siehe dazu Oesch, Schweiz-EU, N 273. Siehe für weitere Hinweise zu Eurojust auch FRA/Europarat/EDSB, Handbuch, 362 ff.

503 Vgl. dazu Art. 101 SDÜ; Art. 27 SIS-II-VO; Art. 40 ff. SIS-II-Beschluss; Art. 1 SIS-II-Kfz-VO. Siehe dazu auch Cassani, et al., 454 f.; Progin-Theuerkauf/Zoeteweij-Turhan/Turhan, 11 ff.

Datenbank als Informationsquelle nutzen.[504] Im Rahmen der jüngsten Revision der gesetzlichen Grundlagen des SIS wurde nun auch der Europäischen Agentur für die Grenz- und Küstenwache (Frontex)[505] ein Zugriffsrecht auf das SIS gewährt.[506] Insgesamt dürfen also verschiedene nationale Behörden sowie unterschiedliche Agenturen – gemäss den jeweiligen Voraussetzungen – auf SIS-Daten zugreifen.[507]

In der Schweiz ist eine Vielzahl von Behörden berechtigt, das SIS zur Erfüllung der jeweiligen Aufgaben abzufragen. So z.B. verschiedene Stellen von fedpol, des Nachrichtendienstes des Bundes (NDB), des Bundesamts für Justiz (BJ), des Bundesamts für Zoll und Grenzsicherheit (BAZG), des Staatssekretariats für Migration (SEM), des Bundesamts für Zivilluftfahrt (BAZL), aber auch die Bundesanwaltschaft, die kantonalen Polizei- und Justizbehörden, die zum Vollzug der Landesverweisung zuständigen Behörden, die schweizerischen Vertretungen im Ausland, die kantonalen und kommunalen Migrationsbehörden, Strassenverkehrs- und Schifffahrtsämter sowie die kantonalen Waffenbüros.[508] Die Zugriffs- und Bearbeitungsrechte der im SIS gespeicherten Daten variieren je nach Behörde.[509]

Im Jahr 2023 wurde das SIS insgesamt ca. 14.7 Milliarden Mal abgefragt. Darunter fallen Abfragen anhand von alphanumerischen und biometrischen Daten sowie auch Abfragen zwecks der Erstellung, Aktualisierung oder Verwaltung von Ausschreibungen. Die Schweiz hat davon rund 183 Millionen Abfragen mit alphanumerischen Daten durchgeführt.[510]

504 Stämpfli, 68 f.

505 Frontex unterstützt die Schengen-Staaten beim Schutz ihrer Aussengrenzen und der Bekämpfung von grenzüberschreitender Kriminalität. Siehe dazu mit weiteren Hinweisen <https://frontex.europa.eu/de/>, zuletzt besucht am 07.03.2025.

506 Art. 36 SIS-Grenze-VO; Art. 50 SIS-Polizei-VO.

507 Siehe dazu im Einzelnen Art. 34 ff. SIS-Grenze-VO; Art. 44 ff. SIS-Polizei-VO; Art. 17 SIS-Rückkehr-VO.

508 Art. 7 Abs. 1 N-SIS-Verordnung.

509 Eine detaillierte Übersicht über die einzelnen Zugriffs- und Bearbeitungsrechte der Behörden in der Schweiz findet sich in Anhang 3 Kapitel 1 N-SIS-Verordnung.

510 eu-LISA, SIS report 2023, 6.

4.6. Ausgewählte Sicherheitsmassnahmen

4.6.1. Übermittlung von SIS-Daten an Drittstaaten und internationale Organisationen

Eine Übermittlung von personenbezogenen Daten, welche im SIS bearbeitet werden, an Drittstaaten oder internationale Organisationen ist grundsätzlich nicht gestattet.[511] Im Bereich der Rückkehr dürfen jedoch gewisse Daten unter bestimmten Voraussetzungen einem Drittland übermittelt oder zur Verfügung gestellt werden.[512]

4.6.2. Protokollierungspflicht

Alle im SIS vorgenommenen Abfragen sind von eu-LISA, Europol, Eurojust, Frontex sowie den Schengen-Staaten zu protokollieren.[513]

4.6.3. Rechte der betroffenen Personen

Eine von einer Ausschreibung betroffene Person kann – unter Vorbehalt einiger Ausnahmen – um Auskunft, Berichtigung unrichtiger und Löschung unrechtmässig gespeicherter Daten ersuchen.[514] In der Schweiz wurden im Jahr 2022 rund 5500 Auskunftsgesuche bearbeitet. Im Jahr zuvor waren es knapp doppelt so viele und im Jahr 2020 etwas mehr als 5000.[515]

Personen, welche von bestimmten Ausschreibungen betroffen sind, sind ausserdem über die Datenbearbeitung zu informieren, wobei das nationale Recht gewisse Einschränkungen vorsehen kann.[516]

---

511 Art. 65 SIS-Polizei-VO; Art. 50 SIS-Grenze-VO.

512 Siehe dazu Art. 15 SIS-Rückkehr-VO.

513 Art. 12, Art. 18, Art. 48 Abs. 7, Art. 49 Abs. 4 und Art. 50 Abs. 4 SIS-Polizei-VO; Art. 12, Art. 18, Art. 35 Abs. 7 und Art. 36 Abs. 4 SIS-Grenze-VO.

514 Art. 53 SIS-Grenze-VO; Art. 67 SIS-Polizei-VO. Für die Wahrnehmung dieser Rechte in der Schweiz stehen den betroffenen Personen verschiedene Musterbriefe zur Verfügung. Diese sind unter <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/international/schengen_dublin.html> abrufbar, zuletzt besucht am 07.03.2025.

515 EJPD, GPK-Bericht 2023, 11.

516 Siehe dazu Art. 52 SIS-Grenze-VO. Siehe zu den Rechten der betroffenen Personen auch Majcher.

4.6.4. Haftung und Sanktionen

Personen resp. Schengen-Staaten können für einen entstandenen Schaden vom verursachenden Schengen-Staat resp. von eu-LISA Schadenersatz verlangen. Die Geltendmachung dieser Schadenersatzansprüche unterliegt dem nationalen Recht des betroffenen Schengen-Staats resp. richtet sich – sofern sich der Anspruch gegen eu-LISA richtet – nach den in den Verträgen genannten Voraussetzungen.[517]

Des Weiteren haben die Schengen-Staaten Sanktionen für die missbräuchliche Verwendung von SIS-Daten und für den nicht vorgesehenen Austausch von Zusatzinformationen vorzusehen.[518] In der Schweiz ist ein Bussgeld vorgesehen, wenn Daten des N-SIS für andere als die vorgesehenen Zwecke bearbeitet werden.[519]

5. Eurodac-Datenbank

5.1. Entstehung

Die Eurodac-Datenbank, welche seit dem 15. Januar 2003 in Betrieb ist, enthält insbesondere die Fingerabdruckdaten von Personen, welche in einem Dublin-Staat um Asyl ersucht haben oder illegal über eine Schengen-Aussengrenze in einen Dublin-Staat eingereist sind und nicht zurückgewiesen werden können. Mittels der Abfrage in der Datenbank kann ein Dublin-Staat überprüfen, ob eine asylsuchende Person bereits in einem anderen Dublin-Staat Asyl beantragt hat.[520] Erzielt eine Abfrage einen Treffer in der Datenbank, so kann dadurch die Zuständigkeit für die Prüfung des Asylgesuchs ermittelt werden. Die in der Eurodac-Datenbank enthaltenen Daten dienen somit als Beweis für die Ermittlung der Zuständigkeit des Dublin-Staats gemäss den Dubliner Kriterien.[521]

---

517 Art. 58 SIS-Grenze-VO; Art. 72 SIS-Polizei-VO. In der Schweiz richtet sich dieser Anspruch nach Art. 19*a*-19*c* VG. Siehe dazu Art. 52 N-SIS-Verordnung.

518 Art. 73 SIS-Polizei-VO; Art. 59 SIS-Grenze-VO.

519 Art. 5*a* BPI.

520 Bundesrat, Botschaft Bilaterale II, 6114 ff.; Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2711.

521 Bundesrat, Botschaft Bilaterale II, 5968, 6111; Progin-Theuerkauf/Egbuna-Joss, 183; Fiolka/Stalder, 176.

Die ursprüngliche gesetzliche Grundlage der Datenbank, die altEurodac-VO, wurde mittlerweile erneuert. Diese revidierte Verordnung, die Eurodac-VO, trat am 20. Juli 2015 in Kraft.[522] Mit der Revision waren zahlreiche Änderungen verbunden. So wurden u.a. die Zugriffsrechte zu Eurodac-Daten und der von der Datenbearbeitung betroffene Personenkreis erweitert.[523] Zudem wurden zusätzliche Daten zur Speicherung in der Eurodac-Datenbank vorgesehen.[524] Ferner wurde auch eine Frist zur Übermittlung der erfassten Daten eingeführt und eine Überprüfung des Ergebnisses der Abfrage in der Datenbank durch einen Spezialisten vorgesehen.[525]

5.2. Betrieb und Aufsicht

Das Informationssystem Eurodac besteht aus dem Zentralsystem mit der Fingerabdruck-Datenbank sowie einer Kommunikationsinfrastruktur, welche die Datenübertragung zwischen den Dublin-Staaten und dem Zentralsystem erlaubt. Die Dublin-Staaten verfügen jeweils über eine einzige nationale Zugangstelle zur Datenbank.[526]

Anfänglich war die Kommission für den Betrieb der Eurodac-Datenbank zuständig. Seit dem 1. Dezember 2012 fällt diese Aufgabe in die Zuständigkeit von eu-LISA.[527]

Die Kontrolle der Datenverarbeitung im Zusammenhang mit Eurodac wird einerseits von den nationalen Kontrollbehörden und andererseits – betreffend eu-LISA – durch den EDSB sichergestellt.[528] Des Weiteren existiert eine Koor-

522 Art. 46 Eurodac-VO; Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2710.

523 Siehe dazu Progin-Theuerkauf/Egbuna-Joss, 183. So sollten die Daten von Personen, welche internationalen Schutz erhalten haben, in der Datenbank sichtbar gemacht werden. Dies soll eine allfällige Rückkehr in diesen Staat ermöglichen, welche in diesem Fall nicht gemäss Dublin-III-VO, sondern gemäss bilateralen Rückübernahmeabkommen erfolgt. Vgl. dazu Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2677.

524 So bspw. das Benutzerkennwort der Behörde, das Datum der Einreise bei einer Aufnahme oder Wiederaufnahme. Vgl. dazu Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2711 f.

525 Siehe dazu Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2677, 2711 f.; Art. 25 Abs. 4 Eurodac-VO.

526 Art. 3 Abs. 1-2 Eurodac-VO. Abgesehen davon existiert auch der Datenübermittlungskanal «*DubliNet*». Vgl. dazu Art. 17, Art. 34 und Art. 35 Abs. 4 Eurodac-VO. Siehe dazu auch Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2687; Thür, 965 ff.

527 Art. 38 Verordnung (EU) Nr. 1077/2011; Gloor Scheidegger, 138.

528 Art. 30 f. Eurodac-VO. Siehe zudem Art. 33 Eurodac-VO betreffend die Überwachung der Datenbearbeitung zur Gefahrenabwehr und Strafverfolgung sowie von Europol.

dinierungsgruppe bestehend aus dem EDSB und den nationalen Kontrollstellen. Diese kann Empfehlungen zum Betrieb von Eurodac erlassen.[529]

5.3. Beteiligung der Schweiz

Im Rahmen der Dublin-Assoziierung wurden sowohl die altEurodac-VO als auch die Dublin-II-VO von der Schweiz übernommen. Der effektive Anschluss der Schweiz an das Dublin-System erfolgte im Jahr 2008.[530] Später übernahm die Schweiz die Dublin-III-VO, welche die Dublin-II-VO ersetzte, sowie die Eurodac-VO.[531] Diese beiden Verordnungen stellen jeweils Weiterentwicklungen des Dublin- resp. Eurodac-Besitzstands dar. Davon ausgenommen ist die Zugriffsgewährung der nationalen Strafverfolgungsbehörden auf die Eurodac-Datenbank. Dieser Zugriff stellt keine solche Weiterentwicklung dar.[532]

Die Anwendung der Dublin-III-VO sowie der Eurodac-VO erfolgte in der Schweiz zeitgleich wie in der EU, nämlich per 1. Januar 2014 resp. per 20. Juli 2015.[533] Sowohl die Dublin-III-VO als auch die Eurodac-VO sind – zumindest weitgehend – direkt anwendbar. Dennoch mussten einige Anpassungen in der nationalen Gesetzgebung vorgenommen werden.[534]

Die Bearbeitung von Personendaten in der Dubliner Zusammenarbeit wird vom EDÖB beaufsichtigt. Diese Aufsichtstätigkeit koordiniert dieser mit den nationalen Datenschutzbehörden. Zudem arbeitet der EDÖB zur Wahrnehmung seiner Aufgaben mit dem EDSB zusammen.[535]

---

529 Gloor Scheidegger, 143 f. In der Schweiz gibt es zudem die Koordinationsgruppe Schengen für die Zusammenarbeit zwischen dem EDÖB sowie den kantonalen Datenschutzbehörden. Gloor Scheidegger, 144.

530 Art. 1 DAA; Progin-Theuerkauf/Egbuna-Joss, 186. Vgl. dazu auch Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2675 ff.; Bundesrat, Botschaft Bilaterale II, 6114.

531 Siehe zu den Änderungen der Dublin-III-VO im Vergleich mit der Dublin-II-VO Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2685 ff. In der Dublin-III-VO werden teilweise Begriffe verwendet, welche die Schweiz nicht kennt. So gelten die im EU-Recht um internationalen Schutz ersuchende Personen in der Schweiz als asylsuchende Personen. Siehe dazu Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2691. Ferner wird der im EU-Recht verwendete Begriff des subsidiären Schutzes grundsätzlich der vorläufigen Aufnahme gemäss Art. 83 AIG gleichstellt. Siehe dazu Progin-Theuerkauf/Egbuna-Joss, 187.

532 Vgl. dazu Art. 1 Abs. 3 und Art. 4 DAA; Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2677 f., 2682.

533 Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2682.

534 Vgl. zu den direkt anwendbaren Bestimmungen der Dublin-III-VO sowie der Eurodac-VO Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2714, 2724. Siehe zu den gesetzlichen Anpassungen Bundesrat, Botschaft Dublin-III-VO/Eurodac-VO, 2683, 2714 f.

535 Art. 120*d* AsylG.

Um ihren nationalen Strafverfolgungsbehörden ebenfalls eine Zugriffsmöglichkeit auf Eurodac-Daten zu ermöglichen, hat die Schweiz mit der EU und dem Fürstentum Liechtenstein ein Protokoll, das sog. Eurodac-Protokoll, abgeschlossen. Dieses ist am 1. Mai 2022 in Kraft getreten. Parallel zum Eurodac-Protokoll wurde auch die Beteiligung der Schweiz an der sog. Prümer Zusammenarbeit verhandelt und ein entsprechendes Abkommen unterzeichnet.[536]

Der Vertrag von Prüm wurde 2005 von sieben Mitgliedstaaten ausserhalb des EU-Rahmens unterzeichnet. Im Rahmen der Prümer Zusammenarbeit können insbesondere DNA-Profile, Fingerabdruckdaten und Fahrzeugregisterdaten zwecks Bekämpfung des Terrorismus und grenzüberschreitender Kriminalität vereinfacht zwischen den zuständigen Behörden ausgetauscht werden. Es soll möglichst rasch in Erfahrung gebracht werden können, ob das eingegebene Datenmuster bereits in einer Datenbank eines anderen Staates erfasst ist. Im Jahr 2008 wurde die Prümer Zusammenarbeit in den EU-Rahmen überführt.[537] Prüm stellt keine Weiterentwicklung des Schengen-Besitzstands dar.[538] Die bestehende Prümer Zusammenarbeit wurde mittlerweile durch die VO 2024/982, die sog. Prüm-II-Verordnung, revidiert.[539] Die Beteiligung an Prüm stellt insofern eine Voraussetzung für das Eurodac-Protokoll dar, als der Zugriff der nationalen Strafverfolgungsbehörden auf Eurodac-Daten u.a. nur dann gewährt wird, wenn vorgängig eine Abfrage in Prüm negativ verlaufen ist.[540]

Aufgrund der technisch notwendigen Vorkehrungen ist in der Schweiz frühestens im Jahr 2024 mit dem Beginn der Prümer Zusammenarbeit und somit auch der Abfragemöglichkeit von Eurodac durch die nationalen Strafverfolgungsbehörden zu rechnen.[541]

---

536 Vgl. dazu das Abkommen Prüm CH-EU. Siehe zum Ganzen auch BUNDESRAT, Botschaft Prüm/Eurodac-Protokoll m.w.H. Siehe betreffend den Zeitpunkt des Inkrafttretens des Eurodac-Protokolls ABl. L 240 vom 16.9.2022, 1. Siehe zu diesen beiden Abkommen auch <https://www.eda.admin.ch/europa/de/home/bilateraler-weg/bilaterale-abkommen-nach-2004/eurodac.html> , <https://www.eda.admin.ch/europa/de/home/bilateraler-weg/bilaterale-abkommen-nach-2004/pruem.html>, beide zuletzt besucht am 07.03.2025.

537 Vgl. dazu die Prümer Beschlüsse: Beschluss 2008/615/JI; Beschluss 2008/616/JI.

538 BOEHM, 8; EJPD, GPK-Bericht 2021, 17. Siehe zur Prümer Zusammenarbeit auch VAVOULA, Police Information Exchange, 16 ff.; MITSILEGAS/VAVOULA, 536 ff. m.w.H.; AMREIN, et al., sektorielle Abkommen 2019, 498 f.

539 Siehe zum entsprechenden Vorschlag der Kommission EUROPÄISCHE KOMMISSION, COM(2021) 784 final.

540 Siehe zu diesem Zugriff der nationalen Strafverfolgungsbehörden Kapitel III.5.5.2.

541 EJPD, GPK-Bericht 2021, 17 f.

5.4. Gespeicherte Daten

Drei Personenkategorien sind von der Datenbearbeitung, welche im Zusammenhang mit der Eurodac-Datenbank vorgenommen wird, betroffen. Dabei handelt es sich um asylsuchende Personen (Kategorie I). Des Weiteren werden auch bei einem illegalen Grenzübertritt an einer Schengen-Aussengrenze in einen Dublin-Staat einreisende aufgegriffene Drittstaatsangehörige oder Staatenlose, welche nicht zurückgewiesen werden können, erfasst (Kategorie II). Davon abgesehen sind auch sich in einem Dublin-Staat illegal aufhaltende Drittstaatsangehörige oder Staatenlose von der Datenbearbeitung betroffen (Kategorie III). Von den in diese Kategorien fallenden Personen werden mindestens (aber je nach Personenkategorie nicht nur) die Fingerabdruckdaten erhoben, wobei die betroffenen Personen mindestens 14 Jahre alt sein müssen.[542]

Bei den Personenkategorien I und II sind neben den Fingerabdruckdaten[543] noch weitere Angaben zu erfassen. So z.B. das Geschlecht, den Zeitpunkt der Abnahme der Fingerabdruckdaten sowie der Ort und der Zeitpunkt des Aufgreifens der betroffenen Person. Diese Angaben sind grundsätzlich innert 72 Stunden an das Zentralsystem zu übermitteln. Fingerabdruckdaten von Personen der Kategorie I werden zuerst automatisch mit den bereits im Zentralsystem gespeicherten Fingerabdrücken abgeglichen, ehe sie gespeichert werden. Angaben von Personen der Kategorie II werden ohne einen solchen vorgängigen Abgleich dem Zentralsystem zugefügt. Diese Daten stehen danach ausschliesslich für einen Abgleich mit Daten der Kategorie I zur Verfügung.[544] Bei der Personenkategorie III werden ausser den Fingerabdruckdaten keine anderen Daten erhoben. Diese Daten werden zwar mit den erfassten Daten der Personenkategorie I abgeglichen, aber nicht in der Eurodac-Datenbank gespeichert.[545]

In der Schweiz sind die Grenzposten und die Polizeibehörden der Kantone und Gemeinden für die Erhebung der Fingerabdruckdaten der Personenkategorien II und III zuständig.[546] Die Erhebung der Fingerabdruckdaten von asylsuchenden Personen, also der Personenkategorie I, erfolgt hingegen durch das SEM im Rahmen der nach der Einreichung des Asylgesuchs anschliessenden

542 Siehe zur Kategorie I Art. 9 ff. Eurodac-VO; zur Kategorie II Art. 14 ff. Eurodac-VO; zur Kategorie III Art. 17 Eurodac-VO.

543 Siehe zur Definition Art. 2 Abs. 1 Bst. l Eurodac-VO.

544 Art. 9, Art. 14 und Art. 15 Eurodac-VO.

545 Art. 17 Eurodac-VO.

546 Art. 111i Abs. 1 und 6 AIG.

Vorbereitungsphase. In diesem Verfahrensschritt erfolgt auch der Abgleich mit der Eurodac-Datenbank.[547]

Daten der Kategorie II werden nach spätestens 18 Monaten automatisch gelöscht, diejenigen der Kategorie I nach spätestens zehn Jahren.[548]

Ende 2023 waren in der Eurodac-Datenbank rund 7.3 Millionen Datensätze gespeichert. Gerade noch rechtzeitig konnte die maximale Speicherkapazität von 7 auf 9 Millionen Datensätze erhöht werden. Die grosse Mehrheit dieser gespeicherten Datensätze stammen von Personen der Kategorie I.[549] Rund 159'000 der in Eurodac gespeicherten Datensätze wurden von den schweizerischen Behörden erhoben.[550]

5.5. Zugriffsberechtigung

Ursprünglich war der Zugriff auf die gespeicherten Daten in der Eurodac-Datenbank auf Behörden aus dem Asylbereich beschränkt gewesen. Durch die Revision der altEurodac-VO wurden jedoch auch nationale Strafverfolgungsbehörden sowie Europol berechtigt, zwecks Strafprävention und -verfolgung auf die Datenbank zuzugreifen.[551] Diese Zugriffsberechtigungen wurden an gewisse Voraussetzungen geknüpft.[552]

5.5.1. Asylbehörden

Die Eurodac-VO legt fest, dass die Dublin-Staaten grundsätzlich nur auf die selbst erhobenen Daten zugreifen dürfen. Auf von einem anderen Staat erhobenen Daten darf nur zugegriffen werden, sofern ein Treffer erfolgt ist. Die Dublin-Staaten bezeichnen die Behörden, welche für die Verfolgung der mit der Eurodac-VO bezweckten Ziele zuständig sind. Diesen wird Zugriff auf das

547 Art. 26 Abs. 2 und 4 AsylG. Da die Schweiz materiellrechtlich im Asylbereich nicht an EU-Recht gebunden ist, folgt das schweizerische Asylverfahren nationalem Recht. Vgl. dazu Progin-Theuerkauf/Egbuna-Joss, 186 f. Vgl. dazu auch Caroni, 87 ff. m.w.H.

548 Siehe zu den Einzelheiten Art. 12, Art. 13 und Art. 16 Eurodac-VO.

549 eu-LISA, Eurodac report 2023, 3.

550 eu-LISA, Eurodac report 2023, 22.

551 Europol ist im Gegensatz zu den nationalen Strafverfolgungsbehörden zusätzlich auf die Zustimmung des Herkunftsmitgliedstaats angewiesen. Diese ist bei der nationalen Europol-Zentralstelle einzuholen. Siehe dazu Art. 21 Eurodac-VO.

552 Siehe dazu Lobsiger/Gloor Scheidegger, 324 ff. m.w.H.; Amrein, et al., sektorielle Abkommen 2018, 523 f. m.w.H.

Zentralsystem gewährt. Eine Liste mit den von den Dublin-Staaten bezeichneten Behörden wird von eu-LISA veröffentlicht.[553]

Nimmt eine solche abfrageberechtigte Behörde einen Abgleich in der Eurodac-Datenbank vor, wird das Ergebnis eines Abgleichs – also entweder ein Treffer oder ein negatives Ergebnis – vom Zentralsystem automatisch demjenigen Staat mitgeteilt, welcher die Daten in das Zentralsystem übermittelt hat. Liegt ein Treffer vor, werden die im Zentralsystem gespeicherten Daten dem entsprechenden Dublin-Staat zugänglich gemacht.[554] Das Ergebnis des Datenabgleichs wird im Dublin-Staat, welcher die Daten des Abgleichs erhält, von einer Fachperson für Daktyloskopie geprüft.[555]

In der Schweiz erhält das SEM im Rahmen des im nationalen Asylverfahren vorgesehenen automatischen Abgleichs Zugang zu Eurodac-Daten, sofern ein Treffer vorliegt.[556] Ausserdem können Grenzposten und die Ausländer- und Polizeibehörden der Kantone und Gemeinden anhand der Abnahme der Fingerabdruckdaten von sich illegal in der Schweiz aufhaltenden Personen über 14 Jahren in der Eurodac-Datenbank überprüfen, ob diese schon in einem anderen Dublin-Staat ein Asylgesuch gestellt haben.[557]

5.5.2. Nationale Strafverfolgungsbehörden

Zum Zweck der Gefahrenabwehr und Strafverfolgung können die Mitgliedstaaten zuständige Behörden benennen. Explizit ausgeschlossen sind jedoch Behörden resp. Einheiten, welche im Rahmen der nationalen Sicherheit ausschliesslich nachrichtendienstlich tätig sind.[558] Diese Behörden, welche im Folgenden als nationale Strafverfolgungsbehörden bezeichnet werden, sind grundsätzlich berechtigt, einen Abgleich für die Verhütung, Aufdeckung oder

553 Art. 27 Abs. 1 und 2 Eurodac-VO. Siehe zur Liste zuletzt EU-LISA, Eurodac list of designated authorities 2024.

554 Art. 9 Abs. 3 und 5 Eurodac-VO; Art. 17 Abs. 5 Eurodac-VO.

555 Art. 25 Abs. 4 Eurodac-VO.

556 Art. 102*a*bis Abs. 3 AsylG.

557 Art. 111*i* Abs. 6 AIG. Dabei handelt es sich um einen Abgleich von Daten der Kategorie III mit Daten der Kategorie I. Siehe dazu PRIULI, in: Kommentar Migrationsrecht, Art. 111i AIG N 2.

558 Siehe dazu Art. 5 Eurodac-VO. Bei anderen Informationssystemen, welche ebenfalls einen solchen Zugriff vorsehen, sind ausschliesslich nachrichtendienstlich tätige Behörden nicht explizit ausgeschlossen (vgl. dazu Art. 29 EES-VO; Art. 50 ETIAS-VO; Art. 3 VIS-VO). Siehe dazu VAVOULA, Right to Private Life, 263.

Untersuchung von terroristischen[559] oder sonstigen schweren Straftaten[560] mit Eurodac-Daten zu beantragen.[561] Solche Anträge sind auf Abfragen anhand von Fingerabdruckdaten beschränkt. Ein Antrag kann nur gestellt werden, wenn vorgängig bereits andere Informationssysteme (insbesondere die nationalen Fingerabdruck-Datenbanken, die Datenbanken der Prümer Zusammenarbeit sowie das VIS) abgefragt worden sind und dabei kein Treffer erzielt worden ist. Diese Pflicht zur vorgängigen Abfrage von anderen Informationssystemen wird auch «*Kaskadenmechanismus*» bezeichnet. Erst wenn diese Abfragen negativ verlaufen sind, also kein Treffer in diesen Systemen erzielt wurde, kann die nationale Strafverfolgungsbehörde einen begründeten Antrag in elektronischer Form auf Einsicht in die Eurodac-Daten bei der von den Mitgliedstaaten bezeichneten nationalen Prüfstelle einreichen.[562]

Der Zugang zu den Eurodac-Daten setzt voraus, dass Abgleich für die Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich und verhältnismässig ist, im Zusammenhang mit einem Einzelfall erforderlich ist (damit werden systematische Abfragen ausgeschlossen) und hinreichende Gründe vorliegen, dass der beantragte Abgleich wesentlich zur Verhütung, Aufdeckung oder Ermittlung einer Straftat beitragen wird.[563]

Kommt die Prüfstelle zum Schluss, dass die Voraussetzungen für eine Einsichtnahme gegeben sind, wird der Antrag an die nationale Zugangstelle weitergeleitet, welche in der Folge den effektiven Abgleich mit dem Zentralsystem vornimmt. In dringenden Fällen kann die Überprüfung des Antrags auch erst nach der Vornahme des Abgleichs erfolgen. Ob ein dringender Ausnahmefall vorgelegen hat, wird im Anschluss geprüft. Wird im Rahmen dieser Prüfung

559 Siehe zur Definition Art. 2 Abs. 1 Bst. j Eurodac-VO. In der Schweiz sind die terroristischen Straftaten in Anhang 1a der N-SIS-Verordnung aufgeführt.

560 Siehe zur Definition Art. 2 Abs. 1 Bst. k Eurodac-VO. In der Schweiz sind die sonstigen schweren Straftaten dem Anhang 1b der N-SIS-Verordnung zu entnehmen.

561 Der Begriff der nationalen Strafverfolgungsbehörden wird auch beim VIS, EES und ETIAS verwendet. Diese Systeme sehen ebenfalls eine solche Abfrage vor, wobei die Zugangsbedingungen sich teilweise unterscheiden. Unter dem Begriff werden in der vorliegenden Untersuchung Behörden der Schengen/Dublin-Staaten verstanden, welche zwecks «*Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit*» zuständig sind. Vgl. dazu FRA, Gesichtserkennungstechnologien, 3.

562 Siehe zum Ganzen Art. 19 f. Eurodac-VO. Vgl. dazu auch Amrein, et al., sektorielle Abkommen 2018, 523 f. Siehe zur Verwendung des Begriffs «*Kaskadenmechanismus*» z.B. in European Commission, Impact assessment IOP Part 1, 25. Siehe zur nationalen Prüfstelle Art. 6 Eurodac-VO.

563 Art. 20 Abs. 1 Eurodac-VO.

festgestellt, dass der Zugang zu Eurodac nicht berechtigt war, sind die übermittelten Daten zu löschen.[564]

Die Gewährung des Zugangs von nationalen Strafverfolgungsbehörden auf Eurodac-Daten war sehr umstritten. So mussten mehrere Vorschläge ausgearbeitet werden, ehe die Eurodac-VO schliesslich verabschiedet werden konnte.[565] Es gab diverse kritische Stimmen, u.a. aufgrund von datenschutzrechtlichen Bedenken. Insbesondere die Notwendigkeit sowie die Verhältnismässigkeit einer solchen Zugriffsgewährung wurden in Frage gestellt.[566]

Im Jahr 2023 wurden knapp 1600 Abfragen in der Eurodac-Datenbank von nationalen Strafverfolgungsbehörden vorgenommen.[567] Diese Zahl ist vergleichbar mit derjenigen vom Vorjahr. In den Jahren 2021 und 2019 wurden jedoch merklich weniger solche Abfragen vorgenommen.[568]

5.5.3. Europol

Der Zugang von Europol zu Eurodac-Daten erfolgt – wie auch derjenige der nationalen Strafverfolgungsbehörden – nicht direkt. Die Voraussetzungen sind insgesamt sehr ähnlich wie für die nationalen Strafverfolgungsbehörden. Anders ist, dass Europol die durch einen Abgleich mit Eurodac-Daten erlangten Angaben nur bearbeiten darf, wenn der Staat, welcher die Daten an das Zentralsystem übermittelt hat, einer Verarbeitung zustimmt. Diese Zustimmung ist über die nationale Europol-Zentralstelle des betroffenen Mitgliedstaats einzuholen.[569] Europol hat im Jahr 2023 über 500 solcher Abfragen vorgenommen.[570] Im Vorjahr waren es noch deutlich weniger.[571]

564 Art. 19 Eurodac-VO.

565 Wobei nicht alle diese Vorschläge einen Zugang der nationalen Strafverfolgungsbehörden vorsahen. Siehe dazu VAVOULA, EU immigration databases, 232 f. Siehe zur Entwicklung des Zugangs der nationalen Strafverfolgungsbehörden zu Eurodac auch VAVOULA, Right to Private Life, 241 ff.; UN HIGH COMMISSIONER FOR REFUGEES, Comment Eurodac 2012, 1 ff.

566 Siehe dazu z.B. EDSB, Stellungnahme Eurodac 2009; MEIJERS COMMITTEE, Vorschlag Eurodac 2012; EDSB, Stellungnahme Vorschlag Eurodac 2012; UN HIGH COMMISSIONER FOR REFUGEES, Comment Eurodac 2012; FRA, Opinion Eurodac 2016, 39 ff.

567 EU-LISA, Eurodac report 2023, 12.

568 EU-LISA, Eurodac 2022, 18.

569 Siehe zu den Einzelheiten Art. 7, Art. 19 und Art. 21 Eurodac-VO. Die Zugriffsgewährung von Europol auf Eurodac-Daten wurde kritisiert. Siehe dazu z.B. MEIJERS COMMITTEE, Vorschlag Eurodac 2012.

570 EU-LISA, Eurodac report 2023, 12.

571 EU-LISA, Eurodac 2022, 15.

5.6. Ausgewählte Sicherheitsmassnahmen

5.6.1. Übermittlung von Eurodac-Daten an Drittstaaten, internationale Organisationen und private Stellen

Eurodac-Daten dürfen grundsätzlich nicht an einen Drittstaat, eine internationale Organisation oder eine private Stelle innerhalb oder ausserhalb der Union weitergeleitet werden. Dieses Verbot erstreckt sich nicht auf Staaten, welche die Dublin-III-VO anwenden.[572]

Eurodac-Daten, welche aufgrund einer Abfrage zwecks Strafverfolgung erhältlich gemacht worden sind, dürfen nicht an Drittstaaten weitergegeben werden, wenn ein ernstzunehmendes Risiko vorliegt, dass die Datenübermittlung zu Folterung, unmenschlicher und erniedrigender Behandlung oder Bestrafung oder anderen Menschenrechtsverletzungen führt.[573]

5.6.2. Protokollierungspflicht

Die Dublin-Staaten sowie Europol haben die Abfragen in der Eurodac-Datenbank zu protokollieren. Alle Datenbearbeitungsvorgänge im Zentralsystem werden von eu-LISA protokolliert.[574]

5.6.3. Rechte der betroffenen Personen

Die Eurodac-VO gewährt Personen, welche von in dieser Verordnung vorgesehenen Datenverarbeitungen betroffen sind, gewisse Rechte. So haben die Dublin-Staaten den betroffenen Personen bestimmte Angaben mitzuteilen. Diese Informationspflicht umfasst u.a. die Erläuterung des Zwecks der Datenbearbeitung, die Bekanntgabe der Empfänger der Daten sowie den Hinweis auf die Möglichkeit Auskunft, Berichtigung oder Löschung hinsichtlich der Daten zu beantragen. Die Kommission hat ein gemeinsames Merkblatt erstellt, welches von den Dublin-Staaten mit Informationen ergänzt werden kann und den betroffenen Personen abzugeben ist. Die Information hat grundsätzlich bei der Fingerabdruckabnahme resp. spätestens zum Zeitpunkt der Übermittlung der Daten an das Zentralsystem zu erfolgen. Von der Informationspflicht kann nur

572 Art. 27 Abs. 5 Eurodac-VO; Art. 35 Eurodac-VO.
573 BUNDESRAT, Botschaft Dublin-III-VO/Eurodac-VO, 2714.
574 Art. 28 Eurodac-VO; Art. 36 Eurodac-VO.

abgesehen werden, wenn diese unmöglich oder mit einem unverhältnismässigen Aufwand verbunden ist.[575]

Darüber hinaus verfügen die betroffenen Personen über ein Recht auf Auskunft, Berichtigung und Löschung der eigenen Daten. Da in der Datenbank keine Angaben zum Namen der Person gespeichert werden, muss sich die um Auskunft begehrende Person nicht nur bezüglich ihrer Identität ausweisen, sondern hat auch ihre Fingerabdruckdaten einzureichen.[576] Wird ein Antrag auf Berichtigung resp. Löschung vom Dublin-Staat abgelehnt, so ist dies von diesem entsprechend zu begründen. Gleichzeitig mit der schriftlichen Begründung ist die betroffene Person über die Möglichkeit einer Beschwerde gegen die Ablehnung des Antrags zu informieren. Grundsätzlich gilt, dass eine Änderung resp. Löschung nur von demjenigen Dublin-Staat vorgenommen werden kann, welcher die Daten in die Datenbank eingegeben hat.[577]

5.6.4. Haftung und Sanktionen

In der Eurodac-VO ist eine Haftung vorgesehen. So kann eine Person oder ein Dublin-Staat, welcher resp. welchem durch eine rechtswidrige Verarbeitung oder einer anderen der Eurodac-VO zuwiderlaufenden Handlung ein Schaden entsteht, von dem für den Schaden verantwortlichen Dublin-Staat Schadenersatz verlangen. Dieser Staat kann sich (teilweise) von seiner Haftung befreien, sofern ihm der Nachweis gelingt, dass er für den Schaden verursachenden Umstand nicht verantwortlich ist. Kommt ein Dublin-Staat seinen Verpflichtungen nicht nach und entsteht dadurch ein Schaden am Zentralsystem, ist dieser Dublin-Staat für den Schaden haftbar, sofern weder eu-LISA noch ein anderer Dublin-Staat angemessene Schritte unternommen haben, um den Schaden abzuwenden resp. zu mindern. Diese Schadenersatzansprüche unterliegen dem nationalen Recht des beklagten Dublin-Staats.[578] In der

575 Art. 29 Abs. 1-3 Eurodac-VO. Eine Ausnahme von der Informationspflicht könnte im Fall eines plötzlichen Massenzustroms von Asylbewerbern vorliegen. Siehe zum Ganzen De Terwangne, migrants et réfugiés, 105 f.

576 Im Gegensatz zum SIS kann das Auskunftsrecht nicht eingeschränkt werden. Die im Rahmen eines Antrags auf Auskunft eingereichten Fingerabdrücke dürfen nur für diesen Zweck verwendet werden und sind danach sofort zu löschen. Siehe dazu Gloor Scheidegger, 138 f.; Thür, 966.

577 Siehe zum Ganzen Art. 29 Abs. 4-15 Eurodac-VO.

578 Art. 37 Eurodac-VO.

Schweiz richten sich solche Ansprüche nach dem Verantwortlichkeitsgesetz (VG), wobei insbesondere die Art. 19*a*-19*c* VG sinngemäss anwendbar sind.[579]

Darüber hinaus haben die Dublin-Staaten Massnahmen vorzusehen, damit jede Datenbearbeitung, welche nicht der Feststellung der Zuständigkeit des Dublin-Staats hinsichtlich einem von einem Drittstaatsangehörigen gestellten Asylantrags dient, mit wirksamen, verhältnismässigen sowie abschreckenden Sanktionen geahndet wird.[580] In der Schweiz ist ein Bussgeld vorgesehen.[581]

5.7. Ausblick

Nach jahrelangen Verhandlungen konnte mit dem Asyl- und Migrationspaket schliesslich eine Einigung für eine Reform im Bereich Migration und Asyl erreicht werden.[582] Der im Mai 2024 verabschiedete Pakt umfasst verschiedene Verordnungen. Eine davon, die VO 2024/1358, wird die Eurodac-VO aufheben. Obwohl diese neue Verordnung bereits in Kraft gesetzt worden ist, wird sie – nach der Umsetzungsfrist für die Dublin-Staaten – grundsätzlich erst ab dem 12. Juni 2026 gelten.[583] Mit der neuen Verordnung wird der Kreis der Personenkategorien erweitert und es werden mehr Daten erhoben. Insbesondere werden neu ein Foto, der Name sowie das Alter der Person erfasst. Ausserdem werden die Fingerabdruckdaten nicht mehr ab 14 Jahren, sondern bereits ab sechs Jahren erhoben.[584] Davon abgesehen muss ein Fachmann für Daktyloskopie das Ergebnis eines Vergleichs der Fingerabdruckdaten nur noch

---

579 Art. 11*b* AsylV 3. Siehe dazu auch Gloor Scheidegger, 140 ff.; Schweizer, Datenschutzrechte, Rz. 12.

580 Art. 41 Eurodac-VO.

581 Art. 117*a* AsylG.

582 Siehe zu den Vorschlägen für die Revision der Eurodac-VO Europäische Kommission, Vorschlag Eurodac Neufassung 2016; Europäische Kommission, Geänderter Vorschlag Eurodac Neufassung 2020. Siehe für eine Bewertung dieser Vorschläge Vavoula, Transforming Eurodac, 10 ff. Siehe zur geplanten Neufassung der Dublin-III-VO Europäische Kommission, Vorschlag Dublin-III-VO Neufassung 2016. Siehe zur Einschätzung des EDSB zum Reformpaket des GEAS EDSB, Stellungnahme Reformpaket GEAS 2016. Siehe zu den Einzelheiten des Asyl- und Migrationspakets Europäische Kommission, COM(2020) 609 final. Für eine Bewertung dieses Pakets siehe EDSB, Stellungnahme Asyl- und Migrationspaket. Siehe für einen Überblick über diese Reformbestrebungen Hruschka/Frei; EJPD, GPK-Bericht 2021, 10 f.; Hruschka, Reformvorschläge; Caroni, et al., § 6 N 383 ff.

583 Siehe zu den Einzelheiten der Anwendbarkeit der Verordnung Art. 63 Verordnung 2024/1358.

584 Siehe für einen Überblick über den Asyl- und Migrationspakt <https://www.sem.admin.ch/sem/de/home/international-rueckkehr/kollab-eu-efta/eu-migrations-asyl-pakt.html>, zuletzt besucht am 07.03.2025.

dann überprüfen, wenn dies erforderlich erscheint. Ausserdem ist es den Dublin-Staaten möglich, das Ergebnis des Vergleichs der Gesichtsbilder zu überprüfen, sofern sowohl ein Treffer bezüglich den Fingerabdruckdaten als auch des Gesichtsbilds vorliegen.[585] Des Weiteren wird das bis anhin strikte Verbot der Übermittlung von Daten an Drittstaaten, internationalen Organisationen oder privaten Stellen unter bestimmten Voraussetzungen gelockert.[586] Auch der Zugang zu Eurodac-Daten zwecks Verhinderung, Aufdeckung sowie Untersuchung terroristischer oder sonstiger schwerer Straftaten wird angepasst. So können einerseits nun auch Behörden berechtigt werden, solche Abfragen vorzunehmen, welche ausschliesslich nachrichtendienstliche Aufgaben wahrnehmen.[587] Andererseits werden die Zugangsvorausetzungen gelockert. Grundsätzlich bleibt zwar das Erfordernis der Kaskade bestehen. Die Abfrage im VIS wird dabei jedoch nicht mehr zwingend verlangt. Ausserdem wird der Kaskadenmechanismus abgeschafft, sofern eine Abfrage gemäss Art. 22 IOP-Polizei-VO einen Treffer in Eurodac ergeben hat.[588] Wie sich im Folgenden noch zeigen wird, wird mit dieser Bestimmung die Abfrageberechtigung von den nationalen Strafverfolgungsbehörden auf Daten von Systemen aus dem Migrationsbereich stark verändert.[589]

6. Visa-Informationssystem

6.1. Entstehung

Die Schengen-Staaten verfügen über eine einheitliche europäische Visumpolitik.[590] Diese beschränkt sich bis anhin auf die Ausstellung von Visa für kurzfris-

585 Siehe dazu Art. 38 VO 2024/1358.

586 Siehe zu den Einzelheiten Art. 50 VO 2024/1358.

587 Art. 6 VO 2024/1358.

588 Art. 33 VO 2024/1358. Diese neue Regelung hat zur Folge, dass der Kaskadenmechanismus bestehen bleibt, sofern gezielt Einsicht in Eurodac-Daten verlangt wird. Wird hingegen eine Abfrage des CIR gemäss Art. 22 EU-IOP-VO vorgenommen, sind keine anderen Datenbanken vorgängig abzufragen. Diese uneinheitliche Regelung erscheint nicht nachvollziehbar. Da mit der Abfrage des CIR gleichzeitig verschiedene Datenbanken abgefragt werden können, dürfte in der Praxis keine Anwendung mehr für eine gezielte Abfrage in Eurodac bestehen. Insofern wird mit dieser neuen Regelung der Kaskadenmechanismus bei Eurodac faktisch abgeschafft.

589 Siehe zur Abfrage gemäss Art. 22 IOP-Polizei-VO Kapitel IV.5.3.3.3 sowie V.3.4.3. Siehe insgesamt kritisch zum Asyl- und Migrationspakt KHENNOUF; <https://www.fluechtlingshilfe.ch/themen/migrationspolitik/eu-pakt-zu-migration-und-asyl>, zuletzt besucht am 07.03.2025.

590 BUNDESRAT, Botschaft Bilaterale II, 6067 f.

tige Aufenthalte. So haben Staatsangehörige bestimmter Länder, welche sich höchstens während 90 Tagen in einem Zeitraum von 180 Tagen auf dem Hoheitsgebiet der Schengen-Staaten aufhalten wollen, ein sog. Schengen-Visum zu beantragen.[591] Die Ausstellung von Visa für längere Aufenthalte, also solchen von mehr als 90 Tagen im Hoheitsgebiet der Schengen-Staaten, fällt bislang noch in die Kompetenz der einzelnen Schengen-Staaten. Diese befinden gemäss ihrem nationalen Recht darüber.[592]

Im Zuge der Errichtung dieses gemeinsamen Visaregimes wurde das VIS geschaffen. Das Informationssystem wurde zwischen Oktober 2011 und Februar 2016 gestaffelt in Betrieb genommen.[593] In dieser Zeitspanne wurden immer mehr Konsulate der Schengen-Staaten – geordnet nach geographischen Regionen – an die Datenbank angeschlossen.[594]

Im Zeitraum zwischen Oktober 2021 und Ende September 2023 wurden über 17 Millionen Visagesuche registriert und bearbeitet. 64 % davon wurde von vier Schengen-Staaten bearbeitet (Frankreich, Deutschland, Italien und Spanien).[595] Vor der COVID-19-Pandemie wurden allein im Jahr 2019 über 17 Millionen Visagesuche bearbeitet.[596] Im Jahr 2022 stammten die meisten Visagesuche von Staatsangehörigen von Ländern Nordafrikas, des Westbalkans (inkl. Türkei), der Golfregion sowie von Indien und Pakistan.[597]

Die VIS-Datenbank enthält generelle Informationen zu erteilten, verweigerten, verlängerten, annullierten resp. aufgehobenen Visa für kurzfristige Aufenthalte im Schengen-Raum.[598] Des Weiteren können im VIS Konsultationen zwischen den zentralen Visumbehörden erfolgen. Diese können sich gegen die Erteilung eines Visums aussprechen.[599]

Mit dem VIS wird der Datenaustausch zwischen den Schengen-Staaten betreffend Visumanträge und damit verbundenen Entscheidungen erleichtert, was zu Verbesserungen bei der Durchführung der gemeinsamen Visapolitik,

591 Siehe zu den visapflichtigen Drittstaatsangehörigen Anhang I VO 2018/1806.

592 Vgl. dazu Art. 18 SDÜ; Art. 1 Visakodex sowie Art. 6 Schengener Grenzkodex.

593 Bundesrat, Botschaft Bilaterale II, 6078; Gloor Scheidegger, 150; eu-LISA, VIS report 2022, 4.

594 Vgl. dazu Bundesamt für Migration, Erläuterungen C-VIS und ORBIS 2013, 4. Siehe zur Entstehung des VIS auch Vavoula, EU immigration databases, 224 ff.; Vavoula, Right to Private Life, 236 ff.

595 eu-LISA, VIS report 2024, 20.

596 eu-LISA, VIS report 2022, 21.

597 eu-LISA, VIS report 2024, 18. Im vorangehenden Jahr stammten die meisten Visagesuche von russischen Staatsangehörigen. Siehe dazu eu-LISA, VIS report 2022, 22.

598 Lobsiger/Gloor Scheidegger, 320 ff. Vgl. dazu auch Art. 32 ff. Visakodex.

599 Bundesrat, Botschaft Bilaterale II, 6077 f.; Art. 16 VIS-VO.

der konsularischen Zusammenarbeit sowie der Konsultationen zwischen den zentralen Visumbehörden führt. Damit können weitere Ziele erreicht werden, insbesondere Erleichterungen der Betrugsbekämpfung, der Visumantragsverfahren, der Kontrollen an den Aussengrenzen sowie im Hoheitsgebiet der Schengen-Staaten und der Anwendung der Dublin-III-VO resp. die Leistung eines Beitrags zur Verhinderung von Gefahren für die innere Sicherheit der einzelnen Schengen-Staaten.[600]

Die VIS-Datenbank basiert auf der Verordnung (EG) Nr. 767/2008 (VIS-VO). Die Bestimmungen zu den Verfahren sowie den Voraussetzungen bezüglich der Erteilung eines kurzfristigen Visums sind der Verordnung (EG) Nr. 810/2009 (Visakodex) zu entnehmen.[601] Der Beschluss 2008/633/JI (VIS-Beschluss) regelt ferner die Möglichkeit von bestimmten Strafverfolgungsbehörden sowie Europol, zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten Zugriff auf das VIS zu beantragen.[602]

Da sich das Umfeld der gemeinsamen Visapolitik insbesondere aufgrund von migrations- und sicherheitspolitischen Herausforderungen stark verändert hatte, erarbeitete die Kommission einen Vorschlag, welcher zwei neue Verordnungen enthielt. Dieser Vorschlag bezweckte die Visumantragsverfahren zu erleichtern, die Kontrollen an den Aussengrenzen sowie auf dem Hoheitsgebiet der Schengen-Staaten zu vereinfachen und zu stärken sowie den Austausch von Informationen von Drittstaatangehörigen, welche über ein Visum für einen längerfristigen Aufenthalt verfügen resp. im Besitz von Aufenthaltstiteln sind, zu vereinfachen. Neu sollten also auch die Angaben rund um die Ausstellung von längerfristigen Visa sowie Aufenthaltstiteln im VIS erfasst werden.[603] Dadurch sollte eine Lücke geschlossen werden, da bislang keine

600 Siehe dazu Art. 2 VIS-VO. Auffällig ist, dass nicht alle diese Ziele primär mit der Visapolitik zusammenhängen. Siehe dazu kritisch VAVOULA, EU immigration databases, 226 f. m.w.H. Vgl. zur Anwendung des VIS im Dublin-Bereich auch Art. 12 Dublin-III-VO. So stellt die Ausstellung eines Schengen-Visums ein Kriterium bei der Bestimmung des zuständigen Dublin-Staates eines Asylgesuchs dar. Mit der Abfrage der Asylbehörden im VIS kann verhindert werden, dass dieses Zuständigkeitskriterium umgangen werden kann. Vgl. dazu BUNDESRAT, Botschaft VIS, 4259 f. Siehe zur Nutzung des VIS für die Zwecke des Dublin-Verfahrens auch EJPD, GPK-Bericht 2022, 13 f.

601 GLOOR SCHEIDEGGER, 144 f.; THÜR, 962; SCHWEIZER, Datenschutzrechte, Rz. 3. Vgl. dazu jedoch auch Art. 6 Schengener Grenzkodex; Art. 3 VEV.

602 Siehe dazu Art. 1 VIS-Beschluss.

603 Der Einbezug von Personen mit längerfristigen Visa sowie Aufenthaltstiteln in den Anwendungsbereich des VIS führt dazu, dass eine weitere Personengruppe von Drittstaatsangehörigen systematisch überwacht wird. Vgl. dazu VAVOULA, Right to Private Life, 249 f.

solchen Informationen erhoben werden.[604] Diese beiden Verordnungen, die VO 2021/1133 und die VO 2021/1134, wurden im Juli 2021 verabschiedet und sind bereits in Kraft getreten. Sie gelten jedoch erst vollständig ab dem von der Kommission noch zu bestimmenden Zeitpunkt der Inbetriebnahme.[605]

6.2. Betrieb und Aufsicht

Das VIS besteht aus einem zentralen Informationssystem (C-VIS)[606], einer nationalen Schnittstelle in jedem Schengen-Staat sowie einer Kommunikationsinfrastruktur zwischen dem zentralen VIS und den nationalen Schnittstellen.[607] Über diese nationalen Schnittstellen wird das VIS mit dem nationalen System verbunden. Jeder Schengen-Staat hat eine zuständige Behörde zu benennen, welche mit der nationalen Schnittstelle verbunden wird und den Zugang der zugriffsberechtigten Behörden zum VIS gewährleistet.[608]

Das VIS wird von eu-LISA betrieben. Es kann rund um die Uhr auf das System zugegriffen werden.[609] Die Überwachung wird vom EDSB resp. von den nationalen Kontrollstellen wahrgenommen. Im Rahmen ihrer jeweiligen Zuständigkeit arbeiten der EDSB und die nationalen Kontrollstellen zusammen.[610] Im Sinne einer Koordination zwischen dem EDSB sowie den nationalen Datenschutzbehörden wurde zudem die Koordinierungsgruppe VIS (VIS SCG) geschaffen.[611]

---

604 Siehe zu den Einzelheiten Europäische Kommission, COM(2018) 302 final; Fiolka/Stalder, 178 f. Siehe dazu auch HLEG, final report, 25 ff.

605 Siehe dazu Art. 12 VO 2021/1134; Art. 6 VO 2021/1133; eu-LISA, VIS report 2022, 7 f. m.w.H. zu den Neuerungen. Siehe zu diesen beiden Verordnungen sowie dem Zeitpunkt der Inbetriebnahme <https://www.sem.admin.ch/sem/de/home/sem/rechtsetzung/vo-vis-reform.html#:~:text=Allgemein,dieser Weiterentwicklungen des Schengen-Besitzstands>, zuletzt besucht am 07.3.2025.

606 Im EU-Recht wird das zentrale Informationssystem «CS-VIS» genannt (siehe z.B. in Art. 27 VIS-VO). In der Schweiz hingegen «C-VIS» (Art. 1 lit. c VISV). Um Missverständnisse zu vermeiden, wird in der vorliegenden Untersuchung der Begriff C-VIS verwendet.

607 Anders als bei Eurodac und dem SIS fehlt beim VIS eine klare Bestimmung zur Struktur des Systems. Siehe dazu Art. 26 Abs. 1 VIS-VO; Art. 45 VIS-VO; Art. 1 Abs. 2 Entscheidung 2004/512/EG.

608 Art. 28 VIS-VO.

609 Gloor Scheidegger, 144 f.; eu-LISA, VIS report 2018, 7.

610 Art. 42 f. VIS-VO. Siehe dazu auch Gloor Scheidegger, 149 f.

611 Lobsiger/Gloor Scheidegger, 323. Siehe zur VIS SCG auch <https://edps.europa.eu/data-protection/european-it-systems/visa-information-system_de>, zuletzt besucht am 07.03.2025.

6.3. Beteiligung der Schweiz

Die VIS-VO sowie auch den VIS-Beschluss hat die Schweiz als Schengen-Weiterentwicklungen übernommen.[612] Zur Umsetzung bedurfte es einiger Anpassungen im nationalen Recht.[613] Auch die beiden EU-Verordnungen zur Reform des VIS stellen Schengen-Weiterentwicklungen dar, weshalb diese ebenfalls von der Schweiz übernommen wurden.[614] Für die Umsetzung der Verordnungen VO 2021/1133 und VO 2021/1134 mussten ebenfalls einige gesetzliche Anpassungen auf nationaler Ebene vorgenommen werden.[615]

In der Schweiz ist – vorbehalten der Zuständigkeiten des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) sowie der kantonalen Migrationsbehörden – das SEM für die Bewilligung oder Verweigerung der Einreise in die Schweiz zuständig. Dieses fungiert ebenfalls als zuständige Behörde, welche die nationalen Visumbehörden mit der nationalen Schnittstelle verbindet. Des Weiteren trägt das SEM die Verantwortung für das nationale Visa-Informationssystem ORBIS.[616] In dieser nationalen Datenbank werden die Angaben zu den Visagesuchen erfasst, gespeichert und im Rahmen der VIS-VO an die Zentraleinheit des VIS übermittelt. Die Datenübermittlung an das C-VIS erfolgt automatisch, sofern die Daten in Anwendung der VIS-VO erfasst wurden. Dies betrifft auch alle Änderungen und Löschungen von Daten.[617] Durch das ORBIS wird zudem der Zugang zu den im zentralen VIS gespeicherten Daten ermöglicht.[618]

Die Datenübermittlung an das zentrale VIS wird vom EDÖB überwacht, welcher seine Aufsichtstätigkeit mit den kantonalen Datenschutzbehörden koordiniert. Der EDÖB fungiert ferner auch als nationale Ansprechstelle für die Zusammenarbeit mit dem EDSB.[619]

---

612 Vgl. dazu BUNDESRAT, Botschaft VIS.

613 Siehe dazu BUNDESRAT, Botschaft VIS, 4256 ff. m.w.H.

614 Siehe dazu Notenaustausch VO 2021/1133; Notenaustausch VO 2021/1134.

615 Vgl. zu den Einzelheiten BUNDESRAT, Botschaft VIS Recast.

616 Vgl. dazu Art. 111*b* Abs. 1 AIG; Art. 35-39 VEV; Art. 3 VISV; Art. 28 Abs. 2 VIS-VO.

617 Art. 5 VISV.

618 Art. 4 VISV. Siehe zu einer Übersicht über die von der Schweiz im Jahr 2022 bearbeiteten Schengen-Visa EJPD, GPK-Bericht 2023, 12.

619 Ausserdem führt der EDÖB Kontrollen bei den Auslandvertretungen durch. Vgl. zum Ganzen Art. 37 VISV; GLOOR SCHEIDEGGER, 149 f.

6.4. Gespeicherte Daten

Ist ein Gesuch für ein Schengen-Visum zulässig, wird grundsätzlich unverzüglich ein Antragsdatensatz im VIS erstellt.[620] Dieser besteht u.a. aus bestimmten Angaben zur Person, welche um ein Visum ersucht. Es handelt sich dabei um den Vor- und Nachnamen, das Geschlecht, die Angaben zur Geburt, die Staatsangehörigkeit, die Angaben zum geplanten Aufenthalt, den Wohnort, die aktuelle Beschäftigung und den Arbeitgeber der gesuchstellenden Person. Abgesehen davon werden auch Einzelheiten zum beantragten Visum sowie Informationen betreffend die natürliche oder juristische Person, welche die gesuchstellende Person eingeladen resp. sich dazu verpflichtet hat, für die Kosten des Lebensunterhalts während der Zeitdauer des Aufenthalts der gesuchstellenden Person aufzukommen, erfasst. Des Weiteren werden auch die Fingerabdruckdaten abgenommen sowie ein Foto erstellt.[621]

Im Rahmen der Bearbeitung des Antrags wird das Vorliegen der Einreisevoraussetzungen geprüft und eine Risikobewertung vorgenommen. Dabei wird u.a. auch das SIS abgefragt.[622]

Je nachdem wie die Visumbehörden über den Antrag entscheiden, wird der Antragsdatensatz um weitere Angaben ergänzt.[623] Wird ein Antrag gutgeheissen, wird u.a. die Gültigkeitsdauer sowie die Anzahl der erlaubten Einreisen in das im Visum bezeichnete Gebiet in der Datenbank gespeichert.[624] Im Falle einer Ablehnung des Antrags wird hingegen insbesondere der Grund für die Ablehnung erfasst.[625] Abgesehen davon werden auch allfällige Verknüpfungen zu anderen Anträgen gespeichert. Die über die Infrastruktur des VIS übermittelten Mitteilungen werden jedoch nicht gespeichert.[626]

---

620 Art. 8 Abs. 1 VIS-VO. Siehe die Abs. 2-4 derselben Bestimmung zur Verknüpfung mit Antragsdatensätzen von früheren Gesuchen derselben Person resp. mit solchen von gemeinsam reisenden Personen.

621 Art. 9 VIS-VO. Es wird kritisiert, dass im VIS auch Daten von Drittpersonen gespeichert werden, also z.B. von Personen, welche die gesuchstellende Person eingeladen haben. Durch den Zugriff von nationalen Strafverfolgungsbehörden (sowie Europol) können diese Daten auch diesen Behörden zugänglich gemacht werden. Die Erhebung solcher Daten erscheint deshalb unverhältnismässig. Siehe dazu VAVOULA, Right to Private Life, 260.

622 Siehe dazu Art. 21 Visakodex. Ist die gesuchstellende Person im SIS zur Einreiseverweigerung ausgeschrieben, wird das beantragte Visum grundsätzlich verweigert. Siehe dazu Art. 32 Abs. 1 lit. a v) Visakodex. Der Grund für die Ablehnung ist im VIS zu erfassen. Siehe dazu Art. 12 Abs. 2 Bst. f VIS-VO.

623 Art. 10-14 VIS-VO.

624 Art. 10 VIS-VO.

625 Art. 12 VIS-VO.

626 Art. 5 VIS-VO.

Die im Zusammenhang mit der COVID-19-Pandemie erlassenen Reiserestriktionen führten – zusammen mit der automatischen Löschung von gespeicherten Daten im VIS – zu einem erstmaligen Rückgang der gespeicherten Daten in der Datenbank. So waren im Jahr 2019, also vor dieser Pandemie, 77 Millionen Visagesuche sowie 68 Millionen Fingerabdruck-Sets im VIS gespeichert.[627] Im Jahr 2022 waren es nur noch 57 Millionen Visagesuche und 52 Millionen Fingerabdruck-Sets. Im Jahr 2023 war ein weiterer Rückgang zu verzeichnen. So waren in diesem Jahr noch 51 Millionen Visagesuche und 47 Millionen Fingerabdruck-Sets im VIS gespeichert.[628]

Die Aufbewahrungsdauer der Antragsdatensätze beträgt höchstens fünf Jahre, wobei nach Ablauf dieser Frist die Antragsdatensätze samt allfälliger Verknüpfungen automatisch gelöscht werden.[629] Eine vorzeitige Löschung ist bei Erlangen der Staatsangehörigkeit eines Schengen-Staates vorgesehen sowie wenn eine Beschwerdeinstanz die Ablehnung des Visums aufgehoben hat und dieser Entscheid rechtskräftig ist.[630] Aus dem VIS gezogene Daten dürfen von den Schengen-Staaten nur unter der Bedingung der Erforderlichkeit in nationalen Datenbanken, also in der Schweiz u.a. im ORBIS, gespeichert werden.[631] Über die im VIS gespeicherten Daten kann nur derjenige Schengen-Staat verfügen, welcher die Daten in die Datenbank eingegeben hat.[632]

6.5. Zugriffsberechtigung

6.5.1. Visum-, Asyl- sowie Grenzkontrollbehörden

Gemäss der VIS-VO ist eine Vielzahl von Stellen berechtigt, Daten im VIS abzufragen. Die Inbetriebnahme der Informationssysteme EES und ETIAS wird zudem noch weitere Abfragemöglichkeiten eröffnen. Bei den zugangsberech-

627 EU-LISA, VIS report 2022, 21.

628 EU-LISA, VIS report 2024, 5.

629 Art. 23 VIS-VO.

630 Art. 25 VIS-VO.

631 Art. 30 VIS-VO; Art. 29 Abs. 1 VISV.

632 Hat ein Schengen-Staat Kenntnis von Anhaltspunkten, welche nahelegen, dass im VIS erfasste Daten unrichtig sind oder widerrechtlich bearbeitet werden, informiert dieser Schengen-Staat den verantwortlichen Schengen-Staat. Dieser hat eine entsprechende Überprüfung vorzunehmen und berichtigt resp. löscht die Daten unverzüglich, sofern dies angezeigt ist. Siehe dazu Art. 24 VIS-VO.

tigten nationalen Behörden handelt es sich insbesondere um Visum-, Asyl- sowie Grenzkontrollbehörden.[633]

In der Schweiz sind im Rahmen des Visumverfahrens gewisse Abteilungen des SEM, die schweizerischen Vertretungen im Ausland und die Missionen sowie die zuständigen kantonalen Migrationsbehörden und die Gemeindebehörden abfrageberechtigt. Bestimmte Einheiten des SEM sind auch bei der Durchführung eines Asylverfahrens berechtigt, Abfragen im VIS durchzuführen. Zudem verfügen das Grenzwachtkorps sowie die kantonalen und kommunalen Polizeibehörden bei der Ausübung bestimmter Tätigkeiten über eine Abfrageberechtigung.[634]

Der Zugang dieser Behörden zum VIS ist jeweils auf bestimmte Daten beschränkt.[635] So haben fast alle zugriffsberechtigten Behörden Einsicht in das Foto der gesuchstellenden Person, der Zugriff auf die Fingerabduckdaten ist jedoch lediglich einzelnen Stellen vorbehalten.[636] Grundsätzlich gilt, dass die Verwendung des VIS im Rahmen der Tätigkeiten der zugriffsberechtigten Behörden stets erforderlich, geeignet und angemessen sein muss. Des Weiteren haben die zuständigen Behörden sicherzustellen, dass die betroffenen Personen nicht diskriminiert und deren Menschenwürde sowie Integrität uneingeschränkt geachtet werden.[637]

Im Jahr 2019 wurden 25 Millionen alphanumerische und sieben Millionen biometrische Abfragen im VIS vorgenommen.[638] In den folgenden zwei Jahren haben diese Abfragen deutlich abgenommen. Dieser Rückgang ist auf die COVID-19-Pandemie zurückzuführen.[639] Im Jahr 2023 war die Anzahl der biometrischen Abfragen mit derjenigen im Jahr 2019 vergleichbar. Alphanumerische Abfragen wurden im Jahr 2023 immer noch weniger als noch vor der Pandemie vorgenommen.[640]

633 Siehe zum Ganzen Art. 6, Art. 15 und Art. 17a ff. VIS-VO. Auch wenn grundsätzlich sowohl das Foto als auch die Fingerabdruckdaten der gesuchstellenden Person von externen Dienstleistungserbringern erhoben werden können, wird diesen kein Zugang zum VIS gewährt. Siehe dazu Art. 40 Abs. 3 Visakodex; Art. 43 Visakodex.

634 Siehe zu den Einzelheiten Art. 109*a* Abs. 2 AIG. Die dort genannten Behörden werden in Art. 11 VISV genauer definiert. Die einzelnen Abfragemöglichkeiten sind in Art. 12 ff. VISV näher geregelt.

635 Art. 11 Abs. 3 VISV.

636 Vgl. dazu Anhang 3 VISV. Anhand der dort aufgeführten Tabelle ist ersichtlich, welche Behörde auf welche Daten zugreifen darf.

637 Art. 7 VIS-VO.

638 EU-LISA, VIS report 2020, 17.

639 Siehe dazu EU-LISA, VIS report 2022, 22.

640 EU-LISA, VIS report 2024, 19.

6.5.2. Nationale Strafverfolgungsbehörden

Bestimmte nationale Strafverfolgungsbehörden sind ebenfalls berechtigt, zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer[641] und sonstiger schwerwiegender Straftaten[642], Einsicht in VIS-Daten zu verlangen.[643] Ein in schriftlicher oder elektronischer Form begründeter Antrag auf Zugang zum VIS ist an die von den Schengen-Staaten benannte zentrale Zugangsstelle zu richten. Diese überprüft die Einhaltung der Voraussetzungen einer solchen Einsichtnahme. Zur Gewährung des Zugangs müssen drei Voraussetzungen erfüllt sein. So muss der Zugang zu den Daten für die Verhütung, Aufdeckung oder Ermittlung terroristischer oder sonstiger schwerwiegender Straftaten erforderlich sein, die Datenabfrage muss im Einzelfall erforderlich sein und es müssen berechtigte Gründe für die Annahme vorliegen, dass die Abfrage im VIS erheblich zur Verhütung, Aufdeckung oder Ermittlung einer der genannten Straftaten beitragen wird. Sind diese Voraussetzungen erfüllt, wird das VIS von der zentralen Zugangsstelle abgefragt. Diese Abfrage kann nur anhand von bestimmten Angaben vorgenommen werden (bspw. anhand der Fingerabdrücke). Bei einem Treffer erhält die um Einsicht ersuchende Behörde Zugriff auf alle Daten des Visa-Antragsformular der Person, deren Daten für die Abfrage verwendet worden sind. Zudem können auch Fotos sowie allfällige Daten von einem früheren Visumgesuch eingesehen werden. Aus Dringlichkeitsgründen kann in Ausnahmefällen die Überprüfung durch die zentrale Zugangsstelle auch erst nach der Abfrage im VIS erfolgen, wobei diese nachträgliche Überprüfung auch die Beurteilung umfasst, ob ein dringender Ausnahmefall tatsächlich vorgelegen hatte.[644]

---

641 Siehe zur Definition Art. 2 Abs. 1 Bst. c VIS-Beschluss. In der Schweiz sind die terroristischen Straftaten in Anhang 1a N-SIS-Verordnung aufgeführt.

642 Siehe zur Definition Art. 2 Abs. 1 Bst. d VIS-Beschluss. In der Schweiz sind die sonstigen schweren Straftaten dem Anhang 1b N-SIS-Verordnung zu entnehmen.

643 In diesem Zusammenhang wird von den «*benannten Behörden*» gesprochen. Die Schengen-Staaten benennen ihre zugriffsberechtigten Behörden und melden diese der EU. Auf EU-Ebene wird eine entsprechende Liste mit diesen Behörden geführt (siehe dazu Art. 3 VIS-Beschluss). Es wird kritisiert, dass den Schengen-Staaten bei der Benennung dieser Staaten ein (zu) grosses Ermessen zukommt. Die auf der Liste aufgeführten Behörden sind häufig nur sehr ungenau bezeichnet. Teilweise wird lediglich in allgemeiner Weise auf ein Departement verwiesen oder es werden Behörden genannt, welche nicht in der Strafverfolgung tätig sind. Das Risiko von Missbrauch sowie Missverständnissen bei der Benennung der Behörden ist somit gross. Eine Kontrolle durch die EU wäre deshalb angezeigt. Siehe zur Kritik VAVOULA, Assessment, 168 ff.; VAVOULA, Deathblow, 148 f.; VAVOULA, EU immigration databases, 228.

644 Siehe dazu Art. 4 f. VIS-Beschluss; THÜR, 963 f.

In der Schweiz fungiert die Einsatzzentrale fedpol (EZ fedpol) als zentrale Zugangsstelle, welche die Anträge der berechtigten nationalen Stellen um Einsicht in das VIS prüft. Grundsätzlich können bestimmte Abteilungen bei fedpol, beim NDB sowie der Bundesanwaltschaft, aber auch die kantonalen Polizei- und Strafverfolgungsbehörden sowie gewisse kommunale Polizeibehörden (Zürich, Winterthur, Lausanne, Chiasso und Lugano) einen Antrag auf Einsicht in das VIS stellen.[645]

Nicht alle Schengen-Staaten machen von dieser Zugriffsmöglichkeit Gebrauch. Diejenigen, die es tun, darunter auch die Schweiz, haben im Zeitraum vom Oktober 2021 bis September 2023 knapp 32'000 solcher Abfragen durchgeführt (dabei sind auch die Abfragen von Europol berücksichtigt). In dieser Zeitspanne wurden 130 dringende Fälle registriert. 26 davon wurden nachträglich als nicht dringend bewertet.[646] Die Schweiz hat im Jahr 2022 769 Abfragen des VIS zu Strafverfolgungszwecken vorgenommen. Dies ist eine merkliche Zunahme im Vergleich zum Vorjahr, in welchem lediglich 312 Abfragen getätigt worden sind. In den beiden Jahren zuvor war jedoch eine ähnlich hohe Anzahl von Abfragen verzeichnet worden (2020: 864, 2019: 778).[647]

6.5.3. Europol

Abgesehen von den bezeichneten nationalen Strafverfolgungsbehörden kommt auch Europol im Rahmen der Wahrnehmung seiner Aufgaben ein Einsichtsrecht in die VIS-Daten zu.[648] Europol wurde im Oktober 2022 an das VIS angeschlossen.[649]

645 Art. 109*a* Abs. 3-4 AIG. Diese Behörden werden in Art. 17 f. VISV noch genauer definiert. Vgl. zu den Einzelheiten des Verfahrens Art. 19 ff. VISV.

646 EU-LISA, VIS report 2024, 22. In der vorangehenden Berichtsperiode war die Anzahl der Abfragen leicht erhöht (über 35'000 Abfragen). Auch wurden mehr dringende Fälle registriert (418, wobei 65 davon nachträglich als nicht dringend bewertet wurden). Siehe dazu EU-LISA, VIS report 2022, 26 f.

647 EJPD, GPK-Bericht 2023, 9.

648 Vgl. Art. 7 VIS-Beschluss.

649 EU-LISA, VIS report 2024, 22.

6.6. Ausgewählte Sicherheitsmassnahmen

6.6.1. Übermittlung von VIS-Daten an Drittstaaten und internationale Organisationen

VIS-Daten dürfen grundsätzlich nicht an Drittstaaten oder internationale Organisationen weitergeleitet werden. Ausnahmen sind jedoch explizit unter gewissen Voraussetzungen vorgesehen.[650]

6.6.2. Protokollierungspflicht

Die Schengen-Staaten sowie eu-LISA haben ihre jeweiligen Datenbearbeitungen zu protokollieren. Diese Protokolle dienen der Überprüfung der Zulässigkeit der Datenbearbeitung sowie der Gewährleistung der Datensicherheit.[651]

6.6.3. Rechte der betroffenen Personen

Bei der Erfassung der Daten für das Antragsformular, des Fotos und der Fingerabdrücke ist die antragstellende Person über verschiedene Aspekte der weiteren Verwendung dieser Angaben zu informieren.[652] Diese Informationspflicht umfasst u.a. die Bekanntgabe des für die Datenbearbeitung Verantwortlichen, der Zwecke der Bearbeitung im VIS, der Kategorien der Datenempfänger sowie der Speicherdauer der Daten. Ausserdem muss darüber informiert werden, dass die Schengen-Staaten und Europol zwecks Gefahrenabwehr und Strafverfolgung auf das VIS zugreifen dürfen und dass die Erhebung der Daten für die Bearbeitung des Gesuchs vorgeschrieben ist. Des Weiteren ist den betroffenen Personen darzulegen, dass sie über bestimmte Rechte verfügen. Dabei handelt es sich um das Recht auf Auskunft, Berichtigung und Löschung.[653] Gegen die Verweigerung eines solchen Rechts können die betroffenen Personen Klage erheben.[654] In der Schweiz kann für die Gel-

650 Siehe dazu Art. 8 Abs. 4 VIS-Beschluss; Art. 31 VIS-VO.

651 Siehe dazu Art. 34 VIS-VO. Vgl. dazu auch Art. 34a VIS-VO.

652 Die Informationspflicht besteht nicht nur gegenüber der antragstellenden Person, sondern auch gegenüber der natürlichen resp. juristischen Person, welche die gesuchstellende Person eingeladen hat resp. sich verpflichtet hat, für die Kosten des Lebensunterhalts während des Aufenthalts aufzukommen.

653 Siehe dazu Art. 37 f. VIS-VO. Siehe zum Recht auf Auskunft, Berichtigung und Löschung betreffend die Datenbearbeitung gemäss dem VIS-Beschluss Art. 14 VIS-Beschluss.

654 Siehe dazu Art. 40 VIS-VO.

tendmachung dieser Rechte beim SEM ein entsprechendes Gesuch eingereicht werden.[655]

6.6.4. Haftung und Sanktionen

Sowohl die VIS-VO als auch der VIS-Beschluss sehen eine Haftungsnorm vor. Gemäss dieser kann eine Person resp. ein Schengen-Staat, welche resp. welcher durch eine rechtswidrige Datenverarbeitung geschädigt wird, Schadenersatz vom verantwortlichen Schengen-Staat verlangen. Letzterer kann sich (teilweise) exkulpieren, sofern ihm der Nachweis gelingt, dass er für den Schaden nicht verantwortlich ist. Des Weiteren haftet ein Schengen-Staat grundsätzlich bei einer Pflichtverletzung für Schäden am VIS. Die Geltendmachung dieser Ansprüche richtet sich nach nationalem Recht.[656] In der Schweiz richtet sich ein entsprechender Haftungsanspruch nach dem VG, insbesondere nach Art. 19*a*-19*c* VG.[657]

Ferner haben die Schengen-Staaten sicherzustellen, dass jeder Missbrauch von in das VIS eingegebenen Daten mittels wirksamer, verhältnismässiger und abschreckender Sanktionen, verwaltungsrechtlicher und/oder strafrechtlicher Art, geahndet wird.[658] In der Schweiz wird mit Busse bestraft, wer zweckwidrig Daten im nationalen Visumsystem oder im VIS bearbeitet.[659]

6.7. Ausblick

Wie bereits erwähnt sind die beiden Verordnungen VO 2021/1133 und VO 2021/1134 zwar bereits in Kraft getreten. Sie gelten jedoch grundsätzlich erst ab dem Zeitpunkt, welchen die Kommission für die Inbetriebnahme festlegt.[660] Die beiden Verordnungen werden u.a. die VIS-VO abändern und den VIS-Beschluss aufheben.[661]

---

655 Siehe zu den Einzelheiten Art. 31 VISV. Auf der Webseite des EDÖB stehen verschiedene Musterbriefe für die Wahrnehmung des Rechts auf Auskunft, Berichtigung und Löschung in der Schweiz zur Verfügung. Unter <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/international/schengen_dublin.html> sind diese abrufbar, zuletzt besucht am 07.03.2025.

656 Art. 33 VIS-VO; Art. 10 VIS-Beschluss.

657 Art. 33 VISV.

658 Art. 36 VIS-VO; Art. 12 VIS-Beschluss.

659 Art. 120*d* Abs. 2 lit. a AIG.

660 Siehe dazu Art. 12 VO 2021/1134; Art. 6 VO 2021/1133.

661 Dies geht aus dem vollständigen Titel der beiden Verordnungen hervor.

Das Visumverfahren wird zudem weitere Veränderungen unterlaufen. So sind Schengen-Visumanträge zukünftig über eine elektronische EU-Plattform einzureichen. Diese muss noch entwickelt werden. Damit wird das Visumverfahren digitalisiert. Ausserdem werden zukünftig digitale Visa ausgestellt. Diese werden die bisher verwendete Visummarke in Papierform ablösen. Die beiden Schengen-Weiterentwicklungen, welche diese Veränderungen vorsehen, wurden am 13. November 2023 verabschiedet (die VO 2023/2685 und die VO 2023/2667). Sie sind bereits in Kraft getreten, sind jedoch grösstenteils noch nicht anwendbar. Die Inbetriebnahme ist aktuell für Januar 2028 vorgesehen.[662]

7. Einreise-/Ausreisesystem

7.1. Entstehung

Das EES wurde vor dem Hintergrund der zunehmenden Reisetätigkeit in den Schengen-Raum entwickelt. Bei rund einem Drittel derjenigen Personen, welche regulär die EU-Aussengrenzen überqueren, handelt es sich um Drittstaatsangehörige, welche für einen Kurzaufenthalt in den Schengen-Raum einreisen. Die Kontrolle dieser Personen an der Grenze wurde bis anhin manuell vorgenommen. So wurden die Reisedokumente der Personen abgestempelt und mit dem Datum und dem Ort der Ein- und Ausreise versehen. Anhand dieser Angaben konnten die Grenzkontrollbehörden sowie die Fluggesellschaften überprüfen, ob die zulässige Aufenthaltsdauer eingehalten oder überschritten wurde. Die in diesem Zusammenhang verwendeten Stempel sind jedoch nicht fälschungssicher und zudem oft auch schwer lesbar. Ein elektronisches System sollte deshalb diesen Problemen Abhilfe schaffen.[663]

Mit dem EES sollen zukünftig insbesondere die Ein- und Ausreisen von visumpflichtigen sowie auch visumbefreiten Drittstaatsangehörigen, welche sich für einen Kurzaufenthalt im Schengen-Raum aufhalten, elektronisch erfasst wer-

662 Siehe dazu <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-103115.html>, zuletzt besucht am 07.03.2025. Siehe zur Inkraftsetzung sowie der Anwendbarkeit auch Art. 8 VO 2023/2667; Art. 3 VO 2023/2685. Siehe zu diesen beiden Verordnungen auch <https://www.sem.admin.ch/sem/de/home/sem/rechtsetzung/archiv/vev-digitale-visa.html>, zuletzt besucht am 07.03.2025.

663 BUNDESRAT, Botschaft EES, 184 f.

den.[664] Das EES ist demnach grundsätzlich an den Aussengrenzen der Schengen-Staaten im Einsatz.[665] Es soll das bisherige Abstempeln der Reisedokumente ersetzen.[666]

Mit dem EES wird ein umfangreicher Katalog von Zielen verfolgt. Im Wesentlichen wird damit ein besseres Management der Aussengrenzen, die Reduktion von irregulärer Migration sowie die Eindämmung von terroristischen Aktivitäten sowie schwerer Kriminalität bezweckt. Insgesamt sollen die Grenzkontrollen verstärkt automatisiert durchgeführt werden. Auch soll der Dokumenten- und Identitätsbetrug besser entdeckt werden können.[667]

Dem EES sollen zudem auch wichtige Informationen zur Visapolitik entnommen werden können. So kann anhand der darin gespeicherten Daten untersucht werden, ob bestimmte Staatsangehörige Auffälligkeiten in Bezug auf das Überschreiten der zulässigen Aufenthaltsdauer aufweisen. Dies könnte sich auf die Visumpflicht der Staatsangehörigen dieser Staaten auswirken. Ferner können anhand der Daten auch die Auswirkungen von Visaliberalisierungsabkommen mit Drittstaaten beurteilt werden.[668]

Für die Errichtung des EES wurde die VO 2017/2226 (EES-VO) geschaffen. Zudem wurden mit der VO 2017/2225 Änderungen der VO 2016/399 (Schengener Grenzkodex) vorgenommen.[669] Diese rechtlichen Bestimmungen sind zwar bereits in Kraft getreten.[670] Die Inbetriebnahme des EES steht jedoch noch aus.[671] Das EES wird ab Oktober 2025 gestaffelt in Betrieb genommen werden.[672]

---

664 Europäische Kommission, COM(2016) 205 final, 14; Schweizer, wirksame Beschwerde, 74 f. Siehe zum genauen Anwendungsbereich Art. 2 EES-VO.

665 Art. 4 Abs. 1 EES-VO. Siehe in den Abs. 2-5 die Einzelheiten dazu.

666 Ausgenommen davon sind u.a. Reisedokumente für den erleichterten Transit (FTD) sowie für den erleichterten Transit im Eisenbahnverkehr (FRTD). Siehe dazu Bundesrat, Botschaft EES, 199.

667 Europäische Kommission, COM(2016) 205 final, 14; Fiolka/Stalder, 171. Siehe dazu im Einzelnen Art. 6 Abs. 1 EES-VO. Damit verfolgt das EES, wie auch das VIS, eine Vielzahl von Zielen. Siehe dazu Vavoula, Right to Private Life, 245.

668 Bundesrat, Botschaft EES, 186.

669 Bundesrat, Botschaft EES, 180 f. Siehe zu den Einzelheiten VO 2017/2225.

670 Siehe dazu Art. 73 EES-VO sowie Art. 2 Abs. 1 VO 2017/2225.

671 Die Kommission bestimmt den Zeitpunkt der Aufnahme des Betriebs des EES, sobald bestimmte Voraussetzungen erfüllt sind. Siehe dazu Art. 66 Abs. 1 EES-VO.

672 <https://www.consilium.europa.eu/de/meetings/jha/2025/03/05/>, zuletzt besucht am 07.03.2025.

7.2. Betrieb und Aufsicht

Das EES umfasst insbesondere ein Zentralsystem, eine einheitliche nationale Schnittstelle in den Schengen-Staaten, einen sicheren Kommunikationskanal zwischen den Zentralsystemen des VIS und des EES sowie eine sichere und verschlüsselte Kommunikationsinfrastruktur zwischen dem Zentralsystem des EES und den nationalen Schnittstellen.[673] Die Verbindung zwischen dem EES und dem VIS erlaubt gegenseitige Abfragen sowie die Übernahme resp. die Aktualisierung von Daten des jeweils anderen Informationssystems.[674] Ausserdem werden bestimmte Hardware- und Softwarekomponenten der Kommunikationsinfrastruktur des VIS und des EES gemeinsam genutzt, wobei eine logische Trennung sichergestellt wird.[675]

Das EES beinhaltet zudem ein automatisiertes Berechnungssystem, welches die Höchstdauer des zulässigen Aufenthalts aufzeigt. Damit erhält die zuständige Behörde u.a. bei der Einreise eines Drittstaatsangehörigen die Information über die Höchstdauer des zulässigen Aufenthalts sowie die Anzahl der möglichen Einreisen. Ausserdem kann das System bei einer innerstaatlichen Kontrolle Aufschluss über den noch verbleibenden zulässigen Aufenthalt geben. Des Weiteren kann bei der Ausreise überprüft werden, ob die Aufenthaltsdauer überzogen wurde.[676]

Um den Grenzübertritt zu automatisieren haben die Schengen-Staaten grundsätzlich die Möglichkeit, ein Self-Service-System sowie e-Gates[677] bereitzustellen. Mit Hilfe eines Self-Service-Systems können die Reisenden ihre Daten vorerfassen. Bei den e-Gates handelt es sich hingegen um eine elektronisch betriebene Infrastruktureinrichtung, an welcher der eigentliche Grenzübertritt stattfindet. Diese kann von allen Reisenden mit einem Reisepass mit (biometrischem) Chip benutzt werden.[678]

Das EES wurde von eu-LISA entwickelt und wird auch von dieser Agentur betrieben werden.[679] Die Aufsicht über die Datenbearbeitung durch eu-LISA wird vom EDSB wahrgenommen. Dieser arbeitet mit den nationalen Aufsichtsbehörden zusammen. Jeder Schengen-Staat hat eine Aufsichtsbehörde einzuset-

673 Art. 7 Abs. 1 EES-VO.
674 Siehe dazu Art. 8 EES-VO.
675 Art. 7 Abs. 3 EES-VO.
676 Art. 11 Abs. 2 EES-VO.
677 Diese werden teilweise auch «*Automated Border Control–Gates*», oder kurz «*ABC-Gates*», genannt.
678 BUNDESRAT, Botschaft EES, 185 f.
679 Art. 5 EES-VO.

zen, welche die Datenbearbeitung im Schengen-Staat im Zusammenhang mit dem EES überwacht.[680]

7.3. Beteiligung der Schweiz

Die Schweiz hat sowohl die EES-VO sowie auch die VO 2017/2225 übernommen.[681] Die EES-VO ist grösstenteils direkt anwendbar. Dennoch mussten einige Anpassungen auf Gesetzes- sowie auch auf Verordnungsebene vorgenommen werden. So wurde insbesondere das AIG geändert und eine neue nationale Verordnung geschaffen, die Verordnung über das Einreise- und Ausreisesystem (EESV).[682] Ausserdem muss die Grenzkontrollinfrastruktur angepasst werden. Es soll ein IT-System eingeführt werden, welches sich an das EES-Zentralsystem anschliessen lässt.[683]

Da das EES an den Schengen-Aussengrenzen eingesetzt wird, wird das System in der Schweiz an den Flughäfen im Einsatz sein.[684]

Obwohl die Daten aus dem EES – mit Ausnahme der biometrischen Daten – grundsätzlich in einem nationalen System oder nationalen Dateien gespeichert werden dürfen, sofern dabei die vorgesehene Speicherfrist eingehalten wird, beabsichtigt die Schweiz kein solches nationales EES einzuführen.[685]

680 Vgl. dazu Art. 55-57 EES-VO.

681 Siehe dazu Notenaustausch EES-VO; Notenaustausch VO 2017/2225.

682 Insbesondere bedurfte es einer formellen Gesetzesgrundlage im AIG, da im EES besonders schützenswerte Daten (Gesichtsbild und Fingerabdrücke) bearbeitet werden. Siehe dazu BUNDESRAT, Botschaft EES, 191 f. Die konkreten Änderungen im AIG finden sich im Anhang vom Bundesbeschluss vom 21. Juni 2019. Der Bundesrat hat auf der Grundlage von Art. 103*f* AIG zudem die EESV erlassen.

683 Siehe dazu <https://www.sem.admin.ch/sem/de/home/themen/einreise/ees.html>, zuletzt besucht am 07.03.2025.

684 SCHWEIZER, wirksame Beschwerde, 74 f. Der Flughafenstandortkanton kann entscheiden, ob ein automatisiertes Grenzkontrollverfahren in der Form eines e-Gates und eines Self-Service-Systems eingeführt wird. Siehe dazu Art. 103*g* AIG. Vgl. dazu ausserdem BUNDESRAT, Botschaft EES, 216 ff. m.w.H.

685 BUNDESRAT, Botschaft EES, 187. Siehe dazu auch Art. 40 Abs. 1 und 2 EES-VO. Auch von der Möglichkeit von nationalen Erleichterungsprogrammen wird die Schweiz zumindest vorläufig keinen Gebrauch machen. Gemäss diesem Programm können vielreisende Drittstaatsangehörige nach entsprechender Sicherheitsprüfung den Status eines «*registrierten Reisenden*» erlangen. Dies führt zu einer erleichterten Grenzkontrolle. Siehe dazu BUNDESRAT, Botschaft EES, 176 f. und 196 f.

7.4. Gespeicherte Daten

Im EES werden bestimmte Daten von Drittstaatsangehörigen[686] erfasst, welche sich für einen Kurzaufenthalt an einer Grenze, an welcher das EES im Einsatz ist, einer Grenzkontrolle unterziehen müssen. Dabei handelt es sich um Drittstaatsangehörige, welche einer Visumpflicht unterliegen, von einer solchen befreit sind oder welchen die Einreise für einen Kurzaufenthalt verweigert wurde.[687]

Beim Grenzübertritt wird die Identität der Person verifiziert. Ausserdem überprüfen die Grenzkontrollbehörden, ob bereits ein persönliches Dossier der Person angelegt worden ist. Sofern ein solches Dossier bereits vorhanden ist, nimmt der Grenzbeamte ggf. Aktualisierungen vor und erfasst den Einreise- resp. Ausreisedatensatz oder ggf. einen Einreiseverweigerungsdatensatz. Die Ein-/Ausreisedatensätze sowie die Einreiseverweigerungsdatensätze werden mit dem persönlichen Dossier verknüpft. Ist noch kein persönliches Dossier vorhanden, wird ein solches angelegt.[688]

Das persönliche Dossier von visumpflichtigen Drittstaatsangehörigen umfasst folgende Angaben: Nachname, Vorname(n), Staatsangehörigkeit(en), Geschlecht, Art und Nummer des Reisedokuments (inkl. dem dreibuchstabigen Code des ausstellenden Staates), dem Ablaufdatum des Dokuments sowie dem Gesichtsbild.[689] In der Regel wird das Gesichtsbild[690] vor Ort erstellt. Ausnahmsweise kann dieses auch aus dem Chip des elektronischen maschinenlesbaren Reisedokuments gezogen werden.[691] Die Fingerabdruckdaten[692] werden aus dem VIS gezogen. Diese Daten müssen deshalb nicht (noch einmal) erhoben werden.[693]

---

686 Siehe zur Definition Art. 3 Abs. 1 Ziff. 6 EES-VO.

687 Siehe zum genauen Anwendungsbereich Art. 2 EES-VO. Die Art. 16-18 EES-VO regeln die Erhebung der Daten von den aufgeführten Personengruppen.

688 Art. 14 Abs. 1-4 EES-VO. Grenzübertritte können auch in Anwendung eines Self-Service-Systems oder eines e-Gates erfolgen. Siehe dazu Art. 14 Abs. 5-7 EES-VO. Art. 16 Abs. 2-3 EES-VO führen die Angaben auf, welche im Einreise- resp. Ausreisedatensatz zu erfassen sind. Art. 18 Abs. 6 EES-VO nennt die Daten, welche für einen Einreiseverweigerungsdatensatz zu erheben sind.

689 Art. 16 Abs. 1 EES-VO.

690 Dabei handelt es sich um «*eine digitale Aufnahme des Gesichts*». Siehe dazu Art. 3 Abs. 1 Ziff. 17 EES-VO.

691 BUNDESRAT, Botschaft EES, 187 f.; Art. 15 Abs. 1-2 EES-VO.

692 Siehe zur Definition Art. 3 Abs. 1 Ziff. 16 EES-VO.

693 SCHWEIZER, Datenschutzrechte, Rz. 4.

Bei Drittstaatsangehörigen, welche von der Visumpflicht befreit sind, werden zusätzlich zu den auch bei den visumpflichtigen Drittstaatsangehörigen erfassten Daten noch die Fingerabdruckdaten – sofern möglich der rechten Hand – abgenommen.[694] Davon ausgenommen sind Kinder unter zwölf Jahren sowie Personen, welchen aus physischen Gründen keine Fingerabdruckdaten abgenommen werden können. Des Weiteren werden auch bestimmte Angaben im Zusammenhang mit der ETIAS-Reisegenehmigung erfasst.[695]

Wird einer Person die Einreise verweigert, wird ebenfalls ein persönliches Dossier angelegt, sofern noch keines vorhanden ist. Je nachdem, ob die betroffene Person einer Visumpflicht unterliegt oder nicht, werden die entsprechenden zuvor genannten alphanumerischen Daten erfasst. Je nach Grund der Einreiseverweigerung werden zudem auch die biometrischen Daten erfasst.[696]

In den Ein-/Ausreisedatensätzen werden insbesondere der Zeitpunkt sowie der Ort der Ein- und Ausreise der betroffenen Person und die Grenzübergangsstelle erfasst.[697] Der Einreiseverweigerungsdatensatz umfasst hingegen das Datum sowie die Uhrzeit der Einreiseverweigerung, die Grenzübergangsstelle, die die Einreise verweigernde Behörde sowie den Grund für die Einreiseverweigerung.[698]

Ein-/Ausreisedatensätze sowie die Einreiseverweigerungsdatensätze werden grundsätzlich während drei Jahren nach dem Datum der Ausreise resp. der Einreiseverweigerung im Zentralsystem des EES gespeichert. Persönliche Dossiers werden samt den Ein-/Ausreisedatensätzen und Einreiseverweigerungsdatensätzen grundsätzlich während drei Jahren und einem Tag nach dem Datum der letzten Ausreise gespeichert, sofern seither keine Einreise mehr erfolgt ist. Fehlt ein Ausreisedatensatz nach dem Ablauf eines zulässigen Aufenthalts werden die Daten während fünf Jahren nach dem Ende des zulässigen Aufenthalts gespeichert.[699]

---

694 Mit den Fingerabdruckdaten sind – sofern vorhanden – die vier Abdrücke des Zeigefingers, des Mittelfingers, des Ringfingers sowie des kleinen Fingers der rechten Hand gemeint. Ansonsten von der linken Hand. Siehe dazu Art. 3 Abs. 1 Ziff. 16 EES-VO.

695 Siehe dazu Art. 17 EES-VO; BUNDESRAT, Botschaft EES, 187 f. Siehe zu den Angaben der ETIAS-Reisegenehmigung, welche im EES gespeichert werden auch BUNDESRAT, Botschaft ETIAS Consequential Amendments, 64.

696 Vgl. zu den Einzelheiten Art. 18 Abs. 1-5 EES-VO.

697 Art. 16 Abs. 2-3 EES-VO; Art. 17 Abs. 2 EES-VO.

698 Art. 18 Abs. 5 EES-VO. In der Schweiz sind verschiedene Behörden berechtigt, Daten im EES einzugeben resp. zu bearbeiten. Siehe dazu Art. 103c Abs. 1 AIG. Siehe dazu auch BUNDESRAT, Botschaft EES, 210 ff. m.w.H.

699 Vgl. zu den Einzelheiten und den Ausnahmen Art. 34 EES-VO.

7.5. Zugriffsberechtigung

7.5.1. Grenzkontroll-, Visum- sowie Einwanderungsbehörden

Die zugriffsberechtigten Stellen sind von den Schengen-Staaten zu bezeichnen. Dabei handelt es sich grundsätzlich um Grenzkontrollbehörden, Visumbehörden sowie Einwanderungsbehörden.[700] Davon abgesehen sind auch Zugriffe auf das EES im Zusammenhang mit den nationalen Erleichterungsprogrammen sowie dem ETIAS möglich.[701]

Die Grenzkontrollbehörden haben bei der Durchführung von Grenzkontrollen an den Schengen-Aussengrenzen Zugriff auf das EES, wobei insbesondere eine Verifizierung der Identität eines Drittstaatsangehörigen durch einen Vergleich der biometrischen Daten erfolgt, sofern die Suchabfrage im EES positiv verlaufen ist.[702] In der Schweiz ist das Grenzwachtkorps sowie die für die Kontrolle an den Schengen-Aussengrenzen verantwortlichen kantonalen Polizeibehörden abfrageberechtigt.[703] Zudem sind die Grenzkontrollbehörden berechtigt eine Abfrage im EES anhand der Fingerabdruckdaten (ggf. in Verbindung mit dem Gesichtsbild) durchzuführen, um Drittstaatsangehörige zu identifizieren, welche eventuell bereits unter einer anderen Identität im EES erfasst sind oder die Voraussetzungen für die Einreise in das Hoheitsgebiet der Schengen-Staaten resp. den dortigen Aufenthalt nicht (mehr) erfüllen.[704] Solche Abfragen dürfen in der Schweiz das Grenzwachtkorps sowie die kantonalen und kommunalen Polizeibehörden, welche Personenkontrollen durchführen, vornehmen.[705]

Dazu kommen alle Visumbehörden, welche zwecks Prüfung von Visumanträgen eine Abfrage im EES durchführen können. Diese Abfrage erfolgt direkt aus

---

700 Art. 9 EES-VO. Eigentlich war ursprünglich vorgesehen, dass auch die Asylbehörden Zugriff auf das EES erhalten sollten. Dieser wurde jedoch nicht gewährt. Die Schweiz hatte sich für einen solchen Zugriff eingesetzt. Siehe dazu Botschaft EES, 183. Beförderungsunternehmen – in der Schweiz betrifft dies die Fluggesellschaften – haben ebenfalls Zugang zum Web-Dienst zwecks Überprüfung, ob die gemäss dem Visum zulässigen Einreisen bereits in Anspruch genommen worden sind. Die Drittstaatsangehörigen können ebenfalls via eines Web-Dienstes den noch verbleibenden zulässigen Aufenthalt überprüfen. Vgl. dazu Art 13 EES-VO; Botschaft EES, 188.

701 Siehe dazu Art. 25 ff. EES-VO. Mit den nationalen Erleichterungsprogrammen können die Schengen-Staaten für bestimmte Personengruppen eine erleichterte Einreise vorsehen. Siehe dazu Art. 8d Schengener Grenzkodex.

702 Siehe zu den Einzelheiten Art. 23 EES-VO.

703 Art. 103c Abs. 2 lit. a AIG.

704 Siehe dazu Art. 27 EES-VO.

705 Siehe dazu Art. 103c Abs. 2 lit. c AIG.

dem VIS im EES. Sind Daten im EES gespeichert, so erhalten die Visumbehörden Zugang zum persönlichen Dossier sowie den damit verknüpften Ein-/Ausreisedatensätzen und allen Einreiseverweigerungsdatensätzen. Ausserdem wird auch Zugang zum automatischen Berechnungssystem gewährt.[706] Im Visumverfahren in der Schweiz haben verschiedene Behörden Zugriff auf das EES. So das SEM, die schweizerischen Vertretungen im Ausland sowie die Missionen, die Migrationsbehörden der Kantone sowie Gemeinden im Bereich Visa, das Staatssekretariat und die Politische Direktion des EDA sowie das Grenzwachtkorps und die Grenzposten der kantonalen Polizeibehörden.[707]

Einwanderungsbehörden können auf dem Hoheitsgebiet der Schengen-Staaten zwecks Verifizierung der Identität der Drittstaatsangehörigen oder zwecks Überprüfung, ob die Einreisevoraussetzungen in das Hoheitsgebiet der Schengen-Staaten resp. für den dortigen Aufenthalt erfüllt sind, Suchabfragen im EES vornehmen.[708] Davon abgesehen können Einwanderungsbehörden – wie auch die Grenzkontrollbehörden – anhand der Fingerabdruckdaten (ggf. in Verbindung mit dem Gesichtsbild) das EES abfragen, um Drittstaatsangehörige, welche womöglich bereits mit einer anderen Identität im EES erfasst sind, zu identifizieren oder die Voraussetzungen für die Einreise resp. den Aufenthalt nicht (mehr) erfüllen.[709] Diese Zugriffsmöglichkeit besteht sowohl an den Schengen-Aussengrenzen als auch im Hoheitsgebiet der Schengen-Staaten.[710] In der Schweiz gelten das SEM sowie die kantonalen und kommunalen Migrationsbehörden als solche Einwanderungsbehörden.[711]

Der Zugriff bezieht sich jeweils auf die im persönlichen Dossier gespeicherten Daten und den damit verknüpften Ein- und Ausreisedatensätzen sowie den vorhandenen Einreiseverweigerungsdatensätzen.[712] Die Visumbehörden, die Grenzkontrollbehörden an den Aussengrenzen des Schengen-Raums sowie die Migrations- und Polizeibehörden, welche im Hoheitsgebiet der Schweiz Kontrollen durchführen, können auch auf das automatisierte Berechnungssystem im EES zugreifen, um zu klären, ob die zulässige Aufenthaltsdauer überschritten wurde.[713]

---

706 Siehe dazu Art. 24 EES-VO.

707 Art. 103c Abs. 2 lit. b AIG.

708 Siehe im Einzelnen Art. 26 EES-VO.

709 Siehe dazu Art. 27 EES-VO.

710 Siehe dazu BUNDESRAT, Botschaft EES, 212.

711 Siehe dazu Art. 103c Abs. 2 lit. c AIG.

712 Art. 23 Abs. 3 EES-VO; Art. 24 Abs. 3 EES-VO; Art. 26 Abs. 2 EES-VO; Art. 27 Abs. 2 EES-VO.

713 Art. 103c Abs. 3 AIG; BUNDESRAT, Botschaft EES, 212. Siehe zum automatisierten Berechnungssystem Art. 11 EES-VO.

7.5.2. Nationale Strafverfolgungsbehörden

Zwecks Verhütung, Aufdeckung und Untersuchung terroristischer[714] oder sonstiger schwerer Straftaten[715] können auch die von den Schengen-Staaten benannten Behörden Zugang zu EES-Daten beantragen.[716] In der Schweiz handelt es sich hierbei um fedpol, den NDB, die Bundesanwaltschaft, die kantonalen Polizei- und Strafverfolgungsbehörden sowie die Polizeibehörden der Städte Zürich, Winterthur, Lausanne, Chiasso und Lugano.[717]

Die von den Schengen-Staaten benannten nationalen Strafverfolgungsbehörden können bei der zentralen Zugangsstelle – in der Schweiz handelt es sich hierbei um die EZ fedpol[718] – Einsicht in die EES-Daten beantragen. Diese überprüft in der Folge jeweils, ob die folgenden Voraussetzungen für die Zugriffsgewährung erfüllt sind: Der Zugang muss zum Zwecke von Abfragen für die Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schweren Straftaten erforderlich sein. Des Weiteren muss der Zugang im Einzelfall erforderlich und verhältnismässig erscheinen. Abgesehen davon müssen Beweise oder hinreichende Gründe für die Annahme vorhanden sein, dass die Abfrage zur Verhütung, Aufdeckung oder Untersuchung der genannten Straftaten beitragen wird. In bestimmten Fällen – nämlich wenn das EES als Instrument für die Identifizierung von unbekannten Verdächtigen, Straftätern oder mutmasslichen Opfern terroristischer oder sonstiger schwerer Straftaten be-

714 Dabei handelt es sich um national geahndete Straftaten, welche den in der RL 2017/541 aufgeführten Straftaten entsprechen oder gleichwertig sind. Siehe dazu Art. 3 Abs. 1 Ziff. 24 EES-VO. In der Schweiz handelt es sich dabei um die im Anhang 1a N-SIS-Verordnung aufgeführten Straftaten. Siehe dazu Art. 2 Abs. 1 lit. d EESV.

715 Dabei handelt es sich um Straftaten, welche den in Art. 2 Abs. 2 Rahmenbeschluss 2002/584/JI aufgeführten Straftaten entsprechen oder gleichwertig sind, wenn die Straftat nach nationalem Recht mit einer freiheitsentziehenden Strafe oder Sicherungsmassnahme mit einer Höchstdauer von mindestens drei Jahren geahndet wird. Siehe dazu Art. 3 Abs. 1 Ziff. 25 EES-VO. In der Schweiz handelt es sich dabei um die in Anhang 1b der N-SIS-Verordnung aufgeführten Straftaten. Siehe dazu Art. 2 Abs. 1 lit. e EESV.

716 Siehe dazu Art. 29 EES-VO. Der Zugang von nationalen Strafverfolgungsbehörden auf EES-Daten war nicht von Anfang an vorgesehen. Auf Druck der Schengen-Staaten wurde schliesslich eine solche Abfragemöglichkeit gewährt. Siehe dazu VAVOULA, EU immigration databases, 237 f.; MITSILEGAS/VAVOULA, 514. Auch der Umfang des Zugriffs von nationalen Strafverfolgungsbehörden auf das EES sorgte für diverse Diskussionen. So wurde von den Delegationen mehrheitlich eine gewisse Flexibilität gefordert. Die Rechtsdienste des Rates sowie der Kommission sprachen sich jedoch gegen eine allzu offene Regelung aus. Schliesslich könnte eine solche Regelung beim EuGH angefochten und ggf. aufgehoben werden. Siehe dazu BUNDESRAT, Botschaft EES, 182.

717 Art. 103c Abs. 4 AIG. Diese zugriffsberechtigten Stellen werden in Art. 10 EESV präzisiert.

718 Art. 103c Abs. 5 AIG.

nutzt wird – müssen in der Regel zudem Abfragen in den nationalen Datenbanken und bei einer Suchabfrage mit Fingerabdruckdaten eine Abfrage gemäss der Prümer Zusammenarbeit ergebnislos verlaufen sein.[719] Sofern die Voraussetzungen erfüllt sind, erfolgt eine Abfrage im EES durch die zentrale Zugangsstelle, wobei bei einem Treffer die Daten der antragstellenden Behörde zur Verfügung gestellt werden.[720]

Ausnahmen von diesem Verfahren sind in dringenden Fällen möglich. So z.B., wenn eine unmittelbar bevorstehende Lebensgefahr, welche im Zusammenhang mit einer terroristischen Straftat oder einer anderen schweren Straftat steht, abgewendet werden muss. In diesen Fällen erfolgt die Überprüfung der Zugangsvoraussetzungen erst nach der Abfrage im EES. Ebenfalls wird nachträglich geprüft, ob tatsächlich ein dringender Fall vorgelegen hatte. Ergibt die nachträgliche Prüfung, dass auf die EES-Daten eigentlich nicht hätte zugegriffen werden dürfen, sind die zugänglich gemachten Daten wieder zu löschen.[721]

7.5.3. Europol

Abgesehen von den nationalen Strafverfolgungsbehörden ist auch Europol berechtigt, Anträge auf Einsicht in Daten des EES zu stellen. Europol bezeichnet eine seiner operativen Stellen (die sog. benannte Europol-Stelle), welche bei der zentralen Europol-Zugangsstelle Zugang zum EES beantragen kann, um die von den Schengen-Staaten zur Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten ergriffenen Massnahmen zu unterstützen und zu stärken. Diese Zugangsstelle überprüft, ob die notwendigen Voraussetzungen vorliegen.[722]

719 Siehe zum Ganzen Art. 29 EES-VO; Art. 31 EES-VO; Art. 32 EES-VO.

720 BUNDESRAT, Botschaft EES, 212 f.

721 Art. 31 Abs. 2-3 EES-VO.

722 Art. 30 EES-VO. Siehe zu den Voraussetzungen für eine solche Zugriffsgewährung Art. 33 EES-VO.

7.6. Ausgewählte Sicherheitsmassnahmen

7.6.1. Übermittlung von EES-Daten an Drittstaaten, internationale Organisationen und private Stellen

Eine Übermittlung an Drittstaaten, internationale Organisationen sowie private Stellen ist grundsätzlich nicht gestattet. Es sind jedoch Ausnahmen vorgesehen.[723]

In der Schweiz ist z.B. im Sinne einer solchen Ausnahme geregelt, dass das SEM zum Nachweis der Identität eines Drittstaatsangehörigen bei der Rückkehr dieser Person in einen Drittstaat unter bestimmten Voraussetzungen Daten an gewisse Organisationen oder Drittstaaten übermitteln darf.[724]

7.6.2. Protokollierungspflicht

Alle Datenverarbeitungsvorgänge im EES sind von eu-LISA zu protokollieren.[725] Auch die Schengen-Staaten sowie Europol haben eine solche Protokollierungs- resp. Dokumentationspflicht.[726]

7.6.3. Rechte der betroffenen Personen

Personen, deren Daten im EES erfasst werden, sind über verschiedene Aspekte zu informieren. So bspw. darüber, dass die Behörden der Schengen-Staaten sowie auch Europol zwecks Gefahrenabwehr- und Strafverfolgungszwecken auf das EES zugreifen dürfen, dass die Aufnahme des Gesichtsbildes eine Pflicht darstellt oder dass bei den Aufsichtsbehörden eine Beschwerde eingereicht werden kann. Zudem sind die betroffenen Personen auch darüber zu informieren, dass ihnen das Recht zukommt, Zugang zu den eigenen Daten zu erhalten, unrichtige Daten zu berichtigen, unvollständige Daten zu vervollständigen sowie unrechtmässig verarbeitete Daten zu löschen resp. die Bear-

723 Siehe dazu Art. 41 EES-VO. Für den Informationsaustausch mit Staaten, welche sich noch nicht am EES-Betrieb beteiligen oder für welche die EES-VO nicht gilt siehe Art. 42 EES-VO sowie Art. 103*e* AIG.

724 Art. 103*d* Abs. 2 AIG. Siehe dazu auch BUNDESRAT, Botschaft EES, 213 ff. Gemäss Anhang I EES-VO kommen nur Folgende in Frage: UN-Organisationen wie das Flüchtlingshochkommissariat der Vereinten Nationen (UNHCR), die Internationale Organisation für Migration (IOM) und das Internationale Komitee vom Roten Kreuz. Siehe dazu auch BUNDESRAT, Botschaft EES, 214.

725 Art. 46 EES-VO.

726 Art. 59 EES-VO.

beitung derselben zu beschränken.[727] Diese Rechte der betroffenen Personen werden in der EES-VO näher ausgeführt.[728]

7.6.4. Haftung und Sanktionen

Jede Person resp. jeder Schengen-Staat, welcher resp. welchem durch eine rechtswidrige Datenverarbeitung ein materieller oder immaterieller Schaden entstanden ist, kann vom verantwortlichen Schengen-Staat Schadenersatz verlangen. Der angeklagte Schengen-Staat kann sich (teilweise) exkulpieren, wenn ihm der Beweis gelingt, dass er hinsichtlich des eingetretenen Schadens nicht verantwortlich ist. Bei einer Pflichtverletzung haftet der Schengen-Staat für einen Schaden, sofern eu-LISA sowie andere Schengen-Staaten es nicht versäumt haben, angemessene Massnahmen für die Prävention des Schadens oder zu dessen Verringerung zu ergreifen. Für die Geltendmachung dieser Schadenersatzansprüche ist das nationale Recht des beklagten Schengen-Staates einschlägig.[729]

Die rechtswidrige Verwendung von EES-Daten ist zudem mit wirksamen, verhältnismässigen und abschreckenden Sanktionen zu ahnden. Diese haben die Schengen-Staaten im nationalen Recht vorzusehen.[730] In der Schweiz ist diesbezüglich ein Bussgeld vorgesehen.[731]

8. Europäisches Reiseinformations- und -genehmigungssystem

8.1. Entstehung

Wie bereits aufgeführt, werden im Rahmen des VIS die Daten von Drittstaatsangehörigen, welche für einen Kurzaufenthalt im Schengen-Raum ein Visum beantragen müssen, erfasst.[732] Eine grosse Anzahl von Drittstaatsangehörigen ist jedoch von einer solchen Visumpflicht befreit.[733] Um die Schengen-Aussengrenzen aufgrund des steigenden Risikos illegaler Migration und des Terroris-

727 Siehe dazu im Einzelnen Art. 50 Abs. 1 EES-VO.
728 Siehe dazu Art. 52 ff. EES-VO.
729 Art. 45 EES-VO.
730 Art. 48 EES-VO.
731 Art. 120*d* Abs. 2 lit. b AIG.
732 Siehe zum VIS Kapitel III.6.
733 Siehe dazu Anhang II VO 2018/1806.

mus besser zu schützen, wurde das Informationssystem ETIAS geschaffen.[734] Mit der verstärkten Kontrolle von visumbefreiten Drittstaatsangehörigen wird ein ausgewogenes Verhältnis zwischen der Reisemöglichkeit der betroffenen Personen sowie der Erhöhung der Sicherheit angestrebt.[735] In den USA, Australien und Kanada gibt es bereits ähnliche Systeme.[736]

ETIAS verfolgt verschiedene Ziele. So soll u.a. durch die Risikoprüfung der Personen vor deren Einreise in den Schengen-Raum ein Beitrag zu einem hohen Mass an Sicherheit, zur Verhinderung illegaler Einwanderung sowie zum Schutz der öffentlichen Gesundheit geleistet werden. Davon abgesehen soll auch die Wirksamkeit der Grenzübertrittskontrollen erhöht und die Erreichung der Ziele des SIS in Bezug auf bestimmte Ausschreibungskategorien sowie der Ziele des EES unterstützt werden. Hinzu kommt, dass mit dem ETIAS auch ein Beitrag zur Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten und zur korrekten Identifizierung von Personen geleistet werden soll.[737]

Mit der Einführung des ETIAS werden insbesondere von der Visumpflicht befreite Drittstaatsangehörige verpflichtet, vor einer Reise in den Schengen-Raum online eine Reisegenehmigung zu beantragen.[738] Diese kostet sieben

734 Fiolka/Stalder, 168 f. Bereits im Jahr 2008 wurde über die Einführung eines EU-ESTA, einem in den USA eingeführten ähnlichen System, diskutiert. Letztlich wurde dieses jedoch wegen Zweifeln an der Notwendigkeit eines solchen Systems verworfen. Trotz des Potentials für die Sicherheit der Schengen-Staaten wurde die umfangreiche Erhebung der personenbezogenen Daten als nicht gerechtfertigt betrachtet. Nach der Visabefreiung von verschiedenen Drittstaaten sowie unter Berücksichtigung von verschiedenen terroristischen Attentaten in Europa in den Jahren 2015 und 2016 lebte diese Idee jedoch wieder auf. Siehe dazu Alegre/Jeandesboz/Vavoula, 14 ff.; Vavoula, Right to Private Life, 246; European Commission, COM(2011) 680 final, 7; Europäische Kommission, COM(2016) 205 final, 15 f.

735 Bundesrat, Botschaft ETIAS, 2892.

736 Europäische Kommission, COM(2016) 602 final, 10 f.

737 Vgl. dazu Art. 4 ETIAS-VO.

738 Siehe zum genauen Anwendungsbereich Art. 2 ETIAS-VO (vgl. Art. 24 ETIAS-VO zu den Sonderbestimmungen von bestimmten Personengruppen). Gemäss dieser Bestimmung wird der Anwendungsbereich u.a. auf visumbefreite Drittstaatsangehörige beschränkt, welche sich zwecks eines kurzfristigen Aufenthalts in den Schengen-Raum begeben wollen. Eine solche Beschränkung findet sich jedoch weder in den ErwG. der ETIAS-VO (siehe z.B. ErwG. 5) noch in den Ausführungen zum Vorschlag der ETIAS-VO (siehe dazu Europäische Kommission, ETIAS-Vorschlag, 7). Fraglich erscheint, ob visumbefreite Drittstaatsangehörige, welche für einen längerfristigen Aufenthalt in den Schengen-Raum einreisen möchten, keine ETIAS-Reisegenehmigung beantragen müssen. Offenbar stellte die Kommission bereits klar, dass es notwendig sei, dass auch solche visumbefreite Drittstaatsangehörige, eine ETIAS-Reisegenehmigung beantragen sollten. Ansonsten hätte dies

Euro und ist maximal drei Jahre gültig.[739] Sie gilt grundsätzlich für den gesamten Schengen-Raum.[740]

Bei der Antragstellung sind verschiedene Angaben zur antragstellenden Person zu machen und diverse Fragen zu beantworten.[741] Ausserdem wird u.a. ein vollständig automatisierter Abgleich mit den im SIS, EES, VIS, Eurodac, ECRIS-TCN und in zwei Interpol-Datenbanken[742] gespeicherten Daten sowie den Europol-Daten vorgenommen.[743] Letztlich erfolgt eine Einschätzung darüber, ob die betroffene Person ein Sicherheitsrisiko[744] darstellt, die Gefahr einer illegalen Einwanderung[745] besteht oder ein hohes Epidemierisiko[746] mit der Einreise der Person verbunden ist.[747]

Mit einer erteilten ETIAS-Reisegenehmigung wird die Einreise in den Schengen-Raum jedoch nicht garantiert.[748] Vielmehr handelt es sich dabei um eine neue Einreisebedingung, welche neben den übrigen Einreisevoraussetzungen gemäss dem Schengener Grenzkodex den visumbefreiten Drittstaatsangehörigen auferlegt wird.[749] Kann keine gültige Reisegenehmigung vorgezeigt werden, dürfen Beförderungsunternehmen diese Personen nicht befördern. Ausserdem wird solchen Personen die Einreise in den Schengen-Raum am Grenzübergang verweigert.[750]

---

zur Folge, dass diese Personengruppe von den Beförderungsunternehmen mangels einer ETIAS-Reisegenehmigung abgewiesen würde. Siehe dazu BUNDESRAT, Botschaft ETIAS Consequential Amendments, 50 f. m.w.H.

739 BUNDESRAT, Botschaft ETIAS, 2905. Gewisse Personen sind von dieser Reisegenehmigungsgebühr befreit. Siehe dazu Art. 18 Abs. 2 ETIAS-VO. Beim ETIAS handelt es sich um das erste System der Schengen-Kooperation, für welches Gebühren auf EU-Ebene erhoben werden. Damit sollen die Betriebs- sowie Unterhaltskosten komplett gedeckt werden können. Vgl. dazu BUNDESRAT, Botschaft ETIAS, 2893. Siehe zu den Modalitäten der finanziellen Beteiligung der assoziierten Staaten BUNDESRAT, Botschaft ETIAS, 2893 f.

740 In Ausnahmefällen kann die Reisegenehmigung räumlich und zeitlich begrenzt werden. Siehe dazu BUNDESRAT, Botschaft ETIAS, 2919; Art. 44 ETIAS-VO.

741 Siehe dazu Art. 17 ETIAS-VO.

742 Dabei handelt es sich um die Interpol-Datenbanken SLTD sowie TDAWN.

743 Siehe zu den Einzelheiten Art. 19 f. ETIAS-VO.

744 Siehe zur Definition des Begriffs Art. 3 Abs. 1 Ziff. 6 ETIAS-VO.

745 Siehe zur Definition des Begriffs Art. 3 Abs. 1 Ziff. 7 ETIAS-VO.

746 Siehe zur Definition des Begriffs Art. 3 Abs. 1 Ziff. 8 ETIAS-VO.

747 FIOLKA/STALDER, 168 f.

748 Siehe dazu Art. 36 Abs. 6 ETIAS-VO.

749 Siehe dazu Art. 80 ETIAS-VO (diese Bestimmung ändert Art. 6 Abs. 1 Bst. b Schengener Grenzkodex).

750 BUNDESRAT, Botschaft ETIAS, 2906; FIOLKA/STALDER, 168 f. Siehe Art. 45 ETIAS-VO zum Datenzugriff der Beförderungsunternehmer zu Überprüfungszwecken.

Für die Errichtung des ETIAS-Informationssystems wurde die VO 2018/1240 (ETIAS-VO) geschaffen, welche am 9. Oktober 2018 in Kraft getreten ist. Während einige Bestimmungen – insbesondere diejenigen Artikel zur technischen Umsetzung – bereits seit diesem Datum gelten, sind andere Bestimmungen erst ab der Inbetriebnahme des ETIAS anwendbar.[751] Am gleichen Tag wie die ETIAS-VO trat auch die VO 2018/1241 in Kraft. Damit werden die mit der ETIAS-VO veranlassten Änderungen in Bezug auf die Tätigkeiten von Europol in der entsprechenden Verordnung, der VO 2016/794, vorgenommen.[752]

Am 7. Juli 2021 wurden die ETIAS-Änderungsverordnungen verabschiedet. Es handelt sich dabei um die VO 2021/1150, VO 2021/1151 und VO 2021/1152. Darin werden die gesetzlichen Anpassungen vorgenommen, welche notwendig sind, um die im Rahmen des ETIAS vorgenommene automatisierte Abfrage mit den anderen Informationssystemen sowie den Europol-Daten zu ermöglichen.[753] Die Inbetriebnahme des ETIAS ist derzeit noch ausstehend.[754] Aktuell ist dafür das letzte Quartal 2026 vorgesehen.[755]

8.2. Betrieb und Aufsicht

Das ETIAS-Informationssystem besteht u.a. aus dem ETIAS-Zentralsystem inklusive der ETIAS-Überwachungsliste, den nationalen Schnittstellen, einer sicheren und verschlüsselten Kommunikationsinfrastruktur zwischen dem ETIAS-Zentralsystem und den nationalen Schnittstellen sowie auch einer sicheren Kommunikationsinfrastruktur zwischen dem ETIAS-Zentralsystem und den Informationssystemen, welche im Rahmen der automatisierten Abfrage konsultiert werden.[756]

---

751 Bundesrat, Botschaft ETIAS, 2927. Es wurde kritisiert, dass im Verfahren zur Errichtung der gesetzlichen Grundlagen des ETIAS keine Folgenabschätzung vorgenommen wurde. Es wurde zwar eine Machbarkeitsstudie erstellt. Dieses Instrument erfüllt jedoch eine andere Funktion. In der Folgenabschätzung werden grundsätzlich verschiedene alternative Optionen geprüft und die vorgeschlagene Option mit Nachweisen versehen. Ohne eine solche Folgenabschätzung erscheint eine Beurteilung des ETIAS nicht möglich. Siehe dazu Alegre/Jeandesboz/Vavoula, 27 ff. m.w.H. Siehe zur Machbarkeitsstudie European Commission, Feasibility Study ETIAS. Siehe für eine Bewertung des Vorschlags FRA, Opinion proposed ETIAS; EDSB, Stellungnahme Vorschlag ETIAS.

752 Vgl. dazu Art. 2 VO 2018/1241 sowie die ausführliche Bezeichnung der genannten Verordnung.

753 Siehe dazu jeweils ErwG. 4 VO 2021/1150, VO 2021/1151 sowie VO 2021/1152.

754 Siehe dazu <https://www.sem.admin.ch/sem/de/home/themen/einreise/etias.html>, zuletzt besucht am 07.03.2025.

755 <https://www.consilium.europa.eu/de/meetings/jha/2025/03/05/>, zuletzt besucht am 07.03.2025.

756 Vgl. zu den Einzelheiten Art. 6 ETIAS-VO.

Auf der Überwachungsliste sind Daten von Personen aufgeführt, die einer (Beteiligung an einer) terroristischen oder anderen schweren Straftat verdächtigt werden oder aufgrund einer Gesamtbeurteilung faktische Anhaltspunkte resp. hinreichende Gründe vorliegen, welche darauf hindeuten, dass eine solche Straftat begangen wird.[757] Diese Daten werden von Europol oder von den Schengen-Staaten in die ETIAS-Überwachungsliste eingetragen. Ist bereits eine Ausschreibung im SIS vorhanden, wird die Person nicht zusätzlich in der ETIAS-Überwachungsliste erfasst.[758]

Die ETIAS-Zentralstelle, welche bei Frontex angesiedelt ist, wird rund um die Uhr im Einsatz sein. Sie ist u.a. dafür zuständig, die im Rahmen der automatisierten Antragsbearbeitung gefundenen Treffer in den anderen Datenbanken zu überprüfen, die Anträge von Europol betreffend Einsicht in ETIAS-Daten zu bearbeiten sowie die Auswirkungen auf die Grundrechte – insbesondere das Recht auf Schutz des Privatlebens sowie das Recht auf Schutz personenbezogener Daten – regelmässig zu beurteilen.[759] Die ETIAS-Zentralstelle ist auch dafür zuständig, dass die gespeicherten und erfassten Daten vollständig und aktuell sind.[760] Ausserdem fallen die ETIAS-Überprüfungsregeln in ihren Zuständigkeitsbereich.[761]

Mit diesen Überprüfungsregeln sollen Personen entdeckt werden können, welche die Sicherheit oder die öffentliche Gesundheit potenziell gefährden oder ein Migrationsrisiko darstellen. Diese Regeln in der Form eines Algorithmus werden von der ETIAS-Zentralstelle in das ETIAS-Zentralsystem eingegeben und basieren u.a. auf Statistiken des EES sowie des ETIAS bezüglich bestimmter Gruppen, welche mit einer ungewöhnlich hohen Zahl von Aufenthaltsüberziehern, Einreiseverweigerungen sowie Verweigerungen von Reisegenehmigungen vertreten sind. Die einzelnen Risikoindikationen können aus einem Zusammenspiel von bestimmten Angaben wie bspw. Altersgruppe, Staatsangehörigkeit, Wohnsitz, Berufsgruppe, Bildungsniveau, etc. entstehen.[762]

---

757 Siehe dazu Art. 34 Abs. 4 ETIAS-VO. Dort werden u.a. verschiedene Angaben zur Person, zum Reisedokument sowie zu den Kontaktmöglichkeiten genannt, wobei jeweils mindestens ein Datenelement in die ETIAS-Überwachungsliste einzutragen ist.

758 Siehe zu den Einzelheiten Art. 34 f. ETIAS-VO.

759 Vgl. zu den Einzelheiten Art. 7 ETIAS-VO; BUNDESRAT, Botschaft ETIAS, 2909.

760 BUNDESRAT, Botschaft ETIAS, 2909 f. m.w.H.

761 Siehe dazu Art. 75 ETIAS-VO.

762 Siehe dazu Art. 33 ETIAS-VO; BUNDESRAT, Botschaft ETIAS, 2915. Siehe dazu kritisch FRA, Opinion proposed ETIAS, 27 ff.; EDSB, Stellungnahme Vorschlag ETIAS, 11 ff.

Des Weiteren hat jeder Schengen-Staat eine sog. nationale ETIAS-Stelle zu bezeichnen. Diese beurteilt u.a. die von der ETIAS-Zentralstelle weitergeleiteten Anträge, speichert die in diesem Zusammenhang zustande gekommenen Ergebnisse im einschlägigen Antragsdatensatz und sorgt für die Aktualität der in den Antragsdatensätzen eingegebenen Daten.[763]

Abgesehen davon besteht ein ETIAS-Überprüfungsausschuss, welcher aus je einem Vertreter der nationalen ETIAS-Stellen, Frontex sowie Europol gebildet wird. Diesem Ausschuss, welcher von Frontex eingerichtet wird, kommt Beratungsfunktion zu. Er erstellt Stellungnahmen, Leitlinien und Empfehlungen und definiert das bewährte Verfahren. Des Weiteren besteht auch ein unabhängiges ETIAS-Beratungsgremium für Grundrechte, welchem eine Beratungs- und Beurteilungsfunktion zukommt. Dieses nimmt regelmässig Beurteilungen vor und verfasst für den ETIAS-Überprüfungsausschuss Empfehlungen betreffend die Einhaltung der Grundrechte. Dabei steht der Schutz der Privatsphäre sowie der personenbezogenen Daten als auch die Nichtdiskriminierung im Vordergrund.[764]

Die technische Verwaltung des ETIAS fällt in die Zuständigkeit von eu-LISA.[765] Der EDSB überwacht die Datenbearbeitung im Zusammenhang mit dem ETIAS durch eu-LISA, Europol und Frontex.[766] Zudem haben die Schengen-Staaten nationale Aufsichtsbehörden einzurichten.[767] Diese arbeiten mit dem EDSB zusammen und tauschen gegenseitig einschlägige Informationen aus.[768]

8.3. Beteiligung der Schweiz

Die EU hat der Schweiz am 7. September 2018 die ETIAS-VO als Weiterentwicklung des Schengen-Besitzstands notifiziert. Der Notenaustausch zur Übernahme der ETIAS-VO ist am 15. Januar 2021 in Kraft getreten. Die Anwendbarkeit dieses Notenaustauschs ist jedoch noch ausstehend, da die Kommission das Datum für die Inbetriebnahme des ETIAS noch nicht festgelegt hat.[769] Die Mehrzahl der Bestimmungen der ETIAS-VO sind direkt anwendbar und müssen demnach nicht ins nationale Recht überführt werden. Vereinzelte Konkretisierungen einzelner Bestimmungen sind jedoch im AIG oder auf Ver-

763 Vgl. zu den Einzelheiten Art. 8 ETIAS-VO.
764 Bundesrat, Botschaft ETIAS, 2910. Siehe zu den Einzelheiten Art. 9 und Art. 10 ETIAS-VO.
765 Vgl. dazu Art. 74 ETIAS-VO.
766 Vgl. dazu Art. 67 ETIAS-VO.
767 Art. 66 ETIAS-VO.
768 Siehe dazu Art. 68 ETIAS-VO.
769 Bundesrat, Botschaft ETIAS Consequential Amendments, 15.

ordnungsstufe vorzunehmen.[770] An die VO 2018/1241, welche die entsprechenden Anpassungen in Bezug auf die Tätigkeiten von Europol vornimmt, ist die Schweiz hingegen nicht gebunden.[771]

Die nationale ETIAS-Stelle soll als Organisationseinheit im SEM geschaffen werden. Diese hat die Prüfung der ihr übermittelten Gesuche vorzunehmen und konsultiert die entsprechenden Behörden des Bundes oder der Kantone im Bereich der Migration, der Sicherheit sowie der Gesundheit.[772] Das SEM ist zudem im Einvernehmen mit fedpol und dem NDB für die Eingabe der Daten in die Überwachungsliste zuständig.[773] Die Überwachungsliste wird zwar regelmässig von fedpol und dem NDB geprüft. Diese Stellen können jedoch lediglich Änderungs- und Löschungsaufträge bei der nationalen ETIAS-Stelle beim SEM stellen. Nur die nationale ETIAS-Stelle beim SEM kann Daten im ETIAS erfassen und bearbeiten.[774]

Des Weiteren wurden der Schweiz am 29. Juni 2021 die VO 2021/1150 sowie die VO 2021/1152 als Schengen-Weiterentwicklungen notifiziert.[775] Die Notenaustausche sind am 21. April 2023 in Kraft getreten.[776] Diese beiden Verordnungen regeln u.a. die Zugriffsrechte der nationalen ETIAS-Stellen auf die im EES, VIS und SIS gespeicherten Daten. In der Schweiz mussten folglich die Zugriffsrechte der nationalen ETIAS-Stelle auf bestimmte nationale Informationssysteme geregelt werden. Davon abgesehen soll auch ein nationales ETIAS-System, das N-ETIAS, geschaffen werden.[777]

Die Kommission geht davon aus, dass rund 47 Millionen ETIAS-Gesuche jährlich für den gesamten Schengen-Raum gestellt werden, wovon rund 2-3 % dieser Gesuche von den nationalen ETIAS-Stellen manuell bearbeitet werden müssten. Der Schweiz würden demnach jährlich rund 37'000 Gesuche zufallen.[778]

770 Siehe zu den Einzelheiten BUNDESRAT, Botschaft ETIAS, 2927 ff.
771 BUNDESRAT, Botschaft ETIAS, 2924.
772 BUNDESRAT, Botschaft ETIAS, 2929, 2935.
773 BUNDESRAT, Botschaft ETIAS, 2906.
774 BUNDESRAT, Botschaft ETIAS, 2937.
775 Die VO 2021/1151 ist hingegen nicht schengenrelevant. Sie betrifft Folgeänderungen für das Informationssystem ECRIS-TCN. Siehe dazu BUNDESRAT, Botschaft ETIAS Consequential Amendments, 14.
776 Siehe dazu Notenaustausch VO 2021/1150; Notenaustausch VO 2021/1152.
777 Siehe zu den Einzelheiten BUNDESRAT, Botschaft ETIAS Consequential Amendments.
778 BUNDESRAT, Botschaft ETIAS, 2944.

8.4. Gespeicherte Daten

Im Antragsformular sind bestimmte Angaben zur gesuchstellenden Person (Vorname(n), Nachname(n), Geburtsdatum, Geburtsort, Geburtsland, Geschlecht, Staatsangehörigkeit(en), Vorname(n) der Eltern sowie ggf. allfällig genutzte sonstige Namen), dem Reisedokument (Art, Nummer, Ausstellungsland, Datum der Ausstellung und des Ablaufs der Gültigkeitsdauer), den Kontaktangaben (Privatanschrift, E-Mail-Adresse, Telefonnummer), der Bildung[779] sowie der aktuellen Tätigkeit – welche als Berufsgruppe aus einer vorgegebenen Liste erfasst wird – und der Angabe zum Schengen-Staat des geplanten ersten Aufenthalts (sowie fakultativ der dortigen Anschrift) zu machen.[780]

Abgesehen davon müssen von der antragstellenden Person verschiedene Fragen beantwortet werden. Diese Fragen zielen insbesondere darauf ab, in Erfahrung zu bringen, ob die gesuchstellende Person aufgrund bestimmter Straftaten verurteilt worden ist, sich in einem bestimmten Kriegs- und Konfliktgebiet aufgehalten hat oder ob gegen die gesuchstellende Person eine Entfernungsmassnahme angeordnet worden ist. Wird eine Frage bejaht, sind weitere Fragen zu beantworten. Bei der Eingabe des Antragsformulars wird zudem die IP-Adresse gespeichert, von welcher das Formular eingereicht wird.[781]

Sobald die Zulassungsbedingungen erfüllt sind (d.h. es sind alle Felder des Formulars ausgefüllt, die Fragen beantwortet und die Gebühr bezahlt), wird ein Antragsdatensatz erstellt.[782] Anschliessend werden bestimmte Daten durch das ETIAS-Zentralsystem gespeichert (u.a. die oben genannten Daten zur Per-

779 Fraglich erscheint, wieso Angaben zur Bildung der gesuchstellenden Person erfragt werden. Die Erfassung dieser Daten im Zusammenhang mit dem Antrag für eine ETIAS-Reisegenehmigung erscheint unverhältnismässig. Siehe dazu VAVOULA, Right to Private Life, 260.

780 Vgl. dazu Art. 17 Abs. 2 ETIAS-VO. Siehe dort auch die speziellen Angaben für Minderjährige, Familienangehörige sowie Dritte, welche einen Antrag für eine andere Person gestellt haben. Das Gesuch für eine Reisegenehmigung muss nicht zwingend von der betroffenen Person eingereicht werden, sondern kann grundsätzlich auch von einem bevollmächtigten Dritten – z.B. einem Reisebüro – gestellt werden. Ferner ist auch für minderjährige Personen ein entsprechendes Gesuch einzureichen. Dieses ist von der Person, welche – ständig oder vorübergehend – über die elterliche Sorge verfügt resp. die gesetzliche Vormundschaft ausübt, zu stellen und elektronisch zu unterschreiben. Siehe dazu BUNDESRAT, Botschaft ETIAS, 2914 f.; Art. 15 Abs. 4 ETIAS-VO; Art. 17 Abs. 1 ETIAS-VO. Siehe zu den Einzelheiten der Antragstellung Art. 15 f. ETIAS-VO.

781 Art. 17 Abs. 4, 6 und 8 ETIAS-VO.

782 Art. 19 Abs. 1 ETIAS-VO.

son, zum Reisedokument, zu den Kontaktangaben sowie zum Beruf).[783] Davon abgesehen prüft das ETIAS-Zentralsystem, ob bereits ein anderer Antragsdatensatz derselben gesuchstellenden Person im ETIAS-Zentralsystem gespeichert ist. Verläuft diese Suche positiv, wird der neue Antragsdatensatz mit dem bereits bestehenden verknüpft. Nach der Erstellung des Antragsdatensatzes wird die gesuchstellende Person informiert, dass möglicherweise weitere Angaben eingefordert werden können oder – ausnahmsweise – eine Befragung durchgeführt werden kann.[784]

Im Weiteren erfolgt eine automatisierte Bearbeitung der Antragsdatensätze. So wird u.a. ein Abgleich von bestimmten erfassten Daten mit den im SIS, EES, VIS, Eurodac, ECRIS-TCN und in zwei Interpol-Datenbanken gespeicherten Daten sowie den Europol-Daten vorgenommen. Ausserdem wird geprüft, ob eine der gestellten Fragen bejaht wurde. Zudem werden gewisse Daten mit der ETIAS-Überwachungsliste und den ETIAS-Überprüfungsregeln abgeglichen.[785] Erfolgt bei diesem automatisierten Abgleich kein Treffer, wird die Reisegenehmigung automatisch durch das System ausgestellt. Liegt jedoch ein Treffer vor, überprüft die ETIAS-Zentralstelle – innerhalb von höchstens zwölf Stunden nach Eingang des Antragdatensatzes – manuell die Richtigkeit der ihr mitgeteilten Angaben sowie die gefundenen Treffer. Entsprechen sich die Daten nicht, wird der Treffer aus dem Antragsdatensatz gelöscht. Wird der Treffer bestätigt oder bestehen weiterhin Zweifel an der Identität der gesuchstellenden Person, erfolgt eine Weiterleitung an die zuständige nationale ETIAS-Stelle.[786] Diese entscheidet abschliessend darüber, ob eine Reisegenehmigung erteilt oder verweigert wird. Sie kann weitere Unterlagen einfordern, in Ausnahmefällen die gesuchstellende Person befragen sowie Konsultationen mit anderen nationalen ETIAS-Stellen oder Europol vornehmen.[787]

Wird die Reisegenehmigung verweigert, kann der begründete Entscheid von der betroffenen Person angefochten werden.[788] Wenn u.a. Zweifel am Vorliegen von hinreichenden Gründen für die Verweigerung einer Reisegenehmi-

783 Art. 19 Abs. 2-3 ETIAS-VO.

784 Art. 19 Abs. 4-5 ETIAS-VO.

785 Siehe Art. 20 ETIAS-VO zu den Einzelheiten dieser automatisierten Bearbeitung.

786 Wurde eine der gestellten Fragen bejaht, jedoch ansonsten kein Treffer erzielt, erfolgt eine Weiterleitung an die zuständige nationale ETIAS-Stelle zur manuellen Bearbeitung. Siehe zum Ganzen Art. 21 f. ETIAS-VO. Art. 25 ETIAS-VO regelt, welche nationale ETIAS-Stelle für die manuelle Bearbeitung zuständig ist. Siehe dazu auch BUNDESRAT, Botschaft ETIAS, 2917.

787 BUNDESRAT, Botschaft ETIAS, 2917. Vgl. zu den Einzelheiten Art. 26 ff. ETIAS-VO.

788 Siehe zu den Einzelheiten Art. 37 ETIAS-VO. Siehe zur Mitteilung über die Verweigerung einer Reisegenehmigung Art. 38 Abs. 2 ETIAS-VO.

gung bestehen, kann die nationale ETIAS-Stelle die ETIAS-Reisegenehmigung mit einer Kennzeichnung versehen.[789]

Nach der Entscheidung über die Erteilung resp. die Verweigerung einer Reisegenehmigung werden dem Antragsdatensatz damit zusammenhängende Angaben hinzugeführt, z.B. das Datum der Entscheidung, der Beginn und das Ende der Reisegenehmigung oder der Grund für die Verweigerung.[790]

Eine bereits erteilte Reisegenehmigung steht unter dem Vorbehalt einer allfälligen Annullierung resp. eines Widerrufs, nämlich wenn die Voraussetzungen für die Erteilung einer solchen bei der Ausstellung nicht erfüllt gewesen waren oder nicht mehr erfüllt sind. Die betroffene Person kann ein Rechtsmittel gemäss dem nationalen Recht des Staates ergreifen, welcher den Entscheid der Annullierung resp. des Widerrufs getroffen hat. Ein rechtskräftiger Entscheid über die Annullierung resp. den Widerruf einer Reisegenehmigung hat zur Folge, dass die betroffene Person den Schengen-Raum sofort zu verlassen hat, da die Einreisevoraussetzungen nicht mehr vorliegen. Ferner kann eine Reisegenehmigung auch auf Antrag der gesuchstellenden Person aufgehoben werden.[791]

Die im ETIAS gespeicherten personenbezogenen Daten dürfen grundsätzlich nur so lange gespeichert werden, wie es für die Zwecke der Datenbearbeitung notwendig ist. Deshalb werden die Daten in der Regel während der Gültigkeitsdauer der Reisegenehmigung gespeichert. Nach Ablauf derselben können die Daten mit dem ausdrücklichen Einverständnis der betroffenen Person zwecks Erleichterung der Einreichung eines neuen Gesuchs für längstens drei weitere Jahre gespeichert bleiben, wobei die Einwilligung jederzeit widerrufbar ist. Nachdem die Speicherfrist abgelaufen ist, wird der Antragsdatensatz automatisch aus dem ETIAS-Zentralsystem gelöscht. Wird eine Reisegenehmigung verweigert, annulliert oder widerrufen, werden die Daten für fünf Jahre ab der letzten Entscheidung über die Reisegenehmigung gespeichert. Fällt der Grund für die Verweigerung, die Annullierung resp. den Widerruf, also z.B. eine Ausschreibung, innert dieser Frist weg, wird der Datensatz im ETIAS ebenfalls bereits vor Ablauf der fünfjährigen Frist gelöscht.[792]

---

789 Siehe zu den Einzelheiten dazu BUNDESRAT, Botschaft ETIAS, 2918; Art. 36 Abs. 2-4 ETIAS-VO.

790 Vgl. dazu Art. 39 ETIAS-VO.

791 Siehe dazu BUNDESRAT, Botschaft ETIAS, 2918 f.; Art. 40-43 ETIAS-VO. In der Schweiz richtet sich das Verfahren nach dem VwVG. Demnach kann beim BVGer innerhalb von 30 Tagen nach Eröffnung der entsprechenden Verfügung schriftlich Beschwerde eingereicht werden. Siehe dazu BUNDESRAT, Botschaft ETIAS, 2936 f.

792 BUNDESRAT, Botschaft ETIAS, 2920 f.; Art. 54 f. ETIAS-VO. Siehe dort auch die Möglichkeiten, Änderungen an den gespeicherten Daten vorzunehmen resp. vorzeitig – z.B. bei Erwerb einer Staatsangehörigkeit eines Schengen-Staates – zu löschen.

8.5. Zugriffsberechtigung

Der Zugriff auf ETIAS-Daten ist für verschiedene Behörden resp. Stellen möglich. So erhalten die ETIAS-Zentralstelle und die nationalen ETIAS-Stellen einen direkten und umfassenden Zugriff auf sämtliche ETIAS-Daten. Die Migrationsbehörden, die Grenzkontrollorgane sowie die Beförderungsunternehmen verfügen über einen direkten, jedoch beschränkten Zugang. Sie erhalten lediglich für einen konkreten Zweck Zugriff auf bestimmte Daten. Die nationalen Strafverfolgungsbehörden wiederum können nur mittelbar auf die Daten zugreifen.[793] Ebenfalls kann Europol in bestimmten Situationen Einsicht in ETIAS-Daten erhalten.[794] Zudem können in bestimmten Fällen im Rahmen von automatischen Benachrichtigungen auch den SIRENE-Büros bestimmte ETIAS-Daten zugänglich gemacht werden.[795]

8.5.1. ETIAS-Zentralstelle und nationale ETIAS-Stellen

Sofern sich bei der automatisierten Bearbeitung der Antragsdatensätze ein Treffer ergeben hat, erhält die ETIAS-Zentralstelle Zugriff auf den entsprechenden Antragsdatensatz inklusive allfälliger damit verbundenen Antragsdatensätze sowie auf die erzielten Treffer.[796]

Die nationalen ETIAS-Stellen erhalten im Rahmen einer manuellen Bearbeitung Zugriff auf den Antragsdatensatz, den damit verbundenen Antragsdatensätzen sowie den bei der automatisierten Bearbeitung gefundenen Treffern in anderen Datenbanken. Ausserdem wird der nationalen ETIAS-Stelle bekannt gegeben, welcher resp. welche Schengen-Staaten resp. Europol die Daten eingegeben haben, die zu dem resp. den Treffer(n) geführt haben.[797] Nationale ETIAS-Stellen können ausserdem bei einer sog. Konsultation Zugriff auf den Antragsdatensatz erhalten.[798]

---

793 BUNDESRAT, Botschaft ETIAS, 2910 f. Vgl. zu den Einzelheiten Art. 13 ETIAS-VO.

794 Siehe dazu Art. 53 ETIAS-VO; Art. 29 ETIAS-VO.

795 Siehe zu den Einzelheiten Art. 23 ETIAS-VO.

796 Siehe dazu Art. 22 Abs. 1-2 ETIAS-VO.

797 Art. 26 Abs. 1 ETIAS-VO.

798 Siehe dazu Art. 28 ETIAS-VO. Die nationalen ETIAS-Stellen haben zudem zur Prüfung von Anträgen auf Erteilung einer Reisegenehmigung resp. zur Entscheidung über diese Anträge Zugang zu bestimmten Daten in anderen Informationssystemen. Siehe dazu Art. 25a ETIAS-VO.

8.5.2. Migrations- und Grenzkontrollbehörden sowie Beförderungsunternehmen

Beförderungsunternehmen – für die Einreise in die Schweiz betrifft dies ausschliesslich Luftverkehrsunternehmen – verfügen über einen sicheren Zugang zum ETIAS. Damit können sie vor der Beförderung der Passagiere überprüfen, ob diese – sofern nötig – über eine entsprechende Reisegenehmigung verfügen. Die Abfrage erfolgt anhand der Daten, welche in der maschinenlesbaren Zone des Reisedokuments gespeichert sind. Abgesehen davon ist derjenige Schengen-Staat einzugeben, in welchen zuerst eingereist werden wird. Das Ergebnis der Abfrage ist eine «OK» resp. «NOT OK» Antwort, woraus geschlossen werden kann, ob eine gültige Reisegenehmigung vorliegt oder nicht. Berücksichtigt wird dabei auch, ob die Reisegenehmigung räumlich begrenzt ist.[799] Drittstaatsangehörige, welchen die Einreise in den Schengen-Raum verweigert wird, haben die Beförderungsunternehmen unverzüglich zurückzubefördern. Kommen die Beförderungsunternehmen ihren Sorgfaltspflichten nicht nach, können Sanktionen verhängt werden.[800]

Bei den Grenzübergangsstellen werden die in der maschinenlesbaren Zone der Reisedokumente gespeicherten Daten der ankommenden Personen von den Grenzkontrollbehörden eingelesen. Da das ETIAS von den Grenzkontrollbehörden lediglich zur Ermittlung des Status der Reisegenehmigung genutzt werden darf, ist der Zugang zu Daten aus dem ETIAS beschränkt. Den Grenzkontrollbehörden wird insbesondere angezeigt, ob eine gültige ETIAS-Reisegenehmigung vorhanden ist (mit allfälliger räumlicher Begrenzung), diese mit einer Kennzeichnung versehen ist oder innerhalb der nächsten 90 Tage abläuft sowie die verbleibende Gültigkeitsdauer. Wird eine Kennzeichnung angezeigt, erfolgt eine Kontrolle in der zweiten Kontrolllinie[801] durch die Grenzkontrollbehörden. In diesem Rahmen sind sie berechtigt, zusätzliche Angaben – wie bspw. den Grund der Kennzeichnung – abzufragen, sofern dies erforderlich ist. Ist keine gültige Reisegenehmigung vorhanden, muss ein entsprechendes Gesuch gestellt werden. Kann keine entsprechende Reisegenehmigung ausgestellt werden, wird eine Einreiseverweigerung erlassen und im EES eingetragen. Ist die Reisegenehmigung einer reisenden Person gültig, wer-

799 Siehe zur räumlichen Begrenzung Art. 44 ETIAS-VO.

800 Siehe dazu BUNDESRAT, Botschaft ETIAS, 2912 f.; Art. 45 ETIAS-VO. Für den Fall, dass ETIAS aus technischen Gründen nicht abgerufen werden kann, ist ein Ausweichverfahren vorgesehen. Siehe dazu Art. 46 ETIAS-VO.

801 Es handelt sich dabei um eine weitere Kontrolle, welche nicht an dem Ort stattfindet, wo alle Personen kontrolliert werden (erste Kontrolllinie), sondern an einem eigens dazu vorgesehenen Ort durchgeführt werden kann. Siehe dazu Art. 3 Abs. 1 Ziff. 3 ETIAS-VO.

den die übrigen Einreisevoraussetzungen gemäss dem Schengener Grenzkodex geprüft und letztlich die Einreise in den Schengen-Raum gewährt oder verweigert.[802]

Die Migrationsbehörden – in der Schweiz primär das SEM sowie die kantonalen und kommunalen Migrationsbehörden[803] – verfügen lediglich über einen subsidiären Zugang zu ETIAS-Daten. Das bedeutet, dass vorgängig eine Abfrage im EES erfolgt sein muss und dort kein Einreisedatensatz vorhanden ist, welcher der Anwesenheit des betroffenen Drittstaatsangehörigen im Hoheitsgebiet der Schengen-Staaten entspricht. Ausserdem darf eine Abfrage lediglich erfolgen, um zu prüfen, ob die Voraussetzungen einer Einreise resp. eines Aufenthalts im Schengen-Staat erfüllt sind sowie im Hinblick auf zu ergreifende Massnahmen in diesem Zusammenhang. Eine Abfrage erfolgt mittels bestimmter Datenkategorien (z.B. Name der Person oder Nummer des Reisedokuments). Das ETIAS-Zentralsystem zeigt an, ob die betroffene Person eine gültige Reisegenehmigung – inkl. allfälliger räumlicher Begrenzung – besitzt sowie ob die Reisegenehmigung in den nächsten 90 Tagen abläuft und die verbleibende Gültigkeitsdauer. Ausserdem wird den Migrationsbehörden zwecks Rückführung eines Drittstaatsangehörigen Zugriff auf ETIAS-Daten gewährt, ebenfalls unter der Bedingung, dass eine Abfrage im EES erfolglos geblieben ist. Mit diesem Zugriff wird bezweckt, dass in Einzelfällen Angaben an den betroffenen Drittstaat übermittelt werden können.[804]

8.5.3. Nationale Strafverfolgungsbehörden

Wie bei den Datenbanken VIS, EES und Eurodac ist auch beim ETIAS ein mittelbarer Zugang für nationale Strafverfolgungsbehörden vorgesehen. Diese sog. «*benannten Behörden*» können bei der unabhängigen zentralen Zugangsstelle mit einem begründeten Antrag elektronisch mittels Formular zwecks Verhütung, Aufdeckung und Untersuchung terroristischer[805] oder sonstiger

802 Zum Ganzen BUNDESRAT, Botschaft ETIAS, 2911 f.; Art. 47 f. ETIAS-VO. Siehe zum Ausweichverfahren, wenn das ETIAS aus technischen Gründen nicht abgerufen werden kann Art. 48 ETIAS-VO.

803 BUNDESRAT, Botschaft ETIAS, 2937.

804 BUNDESRAT, Botschaft ETIAS, 2913 f.; Art. 49 ETIAS-VO; Art. 65 Abs. 3 ETIAS-VO. Dabei handelt es sich um eine der Ausnahmen vom grundsätzlichen Verbot der Übermittlung von ETIAS-Daten an Drittstaaten, internationale Organisationen oder private Stellen. Siehe dazu BUNDESRAT, Botschaft ETIAS, 2922; Art. 65 Abs. 1 ETIAS-VO. Siehe dazu auch Kapitel III.8.6.1.

805 Siehe zur Definition Art. 3 Abs. 1 Ziff. 15 ETIAS-VO. In der Schweiz sind die terroristischen Straftaten in Anhang 1a N-SIS-Verordnung aufgeführt.

schwerer Straftaten[806] Einsicht in Daten des ETIAS beantragen. Die Abfrage ist auf die Suche anhand bestimmter Daten beschränkt.[807]

Die zentrale Zugangsstelle überprüft dabei, ob die folgenden Bedingungen erfüllt sind: Der Zugang muss im Einzelfall für die Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren Straftat erforderlich und verhältnismässig sein. Zudem müssen Beweise oder hinreichende Gründe dafür vorliegen, dass die Abfrage im ETIAS hinsichtlich der Verhütung, Aufdeckung oder Untersuchung der genannten Straftaten beitragen wird. Sind diese Voraussetzungen erfüllt, greift die zentrale Zugangsstelle auf die entsprechenden Daten zu und übermittelt diese der gesuchstellenden Behörde.[808] In dringenden Ausnahmefällen erfolgt die Überprüfung der genannten Voraussetzungen durch die zentrale Zugangsstelle erst nachträglich. Wird der Zugriff auf die Daten im Nachhinein als nicht gerechtfertigt bewertet, so sind die zugänglich gemachten Daten zu löschen.[809]

Bei der zentralen Zugangsstelle handelt es sich in der Schweiz – wie bereits beim VIS und EES – um die EZ fedpol. Auch bei ETIAS sind fedpol, der NDB, die Bundesanwaltschaft und die kantonalen Polizei- und Strafverfolgungsbehörden sowie die Polizeibehörden der Städte Zürich, Winterthur, Lausanne, Chiasso und Lugano berechtigt, Anträge auf Einsicht in das ETIAS zu stellen.[810]

8.5.4. Europol

Europol ist zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Kriminalität ebenfalls befugt, bei der ETIAS-Zentralstelle einen begründeten Antrag auf Einsicht in das ETIAS zu stellen.[811]

Davon abgesehen kann Europol auch im Rahmen einer Konsultation Zugriff auf ETIAS-Daten erhalten.[812]

---

806 Siehe zur Definition Art. 3 Abs. 1 Ziff. 16 ETIAS-VO. In der Schweiz handelt es sich dabei um die in Anhang 1b N-SIS-Verordnung aufgeführten Straftaten.

807 Siehe zu den Einzelheiten dieser Abfrage Art. 50-52 ETIAS-VO.

808 Für gewisse Angaben besteht keine Zugriffsmöglichkeit (z.B. Bildung) resp. müssen ausdrücklich im Antrag beantragt werden (Berufsgruppe sowie Antworten auf die Fragen gemäss dem Fragekatalog). Siehe dazu Art. 52 Abs. 4 ETIAS-VO.

809 Art. 51 ETIAS-VO; Art. 52 ETIAS-VO.

810 Siehe dazu BUNDESRAT, Botschaft ETIAS, 2938 f.

811 Siehe zu den Einzelheiten Art. 53 ETIAS-VO.

812 Siehe zu den Einzelheiten Art. 29 ETIAS-VO. Explizit festgehalten ist jedoch, dass Europol keinen Zugang zu den Angaben betreffend die Bildung der betroffenen Person erhalten darf.

8.6. Ausgewählte Sicherheitsmassnahmen

8.6.1. Übermittlung von ETIAS-Daten an Drittstaaten, internationale Organisationen und private Stellen

Grundsätzlich ist eine Übermittlung von ETIAS-Daten an Drittstaaten, internationale Organisationen sowie private Stellen untersagt. Es sind jedoch bestimmte Ausnahmen von diesem Grundsatz vorgesehen. So dürfen z.B. Einwanderungsbehörden, in der Schweiz das SEM, unter bestimmten Voraussetzungen Daten an einen Drittstaat zwecks Rückführung einer Person übermitteln. Des Weiteren dürfen auch die nationalen Strafverfolgungsbehörden, zu Sicherheitszwecken unter bestimmten Voraussetzungen ETIAS-Daten an einen Drittstaat übermitteln.[813]

8.6.2. Protokollierungspflicht

Alle in ETIAS vorgenommenen Datenverarbeitungsvorgänge werden von eu-LISA protokolliert. Auch die ETIAS-Zentralstelle sowie die Schengen-Staaten haben Protokolle zu erstellen.[814]

Des Weiteren haben eu-LISA sowie auch die Schengen-Staaten und Europol Protokolle von allen Datenbearbeitungsvorgängen im ETIAS-Zentralsystem, welche im Zusammenhang mit der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten erfolgen, zu erstellen.[815]

8.6.3. Rechte der betroffenen Personen

Den von der Datenbearbeitung im Zusammenhang mit dem ETIAS betroffenen Personen stehen gewisse Rechte zu. So dürfen sie Auskunft über die gespeicherten Daten, die Berichtigung unrichtiger und ggf. die Löschung von Daten verlangen. Je nachdem welche Stelle die Daten bearbeitet, kommt ferner ein Recht auf Sperrung resp. ein Recht auf Einschränkung der Verarbeitung dazu. Über das Vorhandensein dieser Rechte sind die betroffenen Personen bei der Erhebung der Daten zu informieren. Diese Rechte können bei der ETIAS-Zentralstelle oder bei der für den Antrag zuständigen nationalen ETIAS-Stelle geltend gemacht werden. Der entsprechende Antrag ist innert 30 Tagen zu bearbeiten. Wird dem Antrag der gesuchstellenden Person nicht entsprochen,

813 Art. 65 ETIAS-VO; BUNDESRAT, Botschaft ETIAS Consequential Amendments, 76 f.
814 Siehe zu den Einzelheiten Art. 69 ETIAS-VO.
815 Siehe zu den Einzelheiten Art. 70 ETIAS-VO.

ist ein entsprechender Verwaltungsentscheid zu fällen, welcher angefochten werden kann.[816]

8.6.4. Haftung und Sanktionen

Die Schengen-Staaten sowie eu-LISA haften für materielle oder immaterielle Schäden, welche durch eine gegen die ETIAS-VO verstossende Handlung einer Person oder eines Schengen-Staats entstanden sind. Von der Haftung können sich die Schengen-Staaten sowie eu-LISA exkulpieren, sofern sie nachweisen können, dass sie für die Entstehung des Schadens nicht verantwortlich sind. Für die Geltendmachung eines entsprechenden Schadenersatzanspruchs gegen einen Schengen-Staat ist das nationale Recht dieses Schengen-Staats einschlägig.[817]

Die Schengen-Staaten haben ferner für Verstösse gegen die ETIAS-VO Sanktionen vorzusehen, welche wirksam, verhältnismässig und abschreckend sein müssen.[818] In der Schweiz ist ein Bussgeld vorgesehen.[819]

9. Europäisches Strafregisterinformationssystem für Drittstaatsangehörige

9.1. Entstehung

Das ECRIS-TCN ist vom Europäischen Strafregisterinformationssystem, dem ECRIS, zu unterscheiden.

Mit dem im April 2012 in Betrieb genommenen ECRIS können die nationalen Strafregisterbehörden der Mitgliedstaaten vom Herkunftsstaat der UnionsbürgerInnen weitgehende Informationen betreffend allfällige frühere strafrechtliche Verurteilungen in Erfahrung bringen.[820] Dieser dezentrale elektronische Austausch von Informationen betreffend strafrechtliche Verurteilungen durch

816 Siehe zu den Einzelheiten Art. 64 ETIAS-VO.
817 Art. 63 ETIAS-VO.
818 Art. 62 ETIAS-VO.
819 Bundesrat, Botschaft ETIAS, 2941.
820 Europäische Kommission, COM(2017) 341 final, 2; Fiolka/Stalder, 173. Die gesetzliche Grundlage für das ECRIS stellen der Rahmenbeschluss 2009/315/JI sowie die RL 2019/884 dar.

EU-Strafgerichte bezweckt die Verbesserung der Sicherheit der EU-BürgerInnen im Raum der Freiheit, der Sicherheit und des Rechts.[821]

Das ECRIS funktioniert wie folgt: Derjenige Mitgliedstaat, welcher einen Staatsangehörigen eines anderen Mitgliedstaates strafrechtlich verurteilt, ist gehalten, den Herkunftsmitgliedstaat entsprechend zu informieren und ggf. Aktualisierungen weiterzuleiten. Diese Informationen haben die Mitgliedstaaten zu speichern. Zudem sind sie verpflichtet, ein Zentralregister mit allen – innerhalb der EU – strafrechtlichen Verurteilungen ihrer BürgerInnen zu führen. Diese Strafregisterinformationen sind den anderen Mitgliedstaaten – sofern angefordert – zur Verfügung zu stellen. Diese Daten werden insbesondere für die Zwecke von Strafverfahren ausgetauscht, können jedoch – sofern gesetzlich vorgesehen – auch anderen Zwecken dienen.[822]

Im ECRIS können zwar auch Angaben zu Drittstaatsangehörigen abgefragt werden. Es besteht jedoch kein einheitliches Unionsverfahren. Bislang werden die entsprechenden Informationen betreffend Drittstaatsangehörige in demjenigen Mitgliedstaat erhoben, in welchem die Verurteilung erfolgt ist. Für einen vollständigen Überblick über alle Vorstrafen eines Drittstaatsangehörigen müssen deshalb Informationen aus allen Mitgliedstaaten eingefordert werden. Dies ist mit einem beträchtlichen Aufwand verbunden, weshalb die Gefahr besteht, dass die Mitgliedstaaten davon absehen, solche Informationen einzufordern. Deshalb wurde das ECRIS-TCN geschaffen. Mit diesem zentralen System können die Zentralbehörden der Mitgliedstaaten effizient und zeitnah feststellen, in welchen Mitgliedstaaten Strafregisterinformationen eines Drittstaatsangehörigen vorhanden sind. Anschliessend kann mit dem bereits bestehenden ECRIS um Auskunft ersucht werden.[823] Die Einführung des ECRIS-TCN soll zu einer massiv höheren Nutzung des ECRIS führen. Ausserdem können dadurch auch die Kosten der bis anhin von den Mitgliedstaaten systematisch gestellten generellen Auskunftsbegehren eingespart werden.[824]

Mit der Einführung des ECRIS-TCN werden also die Strafregisterdaten von Drittstaatsangehörigen zukünftig zentralisiert verwaltet. Diejenigen von EU-BürgerInnen hingegen weiterhin dezentral in den Mitgliedstaaten.[825] Eine Ab-

821 Fiolka/Stalder, 179 f.; Europäische Kommission, COM(2017) 341 final, 2; Europäische Kommission, Vorschlag ECRIS-TCN, 2.

822 Europäische Kommission, COM(2017) 341 final, 2; Fiolka/Stalder, 179 f.

823 ErwG. 4-7 ECRIS-TCN-VO; Fiolka/Stalder, 173.

824 Europäische Kommission, Vorschlag ECRIS-TCN, 12. Siehe für einen Überblick über die Entstehung und die Ausgestaltung des ECRIS-TCN auch Wahl, ECRIS-TCN.

825 Zu dieser unterschiedlichen Behandlung stellte die Kommission fest, dass damit keine wesentlichen Nachteile verbunden seien. Ausserdem lasse sich das Ziel nicht gleich wirksam

frage im ECRIS-TCN darf grundsätzlich nur erfolgen, sofern die darin gespeicherten Informationen im betreffenden Mitgliedstaat in einem gegen den Drittstaatsangehörigen gerichteten hängigen Strafverfahren benötigt werden. Sofern nach nationalem Recht vorgesehen und zulässig, dürfen diese Daten auch für andere Zwecke (wie u.a. für Visa-, Einbürgerungs- und Migrationsverfahren, für die Überprüfung bei einer Personaleinstellung oder für Sicherheitsüberprüfungen) abgefragt werden. Die Mitgliedstaaten können im nationalen Recht zudem noch weitere Zwecke zur Nutzung des ECRIS-TCN vorsehen. Diese sind der Kommission bekannt zu geben und werden im Amtsblatt der EU veröffentlicht.[826]

Die gesetzliche Grundlage des ECRIS-TCN, die VO 2019/816 (ECRIS-TCN-VO), ist bereits in Kraft getreten.[827] Die Inbetriebnahme des ECRIS-TCN steht noch aus.[828]

9.2. Betrieb und Aufsicht

Das ECRIS-TCN besteht aus verschiedenen Elementen. Im Zentralsystem sind die Identitätsangaben von verurteilten Drittstaatsangehörigen enthalten. Des Weiteren verfügt jeder Mitgliedstaat über eine nationale zentrale Zugangsstelle. Zwischen dem Zentralsystem und den zentralen nationalen Zugangsstellen ist eine Kommunikationsinfrastruktur vorhanden. Mittels einer Schnittstellensoftware können die zuständigen Behörden über die nationale zentrale Zugangsstelle sowie die Kommunikationsinfrastruktur schliesslich Zugang zum Zentralsystem erhalten.[829] Das ECRIS-TCN wird sowohl von eu-LISA entwickelt als auch anschliessend betrieben.[830]

---

in dezentralisierter Weise verwirklichen. Siehe dazu EUROPÄISCHE KOMMISSION, Vorschlag ECRIS-TCN, 8.

826 Art. 7 Abs. 1-2 ECRIS-TCN-VO. Bezogen auf den Vorschlag zur ECRIS-TCN-VO empfahl der EDSB zu prüfen, ob die über das Strafverfahren hinausgehenden Zwecke, für welche das ECRIS-TCN benutzt werden dürfe, auch tatsächlich notwendig und verhältnismässig seien und dem Grundsatz der Zweckbindung entsprächen. Siehe dazu EDSB, Stellungnahme Vorschlag ECRIS-TCN, 13 f.

827 Siehe dazu Art. 42 ECRIS-TCN-VO. Siehe für eine Bewertung des Vorschlags zum ECRIS-TCN aus datenschutzrechtlicher Perspektive EDSB, Stellungnahme Vorschlag ECRIS-TCN.

828 Die Kommission legt das Datum der Inbetriebnahme fest, sobald bestimmte Voraussetzungen erfüllt sind. Vgl. dazu Art. 35 ECRIS-TCN-VO.

829 Art. 4 Abs. 1 ECRIS-TCN-VO.

830 Vgl. dazu Art. 11 ECRIS-TCN-VO. Siehe Art. 12 ECRIS-TCN-VO zu den Zuständigkeiten der Mitgliedstaaten.

In den Mitgliedstaaten kontrollieren nationale Aufsichtsbehörden die Datenbearbeitungen im Zusammenhang mit dem ECRIS-TCN.[831] Über die Datenverarbeitung durch eu-LISA übt der EDSB die Kontrolle aus.[832] Dieser arbeitet mit den nationalen Aufsichtsbehörden zusammen.[833]

9.3. Beteiligung der Schweiz

Die Schweiz ist durch die ECRIS-TCN-VO nicht gebunden, da diese keine Schengen/Dublin-Weiterentwicklung darstellt.[834] Die Schweiz prüft derzeit eine Teilnahme am ECRIS resp. am ECRIS-TCN.[835] Dazu müsste ein entsprechendes Abkommen mit der EU abgeschlossen werden.[836]

9.4. Gespeicherte Daten

Von der Datenbearbeitung im Zusammenhang mit dem ECRIS-TCN sind insbesondere Personen aus Drittstaaten betroffen, welche in einem Mitgliedstaat strafrechtlich verurteilt wurden.[837] Sofern UnionsbürgerInnen neben ihrer Unionsbürgerschaft auch über eine Staatsangehörigkeit eines Drittstaats verfügen und in einem Mitgliedstaat strafrechtlich verurteilt wurden, können auch sie durch die Datenbearbeitung durch das ECRIS-TCN betroffen sein.[838]

---

831 Vgl. dazu Art. 28 ECRIS-TCN-VO.

832 Vgl. dazu Art. 29 ECRIS-TCN-VO.

833 Art. 30 ECRIS-TCN-VO.

834 BUNDESRAT, Botschaft IOP, 8019.

835 BUNDESRAT, Botschaft ETIAS Consequential Amendments, 27.

836 Auch der Zugang zu Eurodac-Daten zwecks Gefahrenabwehr und Strafprävention stellt keine Schengen/Dublin-Weiterentwicklung dar. Es wurde jedoch ein entsprechendes Abkommen abgeschlossen, sodass auch die schweizerischen Behörden solche Abfragen vornehmen können. Siehe dazu Kapitel III.5.3.

837 Gemäss der Definition von «*Drittstaatsangehöriger*» fallen unter diesen Begriff auch Personen, welche staatenlos sind resp. deren Staatsangehörigkeit nicht bekannt ist. Siehe dazu Art. 3 Ziff. 7 ECRIS-TCN-VO.

838 Siehe zum Ganzen Art. 2 ECRIS-TCN-VO. DoppelbürgerInnen sind jedoch von Art. 5 Abs. 1 Bst. b Ziff. ii ECRIS-TCN-VO ausgenommen. Dass auch DoppelbürgerInnen vom Anwendungsbereich vom ECRIS-TCN betroffen sind, wird kritisiert. Dies entspreche nicht dem Prinzip der Nichtdiskriminierung. Siehe dazu MEIJERS COMMITTEE, third country national ECRIS-TCN; VAVOULA, Right to Private Life, 251; WAHL, ECRIS-TCN.

Wird eine Person, welche über eine Staatsangehörigkeit eines Drittstaats verfügt, in einem Mitgliedstaat verurteilt, legt die Zentralbehörde[839] – sofern möglich automatisch und unverzüglich, nachdem die Verurteilung im Strafregister des Urteilsmitgliedstaats[840] aufgenommen worden ist – im Zentralsystem des ECRIS-TCN einen Datensatz an. Dieser enthält sowohl alphanumerische Daten als auch Fingerabdruckdaten.[841] Als alphanumerische Daten sind – sofern im Einzelfall bekannt – zwingend folgende Angaben zu speichern: der Vor- und Nachname, das Geburtsdatum, der Geburtsort, die Staatsangehörigkeit(en), das Geschlecht, allfällige frühere Namen sowie die Referenznummer des Urteilsmitgliedstaats. Ausserdem sind die Namen der Eltern zu erfassen, sofern diese Information im nationalen Strafregister eingetragen ist. Ferner sind auch die Identitätsnummer der Person resp. die Art und Nummer der Identitätsdokumente der Person sowie der Name der ausstellenden Behörde, Pseudonyme oder Aliasnamen zu speichern, sofern diese Informationen der Zentralbehörde vorliegen.[842]

Bei den Fingerabdruckdaten handelt es sich um diejenigen, welche gemäss dem nationalen Recht des Urteilsmitgliedstaats im Zuge des Strafverfahrens abgenommen wurden. Es sind zumindest diejenigen Fingerabdruckdaten von den Drittstaatsangehörigen zu erfassen, welche zu einer Freiheitsstrafe von mindestens sechs Monaten verurteilt wurden resp. wegen einer Straftat verurteilt wurden, welche im entsprechenden Mitgliedstaat mit einer Freiheitsstrafe von im Höchstmass mindestens zwölf Monaten bedroht ist. Fingerabdruckdaten, welche unabhängig von einem Strafverfahren erhoben wurden, können ebenfalls verwendet werden, sofern das nationale Recht dies vorsieht.[843]

Abgesehen von diesen Datenkategorien können auch Gesichtsbilder erfasst werden, sofern deren Aufnahme und Speicherung im betreffenden Mitgliedstaat zulässig ist.[844] Gesichtsbilder werden nach der Inbetriebnahme des

839 Die Zentralbehörde ist von der nationalen zentralen Zugangsstelle zu unterscheiden. Die Mitgliedstaaten haben die Zentralbehörden für das ECRIS zu bestimmen. Siehe zur Definition der Zentralbehörden Art. 3 Ziff. 5 ECRIS-TCN-VO.

840 Dabei handelt es sich um denjenigen Mitgliedstaat, in welchem die Verurteilung erfolgt ist. Siehe dazu Art. 3 Ziff. 4 ECRIS-TCN-VO.

841 Siehe zur Definition der Fingerabdruckdaten Art. 3 Ziff. 12 ECRIS-TCN-VO.

842 Art. 5 Abs. 1 Bst. a und Abs. 4 ECRIS-TCN-VO.

843 Art. 5 Abs. 1 Bst. b und Abs. 6 ECRIS-TCN-VO. Die Fingerabdruckdaten müssen gemäss Art. 5 Abs. 2 ECRIS-TCN-VO gewissen technischen Spezifikationen entsprechen. Gemäss Art. 2 ECRIS-TCN-VO sind DoppelbürgerInnen vom Anwendungsbereich von Art. 5 Abs. 1 Bst. b Ziff. ii ECRIS-TCN-VO ausgenommen.

844 Art. 5 Abs. 3 ECRIS-TCN-VO.

ECRIS-TCN zwecks Verifizierung der Identität verwendet. Sofern dies zukünftig technisch möglich sein sollte, können die Gesichtsbilder auch für einen automatisierten Abgleich biometrischer Daten verwendet werden.[845]

Die im ECRIS-TCN gespeicherten Daten dürfen nur von demjenigen Mitgliedstaat, welcher diese eingegeben hat, geändert oder gelöscht werden. Änderungen der Informationen in den Strafregistern sind – sofern diese ebenfalls im ECRIS-TCN gespeichert sind – ebenfalls dort vorzunehmen. Besteht der Verdacht, dass gewisse Daten im ECRIS-TCN unrichtig sind, ist entweder ein Verfahren zur Überprüfung der Richtigkeit der in Frage stehenden Daten einzuleiten resp. es ist die Zentralbehörde desjenigen Mitgliedstaats entsprechend zu benachrichtigen, welche die Daten eingegeben hat. Diese hat wiederum ein Verfahren zwecks Überprüfung der Richtigkeit der Daten einzuleiten und hat dem anderen Mitgliedstaat Meldung zu erstatten.[846] Die Mitgliedstaaten haben zudem die Rechtmässigkeit der Datenverarbeitung sicherzustellen. Diese Pflicht umfasst insbesondere, dass die in das ECRIS-TCN eingespeisten Daten richtig und aktuell sind und dass nur ordnungsgemäss ermächtigte Bedienstete im Rahmen der Wahrnehmung ihrer Aufgaben Zugang zu den Daten haben.[847]

Die Speicherfrist der Daten im Zentralsystem bemisst sich nach derjenigen der Daten über die Verurteilung(en), welche im nationalen Strafregister gespeichert sind. Der Datensatz ist nach Ablauf der Speicherfrist – nach Möglichkeit automatisch – von der Zentralbehörde des Urteilsmitgliedstaats zu löschen, inkl. der Fingerabdruckdaten sowie der Gesichtsbilder.[848] Dies hat zur Konsequenz, dass abhängig von der nationalen Gesetzgebung des Urteilsmitgliedstaats unterschiedlich lange Speicherfristen für im Zentralsystem gespeicherte Daten vorgesehen sind. Diese unterscheiden sich in erheblicher Weise. Mit der ECRIS-TCN-VO wurde jedoch keine Vereinheitlichung dieser unterschiedlichen gesetzlichen Regelungen angestrebt.[849]

---

845 Europäische Kommission, Vorschlag ECRIS-TCN, 15. Siehe dazu auch Art. 6 ECRIS-TCN-VO.

846 Art. 9 ECRIS-TCN-VO.

847 Art. 13 Abs. 1 ECRIS-TCN-VO.

848 Art. 8 ECRIS-TCN-VO. Nicht nachvollziehbar erscheint, wieso in dieser gesetzlichen Bestimmung ausdrücklich festgehalten ist, dass die Löschung «*in jedem Fall spätestens einen Monat nach Ablauf der Speicherfrist*» zu erfolgen hat. Schliesslich hat die Löschung der Daten mit dem Ablauf der Speicherfrist zu erfolgen und sollte nicht erst nach Ablauf derselben vorgenommen werden.

849 Europäische Kommission, Vorschlag ECRIS-TCN, 16.

9.5. Zugriffsberechtigung

Grundsätzlich verfügen die von den Mitgliedstaaten bezeichneten Zentralbehörden für bestimmte Zwecke über eine Zugriffsberechtigung auf ECRIS-TCN-Daten.[850] Die Abfrage im ECRIS-TCN erfolgt aufgrund aller oder lediglich einzelner alphanumerischen Daten resp. der Fingerabdruckdaten. Sobald technisch möglich, kann eine Abfrage auch anhand eines Gesichtsbildes erfolgen.[851] Bei einem Treffer erhält die abfragende Stelle Kenntnis darüber, in welchem resp. welchen Mitgliedstaat(en) Strafregisterinformationen bezüglich der betroffenen Person vorliegen. Diese Information wird mit der entsprechenden nationalen Referenznummer sowie sämtlichen dazugehörigen Identitätsangaben bekannt gegeben. Das Resultat einer Abfrage im Zentralsystem darf nur zu bestimmten Zwecken verwendet werden, u.a. für ein Ersuchen um Informationen über Verurteilungen gemäss Art. 6 Rahmenbeschluss 2009/315/JI.[852] Als Antwort auf ein solches Ersuchen erhält die Zentralbehörde des ersuchenden Mitgliedstaats Informationen betreffend die erfassten strafrechtlichen Verurteilungen.[853]

Des Weiteren sind auch Europol, Eurojust und die Europäische Staatsanwaltschaft (EUStA)[854] berechtigt, das ECRIS-TCN direkt abzufragen, um für bestimmte Aufgaben in Erfahrung zu bringen, in welchen Mitgliedstaaten Strafregisterinformationen zu einem bestimmten Drittstaatsangehörigen vorliegen. Die Eingabe, Berichtigung oder Löschung von ECRIS-TCN-Daten ist diesen Einrichtungen resp. Agenturen jedoch untersagt. Bei einem Treffer können diese Agenturen resp. Einrichtungen die Mitgliedstaaten kontaktieren, um die Übermittlung der Strafregisterinformationen zu ersuchen.[855]

Ausserdem können die ETIAS-Zentralstelle sowie die nationalen ETIAS-Stellen für die Vornahme von bestimmten Überprüfungen auf ECRIS-TCN-Daten zugreifen.[856]

---

850 Siehe dazu Art. 7 Abs. 1 ECRIS-TCN-VO.

851 Art. 7 Abs. 5-6 ECRIS-TCN-VO.

852 Art. 7 Abs. 7-8 ECRIS-TCN-VO.

853 Siehe zu den Einzelheiten Art. 7 Rahmenbeschluss 2009/315/JI.

854 Bei der EUStA handelt es sich um eine unabhängige Stelle der EU. Sie ist im Bereich von Straftaten tätig, welche mit einem Nachteil für die finanziellen Interessen der EU verbunden sind. Sie führt strafrechtliche Untersuchungen, stellt die Verfolgung solcher Straftaten sicher und erhebt Anklage. Siehe für weitere Hinweise <https://www.consilium.europa.eu/de/policies/eppo/>, zuletzt besucht am 07.03.2025.

855 Art. 7 Abs. 3 ECRIS-TCN-VO; Art. 14 ECRIS-TCN-VO.

856 Siehe zu den Einzelheiten Art. 7b ECRIS-TCN-VO.

Ferner können auch Drittstaaten und internationale Organisationen für die Zwecke eines Strafverfahrens Eurojust um Auskunft ersuchen, um so in Erfahrung zu bringen, ob in den Mitgliedstaaten Strafregisterinformationen betreffend Drittstaatsangehörige vorliegen. Ergibt die Abfrage von Eurojust im ECRIS-TCN einen Treffer, so teilt Eurojust der ersuchenden Partei den Namen desjenigen Mitgliedstaats mit, in welchem Strafregisterinformationen vorhanden sind. Vorausgesetzt wird, dass der betreffende Mitgliedstaat dieser Bekanntgabe zustimmt. Mit der Nennung des Mitgliedstaats wird die ersuchende Partei ebenfalls darüber informiert, wie sie beim betreffenden Mitgliedstaat Auszüge aus dem Strafregister erfragen kann.[857]

9.6. Ausgewählte Sicherheitsmassnahmen

9.6.1. Übermittlung von ECRIS-TCN-Daten an Drittstaaten, internationale Organisationen und private Stellen

Grundsätzlich dürfen weder Eurojust, Europol, EUStA noch eine Zentralbehörde Informationen aus dem ECRIS-TCN betreffend eines Drittstaatsangehörigen an einen Drittstaat, eine internationale Organisation oder eine private Stelle übermitteln oder zur Verfügung stellen. Davon ausgenommen ist jedoch die vorstehend beschriebene Möglichkeit von Drittstaaten und internationalen Organisationen im Rahmen eines Auskunftsersuchens an Eurojust an ECRIS-TCN-Daten zu gelangen, sofern die entsprechenden Voraussetzungen erfüllt sind.[858]

9.6.2. Protokollierungspflicht

Alle im ECRIS-TCN vorgenommenen Datenbearbeitungen sind zu protokollieren. Diese Protokolle dienen ausschliesslich dazu, die Rechtmässigkeit der Datenverarbeitung sowie die Gewährleistung der Datenintegrität und -sicherheit zu überwachen.[859]

857 Art. 17 ECRIS-TCN-VO.

858 Art. 18 ECRIS-TCN-VO.

859 Siehe zu den Einzelheiten Art. 31 ECRIS-TCN-VO. Siehe zur Protokollierungspflicht bei ETIAS auch Art. 31b ECRIS-TCN-VO.

9.6.3. Rechte der betroffenen Personen

Drittstaatsangehörige können sowohl Auskunft, Berichtigung sowie auch die Löschung ihrer im ECRIS-TCN gespeicherten Daten verlangen. Entsprechende Anträge können an die Zentralbehörde eines beliebigen Mitgliedstaats gerichtet werden, wobei das Gesuch allenfalls an denjenigen Mitgliedstaat weitergeleitet wird, welcher die Daten in die Datenbank eingegeben hat. Wird die Berichtigung resp. die Löschung abgelehnt, ist eine Verwaltungsentscheidung oder eine gerichtliche Entscheidung zu erlassen, in welcher die Ablehnung begründet wird. Ausserdem muss der Mitgliedstaat den betroffenen Drittstaatsangehörigen darüber in Kenntnis setzen, mit welchen Rechtsmitteln gegen diese Entscheidung vorgegangen werden kann.[860]

9.6.4. Haftung und Sanktionen

Sowohl Personen als auch Mitgliedstaaten, welche u.a. durch eine rechtswidrige Datenverarbeitung im Rahmen des ECRIS-TCN geschädigt werden, können entweder bei dem Schaden verursachenden Mitgliedstaat oder bei eu-LISA, sofern diese ihren Verpflichtungen nicht nachgekommen ist, Schadenersatz verlangen. Diese können von der Haftung – ganz oder teilweise – befreit werden, sofern ihnen der Nachweis gelingt, dass sie nicht für den Schaden verantwortlich sind. Für Schäden am ECRIS-TCN haften die Mitgliedstaaten, Eurojust, Europol und EUStA, sofern diese den eigenen Verpflichtungen nicht nachgekommen sind, ausser wenn eu-LISA oder ein anderer Mitgliedstaat keine angemessenen Massnahmen ergriffen hat, damit der Schaden abgewendet resp. vermindert werden kann. Für die Geltendmachung dieser Ansprüche gegenüber einem Mitgliedstaat ist das nationale Recht des beklagten Mitgliedstaats einschlägig. Wird hingegen ein Schadenersatzanspruch gegenüber einer Agentur geltend gemacht, richtet sich dieser nach den entsprechenden Gründungsrechtsakten.[861]

Ausserdem sind im nationalen Recht sowie auch im Unionsrecht Sanktionen resp. Disziplinarmassnahmen vorzusehen, um jeglichen Missbrauch von ECRIS-TCN-Daten zu ahnden. Diese haben wirksam, verhältnismässig und abschreckend zu sein.[862]

---

860 Vgl. dazu Art. 25 ECRIS-TCN-VO. Siehe zu den Rechtsbehelfen auch Art. 27 ECRIS-TCN-VO.

861 Art. 20 ECRIS-TCN-VO.

862 Art. 22 ECRIS-TCN-VO.

10. Fazit

Die in diesem Kapitel dargestellten Informationssysteme sind – mit Ausnahme des ECRIS-TCN – der Schengener resp. der Dubliner Zusammenarbeit entsprungen. Das SIS, Eurodac und das VIS sind in der aufgeführten Reihenfolge im Abstand von jeweils rund acht Jahren ab 1995 in Betrieb genommen worden. Im Zuge der Entwicklungen im Sicherheits- und Migrationsbereich in Europa sind schliesslich – rund 20 Jahre nach der Inbetriebnahme des SIS – die gesetzlichen Grundlagen für das EES und ETIAS verabschiedet worden.[863] Obwohl mit diesen Schengen/Dublin-Informationssystemen unterschiedliche Ziele verfolgt werden, weisen sie doch denselben Ursprung auf, nämlich die Abschaffung der Binnengrenzen als Ziel von Schengen und somit letztlich auch von Dublin.

Aufgrund der Assoziierung an Schengen und Dublin beteiligt sich auch die Schweiz am SIS, Eurodac und VIS sowie zukünftig auch am EES und ETIAS.[864] Die gesetzlichen Grundlagen dieser Informationssysteme sind für die Schweiz mehrheitlich direkt anwendbar. Dennoch waren zur Umsetzung in der Schweiz stets auch Anpassungen im nationalen Recht nötig. Das ECRIS-TCN stellt keine Schengen/Dublin-Weiterentwicklung dar. Eine Beteiligung der Schweiz auf freiwilliger Basis wird derzeit geprüft.

Die gesetzlichen Grundlagen des SIS, der Eurodac-Datenbank sowie des VIS sind seit der Inbetriebnahme der Systeme den veränderten Bedürfnissen angepasst worden. Dabei ist die klare Tendenz zu beobachten, dass immer mehr Angaben von immer mehr Personengruppen erfasst und gespeichert werden und immer mehr (nationale) Stellen Zugriff auf diese Daten erhalten haben. Die Datenbearbeitung und der Anwendungsbereich dieser Informationssysteme wurden dadurch stetig umfangreicher resp. erweitert. Mit den noch in Betrieb zu nehmenden Systemen sollen nun bestimmte Daten von weiteren Personengruppen erhoben und gespeichert werden. Die Datenbearbeitung wird damit noch einmal stark ausgebaut.

---

863 Bei der Entstehung der Informationssysteme werden teilweise verschiedene Phasen unterschieden. Siehe dazu VAVOULA, EU immigration databases, 218 ff.; VAVOULA, Right to Private Life, 231 ff.

864 Ausgenommen davon ist der Zugang der nationalen Strafverfolgungsbehörden auf Eurodac-Daten. Aufgrund von einem separaten Abkommen wird dieser Zugang auch den nationalen Strafverfolgungsbehörden in der Schweiz ermöglicht werden. Siehe dazu Kapitel III.5.3.

Ein Blick auf die Anwendungsbereiche der Informationssysteme zeigt, dass primär Drittstaatsangehörige von der jeweiligen Datenbearbeitung betroffen sind.[865] Des Weiteren werden mit der Inbetriebnahme der neuen Systeme, insbesondere dem EES sowie dem ETIAS, zukünftig Daten von allen Drittstaatsangehörigen, welche sich in den Schengen-Raum begeben möchten, in mindestens einem der Informationssysteme erfasst.[866] Letztlich zielen die Informationssysteme darauf ab, Drittstaatsangehörige, welche sich nicht im Schengen-Raum aufhalten dürfen, zu lokalisieren, auszuweisen oder auszuschliessen. Dies betrifft sowohl Personen, die rechtmässig eingereist sind, als auch solche, die illegal eingereist sind.[867]

Ein Vergleich der gespeicherten Daten zeigt zudem auf, dass alle sechs Informationssysteme die Bearbeitung von alphanumerischen (insbesondere verschiedene Angaben zur Person sowie zum Reisedokument) und – abgesehen vom ETIAS – auch biometrischen Daten (insbesondere Fingerabdruckdaten und Gesichtsbilder) vorsehen. Identisch oder zumindest vergleichbar sind zudem die Bestimmungen der Informationssysteme zu den Rechten der betroffenen Personen, zum Betrieb durch eu-LISA, zur Aufsicht durch den EDSB und die nationalen Aufsichtsbehörden sowie zur Haftung und den Sanktionen.[868] Dabei handelt es sich aus datenschutzrechtlicher Perspektive zum Teil um wichtige Sicherheitsmassnahmen.[869]

Grundsätzlich unterschiedlich ist hingegen die Zielsetzung der sechs Informationssysteme. Eurodac, VIS, EES und ETIAS wurden primär für die Verfolgung von Zielen im Migrationsbereich errichtet. Mit dem VIS wurde erstmals neben den primär verfolgten Zielen im Migrationsbereich auch – als sog. sekundäres Ziel – festgehalten, dass VIS-Daten unter bestimmten Voraussetzun-

865 Nur ausnahmsweise sind Daten von anderen Personengruppen, z.B. UnionsbürgerInnen, betroffen. So. z.B. bei SIS-Ausschreibungen (siehe Kapitel III.4.4), beim VIS (dort werden Angaben von Sponsoren oder Familienmitgliedern erfasst. Siehe dazu Kapitel III.6.4) oder beim ECRIS-TCN (dort werden strafrechtlich verurteilte UnionsbürgerInnen erfasst, welche zusätzlich über eine Staatsangehörigkeit eines Drittstaats verfügen. Siehe dazu Kapitel III.9.4). Der Begriff «*Drittstaatsangehörige*» wird nicht in allen aufgeführten Informationssystemen definiert. Nur die gesetzlichen Grundlagen vom SIS sowie vom EES kennen eine entsprechende Definition. Demnach handelt es sich um Personen, welche keine UnionsbürgerInnen darstellen. Davon sind Personen ausgenommen, welche von einem Abkommen profitieren, welches ihnen ein gleichwertiges Recht auf Freizügigkeit gewährleisten. Siehe dazu Art. 3 Ziff. 4 SIS-Grenze-VO; Art. 3 Abs. 1 Ziff. 6 EES-VO.

866 Siehe dazu VAVOULA, Interoperability, 165.

867 JONES, 9 ff. m.w.H.

868 Vgl. zum Ganzen auch VAVOULA, IOP Privacy. Siehe zu den einzelnen Systemen Kapitel III.4; III.5; III.6; III.7; III.8 und III.9.

869 Siehe dazu Kapitel II.7.2 und II.7.3.

gen auch für Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten bearbeitet werden dürfen. In der Folge wurde die gesetzliche Grundlage von Eurodac entsprechend angepasst, um ebenfalls einen solchen Zugang – und damit verbunden eine entsprechende Zielsetzung – vorzusehen. Bei den noch in Betrieb zu nehmenden Informationssystemen EES und ETIAS ist – wie beim VIS – eine entsprechende Zugriffsberechtigung resp. Zielsetzung bereits bei der Errichtung des Informationssystems vorgesehen. Diese Entwicklung zeigt, dass ursprünglich für bestimmte Ziele im Migrationsbereich entwickelte Informationssysteme nun auch für die Verfolgung von Zielen aus dem Sicherheitsbereich eingesetzt werden.[870]

Am Beispiel des SIS ist zudem die gegenteilige Tendenz ersichtlich. Mit der neu eingeführten Ausschreibungskategorie Rückkehr finden nun auch Ziele aus dem Migrationsbereich Eingang in das SIS, welches bisher in der Strafverfolgung resp. der justiziellen Zusammenarbeit eingesetzt worden war. Am Beispiel vom ECRIS-TCN zeigt sich auch, dass dieses Informationssystem – abgesehen von der Verbesserung der justiziellen Zusammenarbeit – auch für diverse andere Zwecke (insbesondere auch für Zwecke aus dem Migrationsbereich) genutzt werden kann, sofern dies die Mitgliedstaaten vorsehen. Diese Entwicklungen machen deutlich, dass die ursprünglich klar gezogenen Grenzen zwischen der Verfolgung von Zielen aus dem Migrations- resp. Sicherheitsbereich zunehmend verwischt werden.[871]

Trotz der Vermengung von verschiedenen Zielen und auch unabhängig davon, dass die Informationssysteme verschiedene Gemeinsamkeiten resp. Ähnlichkeiten aufweisen, stellen die sechs Informationssysteme (bis anhin) in sich geschlossene Systeme dar. Sie sind insofern eigenständig, als sie u.a. auf einer eigenen gesetzlichen Grundlage errichtet wurden und spezifische Zwecke verfolgen. Ursprünglich waren zwischen diesen Informationssystemen kaum Berührungspunkte vorhanden.[872] Mit den noch in Betrieb zu nehmenden Informationssystemen EES, ETIAS und ECRIS-TCN werden vermehrt Verbindungen zwischen diesen sechs Informationssystemen geschaffen. So sind die Informationssysteme VIS und EES insofern miteinander verbunden als gegenseitige Abfragen möglich sind und zudem auch Daten von der einen in die

870 Siehe dazu auch VAVOULA, IOP Privacy.

871 Siehe dazu VAVOULA, Deathblow, 135.

872 Eine Verbindung zwischen den Systemen besteht jedoch z.B. darin, dass für die Bearbeitung eines Antrags für ein kurzfristiges Schengen-Visum eine Abfrage in der SIS-Datenbank vorgenommen wird. Siehe dazu Kapitel III.6.4.

jeweils andere Datenbank gezogen werden können.[873] Ausserdem erfolgt im Zuge der Datenbearbeitung im ETIAS eine automatisierte Abfrage in den anderen fünf Informationssystemen.[874] Weiter geht aus den gesetzlichen Grundlagen der Informationssysteme hervor, dass diese zunehmend nicht nur der Erreichung ihrer eigenen Ziele dienen, sondern damit vermehrt auch die Erreichung der Ziele von anderen Informationssystemen anvisiert ist.[875]

Mit der Interoperabilität werden diese Informationssysteme – unabhängig von den bereits bestehenden Verbindungen – noch intensiver miteinander verknüpft. Die Interoperabilität beabsichtigt, dass die ursprünglich eigenständige Struktur der Systeme aufgebrochen wird und gemeinsame Strukturen geschaffen werden. Was genau unter dieser Interoperabilität zu verstehen ist und vor welchem Hintergrund sie entstanden ist, wird im folgenden Kapitel näher dargestellt.

873 Siehe dazu Kapitel III.7.2.
874 Siehe dazu Kapitel III.8.4.
875 Siehe dazu z.B. Art. 4 Bst. e und ea ETIAS-VO. Vgl. dazu auch VAVOULA, Interoperability, 182.

IV. Interoperabilität

1. Einleitung

Im vorliegenden Kapitel wird erklärt, was unter der Interoperabilität der EU-Informationssysteme zu verstehen ist. Bevor auf die Einzelheiten dieses EU-Grossprojekts eingegangen wird, drängt sich eine Erklärung des Begriffs «*Interoperabilität*» in allgemeiner Weise auf. Unter Berücksichtigung der Ausführungen im vorangehenden Kapitel zu den von der Interoperabilität umfassten Informationssystemen sollen einige Erläuterungen zur Entstehungsgeschichte helfen, das Projekt und das damit verfolgte Ziel besser einzuordnen. Im Fokus stehen anschliessend die vier Interoperabilitätskomponenten, welche die mit der Interoperabilität beabsichtigte Verknüpfung der involvierten Informationssysteme ermöglichen sollen. Im Anschluss wird auf die Ausgestaltung des Projekts in der Schweiz eingegangen. Das Fazit hebt schliesslich die wichtigsten Erkenntnisse zur Interoperabilität hervor.

2. Bedeutung des Begriffs «*Interoperabilität*»

Der Begriff «*Interoperabilität*» wird vielfältig verwendet. Insbesondere im Zusammenhang mit den von der Interoperabilität betroffenen Informationssystemen ist der Begriff häufig anzutreffen. So sind die noch nicht in Betrieb genommenen Systeme EES und ETIAS bereits mit dem Gedanken der Interoperabilität konzipiert worden. Das EES ist mit dem VIS interoperabel.[876] Aber auch bezüglich dem bei ETIAS vorgesehenen automatisierten Abgleich mit verschiedenen Datenbanken taucht der Begriff vielfach auf.[877]

Bezugnehmend auf Informationssysteme umschrieb der EDSB den Begriff der Interoperabilität als «*im Allgemeinen die Fähigkeit verschiedener Informationssysteme zur Kommunikation, zum Austausch von Daten und zur Nutzung der ausgetauschten Informationen*».[878] Obwohl Interoperabilität häufig als rein technisches Konzept verstanden werde, sei dennoch eine politische Debatte

---

876 Siehe dazu Art. 8 EES-VO; Art. 17a VIS-VO. Siehe zu den interoperablen Aspekten der EU-Informationssysteme auch VAVOULA, Interoperability, 169 f.

877 So explizit in Art. 11 ETIAS-VO. Siehe dazu zudem u.a. auch Art. 18b VIS-VO; Art. 8b EES-VO.

878 EDSB, Reflexionspapier IOP, N 7.

betreffend den Zweck sowie den geplanten Geltungsbereich zu führen. Des Weiteren führte der EDSB aus, dass Interoperabilität grundsätzlich verschiedene Formen aufweisen könne. So könne diese in einer reinen Kommunikationsinfrastruktur zwischen zwei Systemen bestehen, jedoch auch die Fähigkeit dieser Systeme umfassen, Informationen auszutauschen und diese zu verwenden.[879]

Abgesehen von der Verwendung im Zusammenhang mit Informationssystemen wird der Begriff auch in anderen Bereichen verwendet, so z.B. beim grenzüberschreitenden Verkehr[880] oder bezüglich des öffentlichen Sektors der Union[881].

Für die vorliegende Arbeit wird der Begriff ausschliesslich im Zusammenhang mit dem Grossprojekt «*Interoperabilität der EU-Informationssysteme*» verwendet.[882] Dieses Projekt wird nachfolgend näher erläutert. Auf dieses Projekt bezogen beschrieb die Kommission den Begriff der Interoperabilität als «*die Fähigkeit von Informationssystemen, Daten auszutauschen und die gemeinsame Nutzung von Informationen zu ermöglichen*».[883] Folglich sollen die betroffenen Informationssysteme im Rahmen der Interoperabilität der EU-Informationssysteme befähigt werden, miteinander zu kommunizieren, Daten auszutauschen und diese Daten zu verwenden. Das geschlossene Umfeld der einzelnen Systeme wird durchbrochen und zu einem gemeinsamen Umfeld.[884]

879 EDSB, Reflexionspapier IOP, N 9. Der Aussage, dass die Interoperabilität ein technischer und nicht ein rechtlicher resp. politischer Begriff sei, konnte der EDSB bereits früher nicht (uneingeschränkt) zustimmen. Siehe dazu EDSB, Kommentare IOP 2006, 2. Siehe zu dieser Thematik auch De Hert/Gutwirth, police databases, 22 f., 31 f., wobei dieser Beitrag nicht auf die Interoperabilität gemäss dem Verständnis der vorliegenden Untersuchung Bezug nimmt, sondern auf eine davor geplante Verknüpfung von Informationssystemen.

880 Die EU hat im Bereich des grenzüberschreitenden Verkehrs in Europa bestimmte Anforderungen, die sog. technischen Spezifikationen für die Interoperabilität (TSI), festgelegt. Siehe dazu <https://www.bav.admin.ch/bav/de/home/verkehrsmittel/eisenbahn/fachinformationen/interoperabilitaet/tsi.html>, zuletzt besucht am 07.03.2025.

881 Mit einem Vorschlag wird angestrebt, die grenzüberschreitende Interoperabilität von Netz- und Informationssystemen zu fördern, welche zwecks Erbringung resp. Verwaltung öffentlicher Dienste in der Union genutzt werden. Siehe zum Vorschlag Europäische Kommission, COM(2022) 720 final.

882 Bereits vor diesem Projekt gab es Bestrebungen, Informationssysteme interoperabel auszugestalten (so z.B. das VIS mit dem SIS). Selten wurden jedoch konkrete Projekte ausgearbeitet. Siehe dazu Alegre/Jeandesboz/Vavoula, 35 f. m.w.H.

883 Europäische Kommission, COM(2016) 205 final, 17.

884 Vgl. dazu HLEG, final report, 49.

3. Geschichtlicher Hintergrund

Die Debatte zu einer möglichen Verknüpfung von Datenbanken startete bereits im Nachgang zu den Ereignissen vom 11. September 2001. Damals wurde in Betracht gezogen, das zu diesem Zeitpunkt noch in der Verhandlungsphase befindliche VIS mit dem SIS zu verknüpfen oder in dieses zu integrieren. Nach den Bombenanschlägen in Madrid im Jahr 2004 wurde die Kommission vom Rat aufgefordert, Vorschläge für eine erhöhte Interoperabilität zwischen dem damaligen SIS II, dem VIS und Eurodac zu erarbeiten. Diese Projekte wurden jedoch nie umgesetzt.[885]

Stattdessen wurden andere Projekte verwirklicht, welche insbesondere dazu führten, dass die Datenbearbeitung im Bereich der Gefahrenabwehr sowie der Strafverfolgung intensiviert wurde. So wurde z.B. im Jahr 2006 die RL 2006/24/EG verabschiedet, welche die Verwendung von bestimmten Kommunikationsdaten für Strafverfolgungszwecke vorsah.[886] Zwei Jahre später wurden die Beschlüsse 2008/615/JI und 2008/616/JI, die sog. «*Prümer Beschlüsse*», angenommen. Damit sollte der grenzüberschreitende Austausch von Informationen und Erkenntnissen für strafrechtliche Ermittlungen resp. polizeiliche Erkenntnisgewinnungsverfahren vereinfacht werden. Im Rahmen der Prümer Zusammenarbeit können insbesondere Daten wie DNA-Profile, Fingerabdrücke und Daten aus Fahrzeugregistern zwischen den beteiligten Staaten ausgetauscht werden. Ausserdem wurden zunehmend auch Fluggastdaten, die sog. «*PNR-Daten*», im Kampf gegen den Terrorismus und andere Formen schwerer Kriminalität bearbeitet.[887]

Erst aufgrund von neuen Migrations- und Sicherheitsbedrohungen wurde die Debatte über die Verknüpfung von Informationssystemen vor einigen Jahren wieder aktuell.[888] Aufgrund der Flüchtlingskrise im Jahr 2015 sowie den verschiedenen Terroranschlägen in der EU wurde ein neues Konzept erarbeitet, um den Schutz der EU-BürgerInnen gewährleisten zu können. Dabei wurde insbesondere eine Stärkung des Grenzmanagements sowie der Zusammenarbeit in den Bereichen Migration und Sicherheit angestrebt. Ausserdem sollten

885 Vavoula, Deathblow, 136. Insbesondere der EDSB äusserte sich dazu kritisch. Siehe dazu Gutheil, et al., 9; EDSB, Kommentare IOP 2006, 2 ff.

886 Vgl. dazu Art. 1 Abs. 1 RL 2006/24/EG. Diese Richtlinie wurde im Urteil EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238 für ungültig erklärt.

887 Siehe zum Ganzen Europäische Kommission, KOM(2010)385 endg., 2 f.

888 Vavoula, Deathblow, 136 f.

die Synergien der bereits in den Bereichen Grenzschutz, Migration sowie Sicherheit bestehenden Informationssysteme besser genutzt werden.[889]

4. Entstehung der Interoperabilität

In einer Mitteilung im April 2016 machte die Kommission auf verschiedene strukturelle Mängel der bestehenden Informationssysteme aufmerksam. Die Kommission führte aus, dass diese mangelhaft funktionierten. Zudem seien Lücken in der Datenverwaltungsarchitektur vorhanden, d.h. von bestimmten Personengruppen würden keine Daten vorliegen.[890] Ausserdem seien die Informationssysteme sehr komplex. So könne unklar sein, in welchem System eine Abfrage vorzunehmen sei. Des Weiteren sei die Datenverwaltungsarchitektur im Bereich des Grenzmanagements fragmentiert. So seien die Daten in verschiedenen Systemen gespeichert, wobei zwischen diesen Inkompatibilitäten vorhanden seien. Hinzu komme, dass die Zugriffsmöglichkeiten unterschiedlich ausgestaltet seien. Daraus resultiere insbesondere für die Strafverfolgungsbehörden ein «*lückenhaftes Gesamtbild*».[891]

In derselben Mitteilung stellte die Kommission vier Aspekte vor, um die Informationssysteme interoperabel zu machen: eine zentrale Schnittstelle, welche die gleichzeitige Abfrage in mehreren Informationssystemen erlaubt; die Interoperabilität von Informationssystemen (worunter das automatische Abfragen von in einem anderen System erfassten Daten verstanden wurde); ein gemeinsamer Dienst für den Abgleich biometrischer Daten sowie – als Kernmodul – ein gemeinsamer Datenspeicher für verschiedene Informationssysteme. Ebenfalls in dieser Mitteilung wurde die Einsetzung einer Sachverständigengruppe beschlossen, welche die rechtlichen, technischen sowie operativen Aspekte der geplanten Interoperabilität der Informationssysteme analysieren sollte. Zudem sollte sie auch die Notwendigkeit, die technische Machbarkeit und die Verhältnismässigkeit von verschiedenen Optionen sowie deren Auswirkungen auf den Datenschutz prüfen.[892]

---

889 Vgl. dazu Europäische Kommission, Vorschlag IOP-Grenze, 1; Europäische Kommission, COM(2016) 205 final, 2 f. Siehe zu den Entwicklungen in Europa (sowie in den USA) hinsichtlich neuer Informationssysteme, Prüm, PNR sowie der Interoperabilität Bossung, 7 ff.

890 So z.B. Drittstaatsangehörige, welche ein Visum für einen längerfristigen Aufenthalt benötigen oder solche, die visumbefreit einreisen dürfen.

891 Siehe zum Ganzen Europäische Kommission, COM(2016) 205 final, 1 ff.

892 Europäische Kommission, COM(2016) 205 final, 17 ff. m.w.H. Siehe auch HLEG, Scoping Paper mit weiteren Einzelheiten zum Auftrag resp. Vorgehensweise der Sachverständigengruppe.

Diese Sachverständigengruppe, die sog. hochrangige Expertengruppe für Informationssysteme und Interoperabilität (HLEG), legte im Dezember 2016 resp. im Mai 2017 in ihrem Zwischen- resp. Abschlussbericht ihre Empfehlungen vor.[893] Die HLEG gelangte zum Ergebnis, dass es notwendig und zudem technisch machbar sei, auf die folgenden drei Komponenten hinzuarbeiten, um die Interoperabilität im Einklang mit dem Datenschutz zu ermöglichen: ein europäisches Suchportal (ESP), ein gemeinsamer Dienst für den Abgleich biometrischer Daten (BMS) sowie ein gemeinsamer Speicher für Identitätsdaten (CIR). Hinsichtlich der von der Kommission vorgeschlagenen Komponente der Interoperabilität befand die HLEG, dass diese lediglich zurückhaltend eingesetzt werden sollte.[894] Die Kommission verkündete in der Folge, einen Vorschlag betreffend die Interoperabilität der Informationssysteme zu erarbeiten.[895]

Zur Vorbereitung dieses Vorschlags wurde von der Kommission im Juli 2017 eine öffentliche Konsultation eingeleitet, wobei eine erste Folgenabschätzung als Begleitdokument zur Verfügung stand.[896] Verschiedene Rückmeldungen von Regierungen der Mitgliedstaaten, diversen Organisationen, Denkfabriken sowie auch Privatpersonen sind im Rahmen dieser Konsultation eingegangen. Mehrheitlich wurde der Vorschlag zur Interoperabilität positiv aufgenommen.[897]

---

893 Siehe zu den Berichten: HLEG, Interim Report; HLEG, final report. Die Expertengruppe setzte sich aus ExpertInnen der Mitgliedstaaten und der assoziierten Staaten sowie den EU-Agenturen eu-LISA, Europol, Frontex, FRA und EASO zusammen, wobei auch der EU-Koordinator für die Terrorismusbekämpfung und der EDSB als volle Mitglieder zur Expertengruppe gehörten. Davon abgesehen gab es auch Beobachter. Siehe dazu HLEG, Interim Report, 2. Eine Liste der beteiligten Akteure der Expertengruppe findet sich im Anhang des Dokuments.

894 HLEG, final report, 40. Zu diesen drei Komponenten kam später noch eine vierte dazu. Es handelt sich dabei um den Detektor für Mehrfachidentitäten (MID). Siehe dazu Jones, 15.

895 Europäische Kommission, COM(2017) 650 final, 9.

896 Siehe dazu European Commission, Inception impact assessment IOP. In dieser ersten Folgenabschätzung wurden drei Varianten geprüft. Der EDSB kritisierte diese insofern, als er feststellte, dass in der Folgenabschätzung zwar Probleme aufgeführt werden, aber nicht ersichtlich sei, worum es eigentlich gehe. Es sei häufig unklar, ob es sich um ein technisches oder um ein rechtliches Problem handle. Dies wäre jedoch von zentraler Bedeutung, da je nachdem dem Problem mit anderen Massnahmen begegnet werden müsse. Siehe dazu EDSB, Reflexionspapier IOP, N 17 ff.

897 Europäische Kommission, Vorschlag IOP-Grenze, 17; European Commission, Impact assessment IOP Part 2, 6 f.

Am 17. November 2017 wurde vom EDSB ein Reflexionspapier zur geplanten Interoperabilität vorgelegt.[898] Daraus geht hervor, dass die Interoperabilität ein «*hilfreiches Instrument*» darstellen könne, sofern diese sorgfältig durchdacht und deren Umsetzung notwendig und verhältnismässig sei. Die Interoperabilität hätte grundsätzlich auch dahingehend ausgestaltet werden können, dass lediglich die Nutzung der Systeme erleichtert und die jeweiligen Vorschriften wirksamer und effizienter gemacht würden. Die Kommission strebe aber eine Ausdehnung des Austauschs oder Abgleichs von Daten an. Darin seien neue Formen der Datenbearbeitungen zu sehen, welche durch die damaligen Rechtsgrundlagen nicht abgedeckt seien. Insbesondere forderte der EDSB die Kommission auf, die Probleme, welche die Interoperabilität lösen sollte, klar zu umreissen. Ebenfalls seien die spezifischen Zwecke festzulegen, für welche bestimmte Daten verarbeitet werden dürften.[899]

Am 12. Dezember 2017 präsentierte die Kommission schliesslich zwei Legislativvorschläge.[900] Dabei hielt die Kommission fest, dass durch die Interoperabilität die bestehenden Zugriffsrechte nicht geändert würden. Es solle demnach nicht mehr Einblick in Daten gewährt werden, als die bestehenden gesetzlichen Grundlagen bereits erlaubten.[901]

Diese beiden Vorschläge wurden von einer (weiteren) Folgenabschätzung begleitet.[902] Darin wurde bezüglich der von der HLEG präferierten Variante mit den drei Komponenten (also dem ESP als Europäisches Suchportal, dem BMS als gemeinsamer Dienst für den Abgleich biometrischer Daten sowie dem CIR als gemeinsamer Speicher für Identitätsdaten) festgestellt, dass das SIS aufgrund seiner komplexen Struktur nicht in den CIR integriert werden könne. Um die daraus resultierende Lücke zu schliessen, könnte eine vierte Komponente, der Detektor für Mehrfachidentitäten (MID), eingeführt werden. Letztlich wurde festgehalten, dass nur mit vier Komponenten alle Ziele erreicht werden könnten. Zudem wurde postuliert, die Regeln für Identitätskontrollen im Hoheitsgebiet der Mitgliedstaaten müssten vereinfacht und der Zugang der Strafverfolgungsbehörden für die Prävention, Untersuchung, Aufdeckung oder

898 Siehe dazu EDSB, Reflexionspapier IOP.

899 Siehe dazu EDSB, Reflexionspapier IOP, N 37 ff.

900 Vgl. dazu Europäische Kommission, Vorschlag IOP-Grenze; Europäische Kommission, Vorschlag IOP-Polizei.

901 FRA, Opinion IOP, 10.

902 Diese besteht aus zwei Teilen, in welchen drei verschiedene Optionen vorgestellt wurden. Siehe zu den Einzelheiten European Commission, Impact assessment IOP Part 1; European Commission, Impact assessment IOP Part 2.

Verfolgung schwerer Kriminalität und Terrorismus auf Systeme anderer Behörden erleichtert und einheitlich geregelt werden.[903]

Zu den beiden Vorschlägen der Kommission haben sowohl die Artikel-29-Datenschutzgruppe (WP29), die Agentur der Europäischen Union für Grundrechte (FRA) sowie der EDSB im April 2018 Stellung genommen und verschiedene Empfehlungen formuliert.[904]

Noch vor der Veröffentlichung der beiden Vorschläge zur Interoperabilität der EU-Informationssysteme wurde im September 2017 eine Machbarkeitsstudie zur Komponente ESP erarbeitet.[905] Später folgten weitere Machbarkeitsstudien zu den Komponenten CIR und BMS und eine weitere zur Interoperabilität der Informationssysteme.[906] Diese Machbarkeitsstudien prüften – insbesondere in technischer Hinsicht – jeweils verschiedene Varianten der Umsetzung.[907]

Nach der Vornahme von einigen Anpassungen wurden schliesslich zwei Verordnungen, die VO 2019/817 (IOP-Grenze-VO) und die VO 2019/818 (IOP-Polizei-VO), vom Europäischen Parlament und vom Rat der EU im Mai 2019 angenommen.[908] In der EU traten die beiden Verordnungen am 11. Juni 2019 in Kraft. Die Inbetriebnahme der Interoperabilität steht noch aus. Für die Inbetriebnahme wird u.a. ein erfolgreicher Abschluss eines umfassenden Tests der Komponenten vorausgesetzt, welcher in Zusammenarbeit der Schengen-Staaten sowie den europäischen Agenturen erfolgt. Ausserdem müssen die technischen sowie auch rechtlichen Rahmenbedingungen für die Erhebung resp.

---

903 Siehe dazu EUROPEAN COMMISSION, Impact assessment IOP Part 1, 16 ff. m.w.H. Diese Folgenabschätzung wurde verschiedentlich kritisiert. Siehe z.B. EISELE, impact assessment; WP29, Opinion proposals IOP, 3. Siehe zu einer ausführlichen Beurteilung der Stärken und Schwächen dieser Folgenabschätzung EISELE, Initial Appraisal.

904 Siehe dazu WP29, Opinion proposals IOP; FRA, Opinion IOP; EDSB, Stellungnahme Vorschläge EU-IOP-VO. Vgl. zur Stellungnahme der FRA auch RIEHLE. Per 25. Mai 2018 wurde die WP29 vom European Data Protection Board (EDPB) abgelöst. Siehe dazu und zu einem Überblick über die Stellungnahme der WP29 WAHL, Interoperability.

905 Siehe eine Zusammenfassung der Machbarkeitsstudie zum ESP EUROPEAN COMMISSION, Impact assessment IOP Part 2, Anhang 5.

906 Siehe dazu EUROPEAN COMMISSION, Feasibility Study CIR; EU-LISA, Feasibility Study sBMS; EU-LISA, Feasibility Study Summary IOP. Es wurde kritisiert, dass zum BMS, CIR und MID im Zeitpunkt der Veröffentlichung der Vorschläge der EU-IOP-VO jeweils keine eingehende Folgenabschätzung vorgelegen hatte. Siehe dazu QUINTEL, data retention, 15.

907 Bei den Machbarkeitsstudien handelt es sich im Allgemeinen primär um technische Berichte, in welchen mögliche Auswirkungen der untersuchten Änderungen nur sehr begrenzt diskutiert werden. Vgl. dazu VAVOULA, Police Information Exchange, 26.

908 CASSANI, et al., 459.

Übermittlung der Daten vorhanden sein. Die einzelnen Komponenten werden zeitlich gestaffelt in Betrieb genommen, wobei verschiedene Übergangsphasen vorgesehen sind.[909]

5. Ausgestaltung der Interoperabilität

5.1. Gesetzliche Grundlage

Als gesetzliche Grundlage für die Interoperabilität wurden zwei Rechtsakte geschaffen. Dies ist darauf zurückzuführen, dass von der Interoperabilität Informationssysteme betroffen sind, welche entweder dem Schengen-Besitzstand im Bereich Grenzen und Visa oder dem Schengen-Besitzstand im Bereich der polizeilichen Zusammenarbeit zuzuordnen resp. ausserhalb der Schengen-Zusammenarbeit angesiedelt sind.[910] Die IOP-Grenze-VO deckt die Bereiche Grenzen und Migration ab, die IOP-Polizei-VO hingegen die polizeiliche und justizielle Zusammenarbeit, Asyl und Migration.[911] Diese beiden Verordnungen, die EU-IOP-VO, sind weitgehend deckungsgleich. Damit werden keine neuen Datenbanken geschaffen. Es werden jedoch neue Funktionen für bereits bestehende resp. neue Informationssysteme eingeführt.[912] Die Interoperabilität wird primär in den EU-IOP-VO geregelt, wobei diese beiden Rechtsakte in gewissen Bestimmungen den Erlass von Durchführungsrechtsakten ermöglicht.[913]

---

909 BUNDESRAT, Botschaft IOP, 8002. In der Planungsphase der Interoperabilität wurde davon ausgegangen, dass diese bis im Jahr 2020 umgesetzt werden kann. Siehe dazu EUROPÄISCHE KOMMISSION, COM(2017) 261 final, 2, 8, 10.

910 EDSB, Stellungnahme Vorschläge EU-IOP-VO, 9.

911 Gemäss Art. 3 Abs. 1 IOP-Grenze-VO gilt diese Verordnung für die Systeme EES, VIS, ETIAS und SIS. Die IOP-Polizei-VO hingegen für Eurodac, das SIS sowie das ECRIS-TCN (Art. 3 Abs. 1 IOP-Polizei-VO). Die EU-IOP-VO enthalten keine konkreten Verweise auf die gesetzliche Grundlage von Eurodac. Aufgrund der Revision der Eurodac-VO sollen die EU-IOP-VO für Eurodac erst ab dem Tag der Anwendbarkeit der Neufassung der Eurodac-VO gelten. Siehe dazu Art. 75 IOP-Polizei-VO; Art. 79 IOP-Grenze-VO; BUNDESRAT, Botschaft IOP, 8002 f.

912 BUNDESRAT, Botschaft IOP, 8000.

913 So z.B. in Art. 37 Abs. 4 EU-IOP-VO.

5.2. Betroffene Informationssysteme

Von der Interoperabilität sind primär die Informationssysteme SIS, Eurodac, VIS, EES, ETIAS sowie ECRIS-TCN betroffen. Diese Systeme wurden im vorangehenden Kapitel bereits dargestellt.[914]

5.3. Interoperabilitätskomponenten

Die vier Interoperabilitätskomponenten – das ESP, der BMS, der CIR und der MID – stellen das Herzstück der Interoperabilität dar und unterstützen resp. ergänzen sich gegenseitig. Erst das Zusammenspiel dieser Komponenten ermöglicht es, die Zielsetzung der Interoperabilität zu erreichen.[915]

Abgesehen davon unterstützt der zentrale Speicher für Berichte und Statistiken (CRRS) die Interoperabilität. Dieser stellt u.a. systemübergreifende statistische Daten und analytische Berichte für politische und operative Zwecke sowie für die Zwecke der Datenqualität bereit, wobei die Daten anonymisiert sind.[916] Mit dem Universellen Nachrichtenformat (UMF) wird zudem die Interaktion zwischen mehreren Systemen ermöglicht. Dabei handelt es sich um einen gemeinsamen Standard für den grenzüberschreitenden Informationsaustausch, welcher beim EES, ETIAS, Eurodac, ECRIS-TCN, ESP, CIR und MID verwendet werden soll.[917]

5.3.1. Europäisches Suchportal

Das ESP besteht aus einer zentralen Infrastruktur sowie einem Suchportal, welches die gleichzeitige Abfrage im SIS, Eurodac, VIS, EES, ETIAS sowie im ECRIS-TCN ermöglicht. Zudem wird ein sicherer Kommunikationskanal zwischen dem ESP und den nutzungsberechtigten Stellen eingerichtet. Eine sichere Kommunikationsinfrastruktur zwischen dem ESP und den genannten

914 Siehe dazu Kapitel III.4; III.5; III.6; III.7; III.8 und III.9. Wie dort bereits erwähnt, wird der Einbezug der Europol-Daten sowie Daten von zwei Interpol-Datenbanken in die Interoperabilität in der vorliegenden Untersuchung nicht näher analysiert.

915 BUNDESRAT, Botschaft IOP, 8003. Siehe zu den Interoperabilitätskomponenten Art. 1 Abs. 2 EU-IOP-VO.

916 Siehe zum CRRS Art. 39 EU-IOP-VO. Siehe dazu auch EUROPÄISCHE KOMMISSION, Vorschlag IOP-Grenze, 11 f.

917 Siehe zum UMF Art. 38 EU-IOP-VO. Siehe dazu auch EUROPÄISCHE KOMMISSION, Vorschlag IOP-Grenze, 11 f.; BUNDESRAT, Botschaft IOP, 8015 f.

Datenbanken sowie den Interoperabilitätskomponenten CIR und MID ist ebenfalls vorgesehen.[918]

Das ESP soll den zugriffsberechtigten Stellen einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den EU-Informationssystemen ermöglichen, wobei die in den gesetzlichen Grundlagen gewährten Zugriffsrechte der einzelnen Systeme nicht verändert werden. Um dies zu gewährleisten werden verschiedene Nutzer-Profile erstellt.[919] Diese legen fest, auf welche Datenbanken der Nutzer zugreifen darf, welche spezifischen Daten abgefragt und welche Kategorien von Daten als Abfrageergebnis ausgegeben werden dürfen.[920]

Die ESP-Nutzer können anhand der Eingabe von alphanumerischen und/oder biometrischen Daten eine Abfrage im ESP starten. Die Abfrage erfolgt im EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN sowie im CIR. Resultiert ein Treffer, werden die Daten, auf welche der Nutzer gemäss dem Unionsrecht resp. dem nationalen Recht zugreifen darf, über das ESP angezeigt. Dabei wird dem Nutzer auch bekannt gegeben, aus welchem Informationssystem die Daten stammen.[921] Das ESP wird ferner auch für die in den EU-IOP-VO vorgesehenen drei Abfragemöglichkeiten des CIR verwendet.[922] Das ESP wird zudem auch benötigt, um die Prüfung auf Mehrfachidentitäten vorzunehmen.[923] Sowohl auf die Abfragen des CIR als auch auf die Prüfung auf Mehrfachidentitäten wird im Folgenden noch näher eingegangen.[924]

---

918 Art. 6 Abs. 2 EU-IOP-VO.

919 Siehe dazu Art. 6 Abs. 1 EU-IOP-VO; Art. 8 EU-IOP-VO.

920 Die Zugriffsberechtigungen sind den Rechtsgrundlagen der einzelnen Systeme zu entnehmen. Mindestens jährlich werden diese Nutzerprofile von eu-LISA zusammen mit den Schengen-Staaten überprüft und ggf. angepasst. Siehe dazu BUNDESRAT, Botschaft IOP, 8005.

921 Davon ausgenommen sind die Abfragen des CIR zu Identifikationszwecken. Siehe dazu Art. 20 EU-IOP-VO. Dabei steht lediglich die Identifikation der Person im Vordergrund. Die zuständigen Polizeibehörden sollen keine Kenntnis darüber erhalten, aus welchem System die Daten stammen. Wird der CIR gemäss Art. 22 EU-IOP-VO abgefragt, werden die nationalen Strafverfolgungsbehörden lediglich darüber informiert, ob Daten in einem System vorhanden sind. Der Zugang zu den Daten muss separat beantragt werden. Siehe zum Ganzen Art. 8 EU-IOP-VO; Art. 9 EU-IOP-VO. Siehe zur Nutzung des ESP auch Art. 7 EU-IOP-VO; BUNDESRAT, Botschaft IOP, 8003 ff.

922 Art. 7 Abs. 2 EU-IOP-VO.

923 Siehe dazu Art. 27 Abs. 3 EU-IOP-VO.

924 Siehe zu den Abfragen des CIR Kapitel IV.5.3.3 sowie Kapitel V.3.4.3; V.3.4.4 und V.3.4.5. Siehe zur Prüfung auf Mehrfachidentitäten Kapitel IV.5.3.4 sowie Kapitel V.3.4.7.

Das ESP verarbeitet und speichert keine Daten, sondern fungiert als Schnittstelle und ermöglicht die gleichzeitige Abfrage der im Rahmen der Interoperabilität miteinander verknüpften Informationssysteme. Unter Wahrung der jeweiligen Zugriffsrechte können dem Nutzer somit zeitnah die Ergebnisse der Suchabfrage in allen Informationssystemen, bezüglich welchen sie zugriffsberechtigt sind, zur Verfügung gestellt werden. Dies erleichtert die Nutzung der betroffenen Informationssysteme massgeblich.[925]

Alle nationalen Behörden sowie auch die europäischen Agenturen können das ESP nutzen, sofern sie auf mindestens eines der sechs an das ESP angeschlossenen Informationssysteme oder die Interoperabilitätskomponenten CIR resp. MID Zugriff haben.[926] Über die vorgenommenen Abfragen im ESP haben eu-LISA, die Stellen der Union resp. die Schengen-Staaten Protokoll zu führen.[927] Für die Entwicklung des ESP sowie auch dessen technische Verwaltung ist eu-LISA zuständig.[928]

5.3.2. Gemeinsamer Dienst für den Abgleich biometrischer Daten

Mit dem BMS sollen systemübergreifende Abfragen mit biometrischen Daten ermöglicht werden.[929] Die biometrischen Daten, welche im Rahmen der Interoperabilität bearbeitet werden, beschränken sich auf Fingerabdruckdaten sowie Gesichtsbilder.[930] Der Abgleich wird mittels biometrischen Templates vor-

925 Europäische Kommission, Vorschlag IOP-Grenze, 7; Europäische Kommission, COM(2016) 205 final, 18; Fiolka/Stalder, 174.

926 Bundesrat, Botschaft IOP, 8004 f.

927 Bundesrat, Botschaft IOP, 8005; Art. 10 EU-IOP-VO.

928 Art. 6 Abs. 3 EU-IOP-VO.

929 Der BMS wird teilweise auch «*shared biometric matching system*» (sBMS) genannt. Siehe dazu z.B. Bundesrat, Botschaft IOP, 8022. Zur Vermeidung von Unklarheiten wird in der vorliegenden Untersuchung stets die Bezeichnung «BMS» verwendet.

930 Siehe dazu Art. 4 Ziff. 11 EU-IOP-VO. Beim Gesichtsbild handelt es sich um «*eine digitale Aufnahme des Gesichts einer Person*» (siehe dazu Ziff. 10 derselben Bestimmung). Diese Definition deckt sich zumindest sinngemäss mit derjenigen, welche in den gesetzlichen Grundlagen der Systeme, welche solche Daten bearbeiten, verwendet wird (siehe dazu Art. 3 Ziff. 15 SIS-Grenze-VO; Art. 3 Abs. 1 Ziff. 17 EES-VO; Art. 3 Ziff. 13 ECRIS-TCN-VO). Unter dem Begriff Fingerabdruckdaten werden Fingerabdrücke sowie Fingerabdruckspuren verstanden, welche «*aufgrund ihrer Einzigartigkeit und der darin enthaltenen Bezugspunkte präzise und schlüssige Abgleiche zur Identität einer Person ermöglichen*» (siehe dazu Art. 4 Ziff. 9 EU-IOP-VO). Diese Definition unterscheidet sich insofern von derjenigen, welche in den gesetzlichen Grundlagen der Informationssysteme, welche solche Daten bearbeiten, verwendet wird, als dort teilweise aufgeführt wird, von welchen Fingern die Abdrücke abzunehmen sind (siehe dazu Art. 2 Abs. 1 Bst. l Eurodac-VO; Art. 3 Abs. 1 Ziff. 16

genommen. Solche Templates werden auf der Grundlage von biometrischen Daten generiert und sind auf Merkmale beschränkt, welche für die Identifizierung und Verifizierung von Personen erforderlich sind.[931] Ausser dem ETIAS sehen alle von der Interoperabilität betroffenen Informationssysteme biometrische Abgleiche vor. Die zentrale Struktur des BMS ersetzt die Speicherung von biometrischen Templates in den Zentralsystemen der Systeme SIS, Eurodac, VIS, EES und ECRIS-TCN. Künftig werden die biometrischen Templates ausschliesslich und zentralisiert im BMS gespeichert. Des Weiteren umfasst der BMS eine sichere Kommunikationsinfrastruktur zwischen dem BMS, dem zentralen SIS sowie dem CIR.[932]

Im BMS werden nur die Templates von Fingerabdruckdaten und Gesichtsbildern, welche beim EES, VIS, SIS, ECRIS-TCN sowie bei Eurodac erhoben werden, gespeichert.[933] Diese Templates sind jeweils mit einem Verweis auf das System, aus welchem die biometrischen Original-Daten stammen, sowie einem Verweis auf die darin enthaltenen Datensätze versehen. Vorausgesetzt für die Eingabe in den BMS ist ein Mindeststandard der Datenqualität.[934] Die Speicherdauer der Templates im BMS richtet sich nach derjenigen im CIR resp. im SIS. Anschliessend erfolgt eine automatische Löschung.[935] Über die Datenverarbeitungsvorgänge haben eu-LISA sowie die beteiligten Schengen-Staaten Protokoll zu führen.[936]

EES-VO; Art. 3 Ziff. 12 ECRIS-TCN-VO. Beim SIS werden hingegen nicht spezifisch Fingerabdruckdaten definiert, sondern «*daktyloskopische Daten*». Siehe dazu Art. 3 Ziff. 14 SIS-Grenze-VO).

931 Gemäss Art. 4 Ziff. 12 EU-IOP-VO handelt es sich bei einem biometrischen Template um «*eine mathematische Repräsentation, die mittels Merkmalsauszug aus biometrischen Daten generiert wird, welche auf die für Identifizierungs- und Verifizierungszwecke erforderlichen Merkmale begrenzt sind*».

932 Siehe dazu Art. 12 Abs. 1-2 EU-IOP-VO.

933 Siehe dazu Art. 4 Ziff. 11-12 EU-IOP-VO. Diese Beschränkung der biometrischen Daten erscheint nachvollziehbar. So werden Fingerabdruckdaten sowie Gesichtsbilder bei verschiedenen Systemen gespeichert. Andere biometrische Daten, wie z.B. das DNA-Profil hingegen nur bei einzelnen (siehe dazu Art. 20 Abs. 3 Bst. x SIS-Polizei-VO). Ein systemübergreifender Abgleich macht nur Sinn, wenn mehrere Systeme abgefragt werden können. Werden bestimmte biometrische Daten nur in einem System erhoben, ist kein solcher Abgleich möglich, weshalb es auch nicht nötig ist, Templates von solchen biometrischen Daten im BMS zu speichern.

934 Siehe dazu Art. 13 Abs. 2-3 EU-IOP-VO.

935 Art. 15 EU-IOP-VO; BUNDESRAT, Botschaft IOP, 8006 f.

936 BUNDESRAT, Botschaft IOP, 8007. Siehe zu den Einzelheiten der Protokollierungspflicht Art. 16 EU-IOP-VO.

Da im EES mit Abstand am meisten biometrische Daten erhoben werden, wird der BMS im Zuge der Entstehung des EES geschaffen. Anschliessend werden die Daten aus den restlichen Systemen überführt.[937] Der BMS wird sowohl von eu-LISA entwickelt als auch später technisch verwaltet.[938]

5.3.3. Gemeinsamer Speicher für Identitätsdaten

Mit dem CIR wird ein Speicher geschaffen, welcher bestimmte Daten, die im Zusammenhang mit dem EES, VIS, Eurodac, ETIAS sowie ECRIS-TCN erhoben werden, speichert.[939] Die zentrale Struktur des CIR ersetzt dabei die Zentralsysteme der genannten Informationssysteme insoweit, als die im CIR gespeicherten Daten betroffen sind. Daten, welche gemäss den gesetzlichen Grundlagen der Informationssysteme erhoben werden müssen, aber nicht im CIR gespeichert werden, werden (weiterhin) im Zentralsystem des jeweiligen Informationssystems gespeichert. Davon abgesehen umfasst der CIR einen sicheren Kommunikationskanal mit allen zugriffsberechtigten Stellen und eine sichere Kommunikationsinfrastruktur zwischen dem CIR sowie den Systemen Eurodac, VIS, EES, ETIAS, ECRIS-TCN und den Komponenten ESP, BMS sowie MID.[940] Wie bereits erwähnt, kann das SIS nicht an den CIR angeschlossen werden, da dieses Informationssystem eine zu komplexe Struktur aufweist.[941]

Werden Daten von Personen im EES, VIS, ETIAS, ECRIS-TCN sowie in Eurodac erfasst, wird im CIR jeweils eine individuelle Datei angelegt. Diese umfasst sowohl die Identitätsdaten[942] (insbesondere Nachname(n), Vorname(n), Staatsangehörigkeit(en), Geburtsdatum, Geburtsort, Geschlecht) als auch – sofern vorhanden – Daten zu den Reisedokumenten und die Fingerabdruckdaten sowie Gesichtsbilder. Der jeweilige Datensatz wird dabei auch mit einem Verweis auf das Informationssystem versehen, aus welchem die Daten stammen.[943] Werden Daten in den genannten Informationssystemen neu aufgenommen, geändert resp. gelöscht, erfolgt automatisch eine entsprechende Änderung im CIR.[944] Die im CIR gespeicherten Daten dürfen so lange gespeichert werden, wie dies gemäss den gesetzlichen Grundlagen des jeweiligen Informationssys-

937 FRA, Opinion IOP, 21; Europäische Kommission, Vorschlag IOP-Grenze, 92 f.
938 Art. 12 Abs. 3 EU-IOP-VO.
939 Siehe dazu Art. 18 Abs. 1 EU-IOP-VO.
940 Art. 17 Abs. 1-2 EU-IOP-VO.
941 Siehe dazu Kapitel IV.4.
942 Vgl. zur Definition von Identitätsdaten Art. 4 Ziff. 8 EU-IOP-VO.
943 Siehe dazu Art. 17 Abs. 1 EU-IOP-VO; Art. 18 EU-IOP-VO.
944 Art. 19 Abs. 1 EU-IOP-VO.

tems, aus welchem die Daten stammen, vorgesehen ist. Danach werden sie automatisch gelöscht.[945]

Auf den CIR zugriffsberechtigt sind diejenigen Behörden, welche gemäss den einschlägigen Rechtsgrundlagen der involvierten Informationssysteme auf diese zugreifen dürfen.[946] Wie auch bei den Komponenten ESP und BMS haben eu-LISA, die Schengen-Staaten sowie Europol im CIR über die jeweiligen Datenverarbeitungsvorgänge resp. Zugriffe Protokoll zu führen.[947]

Der CIR wird von eu-LISA entwickelt. Diese Agentur ist nach der Inbetriebnahme auch für die technische Verwaltung dieser Komponente zuständig.[948]

Mit der Errichtung des CIR werden einerseits zwei neue Abfragen ermöglicht. Dabei handelt es sich um die Abfrage des CIR zwecks Identifizierung gemäss Art. 20 EU-IOP-VO sowie um die Abfrage des CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten gemäss Art. 21 EU-IOP-VO. Andererseits ermöglicht die Schaffung des CIR, dass die bei Eurodac, VIS, EES und ETIAS vorgesehene Abfrage zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten vereinheitlicht sowie erleichtert wird. Mit Art. 22 EU-IOP-VO wird eine generelle Bestimmung für solche Abfragen geschaffen. Diese Abfragen waren bis anhin ausschliesslich in den gesetzlichen Grundlagen der betroffenen Informationssysteme geregelt. Die entsprechenden Verfahren weisen zwar gewisse Ähnlichkeiten auf, sind jedoch nicht identisch.[949]

Diese drei Bestimmungen, also Art. 20-22 EU-IOP-VO, stellen gleichzeitig auch die Zielsetzung des CIR dar. So soll mit dem CIR eine korrekte Identifizierung von im EES, VIS, ETIAS, Eurodac und ECRIS-TCN erfassten Personen gemäss Art. 20 EU-IOP-VO erleichtert und unterstützt werden. Des Weiteren unterstützt der CIR das Funktionieren des MID gemäss Art. 21 EU-IOP-VO. Ausserdem erleichtert der CIR den Zugang der nationalen Strafverfolgungsbehörden sowie Europol zu den im EES, VIS, ETIAS und Eurodac gespeicherten Daten und vereinheitlicht dieses Verfahren.[950]

945 Art. 23 Abs. 1 EU-IOP-VO.
946 BUNDESRAT, Botschaft IOP, 8007.
947 Siehe dazu Art. 24 EU-IOP-VO.
948 Art. 17 Abs. 3 EU-IOP-VO.
949 Siehe zur gesetzlichen Regelung der Systeme, welche eine solche Abfrage vorsehen Kapitel III.5.5.2; III.6.5.2; III.7.5.2 und III.8.5.3.
950 Art. 17 Abs. 1 EU-IOP-VO.

5.3.3.1 *Zugang zum CIR zwecks Identifizierungen*

Art. 20 EU-IOP-VO räumt den Polizeibehörden auf EU-Ebene zwei Möglichkeiten ein, auf den CIR zuzugreifen. Sofern die einzelnen Schengen-Staaten von diesen Abfragemöglichkeiten profitieren wollen, müssen sie ihren nationalen Polizeibehörden in der nationalen Gesetzgebung die entsprechenden Befugnisse übertragen. Ebenfalls müssen im nationalen Recht jeweils die Verfahren, Bedingungen sowie die Kriterien von solchen Abfragemöglichkeiten festgelegt werden.[951]

Die erste vorgesehene Zugriffsmöglichkeit der Polizeibehörden ist der Zugriff auf den CIR via ESP zwecks Identifizierung von Personen bei Polizeikontrollen. Dieser Zugriff ist nur in bestimmten Situationen erlaubt. So bspw. wenn Zweifel bezüglich der von einer Person gemachten Identitätsangaben bestehen, wenn eine Person die Zusammenarbeit verweigert oder dazu nicht in der Lage ist oder wenn die Polizeibehörde eine Person mangels eines Reisedokuments resp. eines anderen glaubwürdigen Dokuments als Nachweis der Identität nicht identifizieren kann. Eine Abfrage ist anhand der vor Ort abgenommenen biometrischen Daten vorzunehmen und darf nur erfolgen, sofern das Verfahren im Beisein der betroffenen Person eingeleitet wurde. Können die erhobenen biometrischen Daten nicht für die Abfrage verwendet werden resp. ist die Abfrage mit diesen Daten nicht erfolgreich, kann eine Abfrage auch mit den Identitätsdaten der betroffenen Person zusammen mit den Daten eines Reisedokuments oder anhand der von der betroffenen Person angegebenen Identitätsdaten erfolgen. Liegt ein Treffer im CIR vor, ist die Polizeibehörde berechtigt, die gespeicherten Daten zu konsultieren. Die Angabe, aus welchem Informationssystem die Daten stammen, wird der abfragenden Behörde jedoch verwehrt.[952] Die Schengen-Staaten, welche diese Abfrage nutzen möchten, haben – abgesehen von den Verfahren, Bedingungen und Kriterien – im nationalen Recht die zugriffsberechtigten Behörden zu bezeichnen sowie die genaueren Zwecke der Abfrage festzulegen. Das EU-Recht sieht lediglich vor, dass die Abfragen im Rahmen der Verhinderung und Bekämpfung illegaler Einwanderung resp. der Gewährleistung der Sicherheit zu erfolgen haben.[953]

Als zweite Zugriffsmöglichkeit sieht das EU-Recht vor, dass Polizeibehörden im Falle einer Naturkatastrophe, eines Unfalls oder eines Terroranschlags ausschliesslich für die Identifizierung von unbekannten Personen, welche sich nicht ausweisen können, sowie nicht-identifizierter menschlicher Überreste

951 Siehe dazu Art. 20 Abs. 5-6 EU-IOP-VO.
952 Art. 20 Abs. 1-3 EU-IOP-VO.
953 Siehe dazu Art. 20 Abs. 5 EU-IOP-VO.

eine Abfrage im CIR vornehmen dürfen. Diese Abfrage erfolgt anhand der biometrischen Daten der betroffenen Person.[954]

5.3.3.2 *Zugang zum CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten*

Art. 21 EU-IOP-VO sieht die Abfrage des CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten vor. Um diese Abfragemöglichkeit besser zu erfassen, sei bereits an dieser Stelle erwähnt, dass der MID zur Aufdeckung von Mehrfachidentitäten in bestimmten Konstellationen verschiedenfarbige Verknüpfungen zwischen Daten erstellt, welche aus verschiedenen Informationssystemen stammen.[955]

Die in Art. 21 EU-IOP-VO vorgesehene Abfrage sieht vor, dass wenn bei einer Abfrage des CIR eine gelbe Verknüpfung erstellt wird, die für die manuelle Verifizierung zuständige Behörde – ausschliesslich zu Verifizierungszwecken – auch auf die anderen von der Verknüpfung betroffenen Daten zugreifen darf. Wird hingegen bei einer Abfrage des CIR eine rote Verknüpfung angezeigt, sind bestimmte Behörden – ausschliesslich zur Bekämpfung von Identitätsbetrug – berechtigt, auch auf die durch die Verknüpfung bezeichneten Daten zuzugreifen.[956] Insofern wird das Zugriffsrecht der entsprechenden Behörden in diesen Konstellationen erweitert.

5.3.3.3 *Abfrage des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten*

Des Weiteren wurde mit Art. 22 EU-IOP-VO eine gemeinsame Bestimmung für die Abfrage des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer[957] oder sonstiger schwerer Straftaten[958] geschaffen. Die-

954 Art. 20 Abs. 4 EU-IOP-VO.

955 Siehe dazu Kapitel IV.5.3.4. Vgl. dazu auch Art. 25 ff. EU-IOP-VO.

956 Siehe dazu Art. 21 EU-IOP-VO.

957 Siehe zur Definition Art. 4 Ziff. 21 EU-IOP-VO. Dieser Begriff wird gleich wie in den gesetzlichen Grundlagen der Systeme Eurodac, VIS, EES und ETIAS definiert (wobei die Bestimmungen von Eurodac und VIS auf einen Rechtsakt verweisen, welcher mittlerweile ersetzt wurde). Siehe dazu Art. 2 Abs. 1 Bst. j Eurodac-VO; Art. 2 Abs. 1 Bst. c VIS-Beschluss; Art. 3 Abs. 1 Ziff. 24 EES-VO sowie Art. 3 Abs. 1 Ziff. 15 ETIAS-VO. In der Schweiz sind die terroristischen Straftaten in Anhang 1a N-SIS-Verordnung aufgeführt.

958 Siehe zur Definition Art. 4 Ziff. 22 EU-IOP-VO. Diese deckt sich mit derjenigen in den gesetzlichen Grundlagen der Systeme Eurodac, EES und ETIAS. Siehe dazu Art. 2 Abs. 1 Bst. k Eurodac-VO; Art. 3 Abs. 1 Ziff. 25 EES-VO sowie Art. 3 Abs. 1 Ziff. 16 ETIAS-VO. Die Defi-

ser Zugang von den nationalen Strafverfolgungsbehörden sowie von Europol auf Daten aus dem EES, VIS, ETIAS und Eurodac ist grundsätzlich nicht neu.[959] Im Rahmen der EU-IOP-VO wird jedoch beabsichtigt, diesen Zugang zu erleichtern und einheitlich zu regeln.[960]

Neu sieht Art. 22 EU-IOP-VO ein zweistufiges Verfahren vor, wobei dieser Artikel die erste Stufe regelt. Die zweite Stufe ist den bestehenden Regelungen des entsprechenden Informationssystems zu entnehmen, aus welchem die Daten stammen, die zum Treffer geführt haben.[961]

Gemäss Art. 22 EU-IOP-VO wird auf erster Stufe für die Vornahme einer Abfrage vorausgesetzt, dass im konkreten Einzelfall vernünftige Gründe ersichtlich sind, eine solche Abfrage könne zur Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten beitragen (insbesondere, wenn der Verdacht besteht, dass der Verdächtige, der Täter oder das Oper einer terroristischen Straftat resp. einer sonstigen schweren Straftat in einem der Systeme erfasst ist). Liegen diese Voraussetzungen vor, dürfen die von den Schengen-Staaten benannten Behörden resp. Europol den CIR abfragen.[962]

Wird in einer solchen Abfrage festgestellt, dass zutreffende Daten im CIR vorhanden sind, wird der abfragenden Behörde resp. Europol mitgeteilt, in welchem der Informationssysteme übereinstimmende Daten vorhanden sind. Diese Information darf einzig für die Übermittlung eines Antrags auf uneingeschränkten Zugang zu diesen Daten gemäss den Bestimmungen des einschlägigen Rechtsinstruments des betroffenen Informationssystems verwendet werden. Wird kein

---

nition beim VIS weicht etwas davon ab. Siehe dazu Art. 2 Abs. 1 Bst. d VIS-Beschluss. Ob die Abweichung in der Formulierung tatsächlich dazu führt, dass beim VIS nicht dieselben Straftaten erfasst werden wie bei den anderen drei genannten Systemen, wird vorliegend nicht näher untersucht. Für die Abfrage zu Zwecken der Verhinderung, Aufdeckung und Untersuchung terroristischer sowie sonstiger schwerer Straftaten könnte es jedoch problematisch sein, wenn das VIS nicht dieselben Straftaten wie Art. 22 EU-IOP-VO vorsieht. Schliesslich sollen zukünftig beide Bestimmungen betreffend die Zugangsbedingungen einschlägig sein.

959 Siehe dazu Kapitel III.5.5.2; III.5.5.3; III.6.5.2; III.6.5.3; III.7.5.2; III.7.5.3; III.8.5.3 und III.8.5.4. In Art. 22 Abs. 1 EU-IOP-VO wird der Begriff der «*benannten Behörden*» verwendet. Diese werden in der vorliegenden Untersuchung als nationale Strafverfolgungsbehörden bezeichnet.

960 Siehe dazu Art. 17 Abs. 1 EU-IOP-VO.

961 Siehe zu den Einzelheiten Art. 22 EU-IOP-VO.

962 Art. 22 Abs. 1 EU-IOP-VO. Die Definitionen der Begriffe «*terroristische Straftat*» und «*schwere Straftat*» verweisen auf andere EU-Rechtsakte. Siehe dazu Art. 4 Ziff. 21-22 EU-IOP-VO.

solcher Antrag gestellt, hat die nationale Strafverfolgungsbehörde resp. Europol dies zu begründen. Der vollständige Zugang zu den Daten wird – auf der zweiten Stufe – gemäss den in den Rechtsgrundlagen der einzelnen Informationssysteme vorgesehenen Bedingungen und Verfahren gewährt.[963]

Die durch Art. 22 EU-IOP-VO vorgenommene Änderung des Zugangsverfahren der nationalen Strafverfolgungsbehörden resp. Europol auf das EES, VIS, ETIAS sowie Eurodac ermöglicht mit einem einzigen Suchvorgang – und ohne vorherige Kontrolle durch eine unabhängige Stelle – im CIR in Erfahrung zu bringen, ob und falls ja in welchem System Daten von der betroffenen Person vorhanden sind. Dies ist insbesondere in Fällen hilfreich, in welchen unbekannte Verdächtige, Täter oder mutmassliche Opfer einer terroristischen oder sonstigen schweren Straftat identifiziert werden müssen.[964]

5.3.4. Detektor für Mehrfachidentitäten

Der MID musste geschaffen werden, damit auch SIS-Daten einer Prüfung auf Mehrfachidentitäten unterzogen werden können.[965] Die Komponente wird von eu-LISA entwickelt und anschliessend auch technisch verwaltet.[966]

Mit dem MID können Personen erkannt werden, welche mehrere resp. falsche Identitäten verwenden. Dadurch werden zwei Ziele verfolgt, nämlich einerseits die Vereinfachung von Identitätsprüfungen und andererseits die Bekämpfung von Identitätsbetrug. Die Prüfung auf Mehrfachidentitäten erfolgt, damit Daten der verschiedenen Informationssysteme abgeglichen werden können. Eine entsprechende Prüfung wird bei jeder Erfassung resp. Aktualisierung von Personendaten, Daten zu Reisedokumenten oder den biometrischen Daten der Systeme VIS, SIS, ETIAS, ECRIS-TCN, Eurodac und EES vorgenommen. Ein automatisierter Abgleich der neuen resp. aktualisierten Daten erfolgt mit denjenigen im CIR und im SIS, wobei der BMS bezüglich der biometrischen Daten und das ESP hinsichtlich der Identitätsdaten sowie der Daten zu den Reisedokumenten zur Anwendung gelangen.[967] Der MID ist deshalb über eine

963 Art. 22 Abs. 2-3 EU-IOP-VO.

964 Vgl. dazu Europäische Kommission, Vorschlag IOP-Grenze, 11.

965 Vgl. dazu Kapitel IV.4.

966 Art. 25 Abs. 3 EU-IOP-VO. Vor der Inbetriebnahme des MID sollen anhand von biometrischen Daten durch die ETIAS-Zentralstelle alle bereits im EES, VIS, Eurodac und im SIS vorhandenen Daten einer Prüfung auf Mehrfachidentitäten unterzogen werden. Erst wenn alle gelben Verknüpfungen geprüft wurden, soll der Zeitpunkt der effektiven Inbetriebnahme des MID festgelegt werden. Siehe dazu Art. 69 IOP-Grenze-VO; Art. 65 IOP-Polizei-VO; Bundesrat, Botschaft IOP, 8015.

967 Art. 25 Abs. 1 EU-IOP-VO; Art. 27 EU-IOP-VO; Bundesrat, Botschaft IOP, 8003, 8010.

sichere Kommunikationsinfrastruktur mit dem SIS und den zentralen Infrastrukturen des ESP sowie des CIR verbunden.[968]

Kann bei der Prüfung auf Mehrfachidentitäten keine Übereinstimmung mit in anderen Systemen gespeicherten Daten festgestellt werden, werden die Daten gemäss den gesetzlichen Bestimmungen erfasst. Übereinstimmungen von den für die Abfrage verwendeten Daten mit bereits vorhandenen Daten haben hingegen zur Folge, dass eine Verknüpfung zwischen allen betroffenen Daten erstellt wird. Bereits bestehende Verknüpfungen werden entsprechend erweitert.[969]

Im MID gespeichert wird eine Identitätsbestätigungsdatei, welche u.a. die Art der Verknüpfung und die Angabe desjenigen Systems enthält, in welchem die verknüpften Daten gespeichert sind. Zudem enthält die Identitätsbestätigungsdatei eine einmalige Kennnummer, mit welcher die verknüpften Daten abgerufen werden können, die Angabe derjenigen Behörde, welche für die manuelle Verifizierung zuständig ist, sowie das Datum der Erstellung resp. jeder Aktualisierung einer Verknüpfung.[970] Diese Identitätsbestätigungsdateien werden so lange gespeichert, wie die verknüpften Daten in zwei oder mehr Systemen gespeichert sind, wobei eine automatische Löschung vorgesehen ist.[971]

Über die Datenverarbeitungsvorgänge sowie die Abfragen im MID haben sowohl die Schengen-Staaten als auch eu-LISA Protokoll zu führen.[972]

Die Verknüpfungen werden anhand von verschiedenen Farben (weiss, gelb, rot und grün) gekennzeichnet.[973] Die Bedeutung dieser Kennzeichnungen wird im Folgenden näher ausgeführt.

5.3.4.1 *Weisse und gelbe Verknüpfungen*

Werden bei einer Prüfung auf Mehrfachidentitäten eine oder mehrere Übereinstimmungen entdeckt, wird eine Verknüpfung erstellt. Die Verknüpfung ist weiss, sofern die Identitätsdaten der verknüpften Dateien gleich oder ähnlich sind. Eine gelbe Verknüpfung wird hingegen erstellt, wenn die Identitätsdaten der verknüpften Dateien nicht als ähnlich angesehen werden können.[974]

968 Art. 25 Abs. 2 EU-IOP-VO.
969 BUNDESRAT, Botschaft IOP, 8010 f.
970 Siehe dazu Art. 34 EU-IOP-VO.
971 Art. 35 EU-IOP-VO.
972 BUNDESRAT, Botschaft IOP, 8015; Art. 36 EU-IOP-VO.
973 Vgl. dazu Art. 30-33 EU-IOP-VO.
974 Art. 28 Abs. 3-4 EU-IOP-VO.

Gelbe Verknüpfungen kennzeichnen also, dass nicht alle verknüpften Daten übereinstimmen. Sie werden bspw. erstellt, wenn die biometrischen Daten zwar identisch sind, die Identitätsdaten hingegen nicht. Die Klassifizierung als gelbe Verknüpfung hat zur Folge, dass eine manuelle Verifizierung vorgenommen werden muss.[975]

Für die manuelle Verifizierung sind grundsätzlich diejenigen Stellen zuständig, welche die Daten im EES, VIS, ETIAS, ECRIS-TCN, SIS oder in Eurodac erfasst resp. aktualisiert haben, welche anschliessend zu einer Übereinstimmung geführt haben. Davon ausgenommen sind Verknüpfungen mit bestimmten SIS-Ausschreibungen. In diesen Fällen ist das SIRENE-Büro desjenigen Schengen-Staates für die manuelle Verifizierung zuständig, welcher die Ausschreibung vorgenommen hat.[976]

Die zuständige Behörde erhält grundsätzlich Zugriff auf die in der Identitätsbestätigungsdatei gespeicherten Daten sowie auf die im CIR resp. im SIS verknüpften Identitätsdaten, um die manuelle Verifizierung vorzunehmen. Diese hat unverzüglich zu erfolgen. Abhängig vom Resultat der manuellen Verifizierungen wird eine rote, grüne oder weisse Verknüpfung erstellt. Sind mehrere Verknüpfungen erstellt worden, hat jeweils eine separate Prüfung zu erfolgen.[977]

5.3.4.2 *Grüne Verknüpfungen*

Grüne Verknüpfungen können erst nach einer manuellen Prüfung erstellt werden und bedeuten, dass die verknüpften Identitätsdaten nicht derselben Person zugehörig sind. So können bspw. zwei Personen mit demselben Namen sowie Geburtsdatum zwar identische Identitätsdaten, jedoch unterschiedliche biometrische Daten aufweisen.[978]

Eine grüne Verknüpfung wird also erstellt, wenn im Rahmen der manuellen Verifizierung bestätigt werden kann, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen.[979]

---

975 Siehe dazu Art. 30 EU-IOP-VO. Siehe zur manuellen Verifizierung Art. 29 EU-IOP-VO; BUNDESRAT, Botschaft IOP, 8012.

976 Art. 29 Abs. 1-2 EU-IOP-VO; BUNDESRAT, Botschaft IOP, 8010 f.

977 Art. 29 Abs. 3 und Abs. 5 EU-IOP-VO. Siehe Art. 29 Abs. 4 EU-IOP-VO zur Regelung wenn beim Anlegen resp. Aktualisieren eines persönlichen Dossiers im EES eine gelbe Verknüpfung erstellt wird.

978 BUNDESRAT, Botschaft IOP, 8012.

979 Siehe dazu Art. 31 EU-IOP-VO.

Ein Zugriff auf eine grüne Verknüpfung ist für Behörden der Schengen-Staaten sowie Stellen der Union möglich, sofern sie hinsichtlich beider Informationssysteme, zwischen denen die Verknüpfung erstellt worden ist, zugriffsberechtigt sind.[980]

5.3.4.3 *Rote Verknüpfungen*

Eine rote Verknüpfung kann ebenfalls erst nach der Vornahme einer manuellen Verifizierung erfolgen. Die rote Kennzeichnung bedeutet, dass eine unrechtmässige Mehrfachidentität resp. ein Identitätsbetrug vorliegt. So wird bspw. eine rote Verknüpfung erstellt, wenn die biometrischen Daten zwar identisch sind, jedoch ähnliche oder unterschiedliche Identitätsdaten vorliegen und die manuelle Verifizierung ergeben hat, dass sich die verknüpften Daten ungerechtfertigt auf dieselbe Person beziehen. Die zuständige Behörde, welche eine rote Verknüpfung erstellt, kann die betroffene Person mittels Standardformular über das Vorliegen von illegalen Mehrfachidentitäten informieren. Der MID informiert im Zuge der Erstellung von roten Verknüpfungen automatisch diejenigen Behörden, welche für die verknüpften Daten zuständig sind. Allfällig zu ergreifende Massnahmen können dem EU-Recht oder dem nationalen Recht entnommen werden. Eine rote Verknüpfung hat für sich allein genommen für die betroffene Person keine (negativen) Folgen.[981]

Die nationalen Behörden sowie die Stellen der Union können auf von einer roten Verknüpfung betroffene Daten zugreifen, sofern sie mindestens betreffend eines der betroffenen Informationssysteme zugriffsberechtigt sind.[982]

5.3.4.4 *Weisse Verknüpfungen*

Eine weisse Verknüpfung kann nicht nur – wie vorne bereits erwähnt – bei der automatisierten Prüfung durch den MID erfolgen, sondern auch nachdem die manuelle Verifizierung durchgeführt wurde. So wird bspw. eine weisse Verknüpfung erstellt, wenn identische biometrische Daten, aber bloss ähnliche resp. unterschiedliche Identitätsdaten vorliegen, welche sich in gerechtfertigter Weise auf ein und dieselbe Person beziehen. Bei einer weissen Verknüpfung wird u.a. die Mobilität von Personen vereinfacht, welche rechtmässig über mehrere gültige Reisedokumente verfügen. Wenn die weisse Verknüpfung im Zuge der manuellen Verifizierung vorgenommen wurde, kann die zuständige Behörde die be-

980 Art. 26 Abs. 4 EU-IOP-VO.
981 Art. 32 EU-IOP-VO; BUNDESRAT, Botschaft IOP, 8012 f.
982 Art. 26 Abs. 2 EU-IOP-VO.

troffene Person dahingehend informieren, dass ähnliche resp. unterschiedliche Identitätsdaten vorhanden sind. Aus Sicherheitsgründen kann von einer solchen Mitteilung mittels Standardformular abgesehen werden.[983]

Behörden, welche auf eine weisse Verknüpfung zugreifen wollen, müssen auf alle Informationssysteme Zugriff haben, zwischen deren Daten eine Verknüpfung besteht.[984]

5.4. Ausgewählte Sicherheitsmassnahmen

5.4.1. Datensicherheit

5.4.1.1 *Veränderung der Datenverwaltungsarchitektur*

Bevor auf die Bestimmungen zur Datensicherheit eingegangen wird, wird untersucht, inwiefern sich die Interoperabilität auf die bestehende Architektur der von der Verknüpfung betroffenen Systeme auswirkt.

Die Interoperabilität bewirkt, dass das einst geschlossene Umfeld der einzelnen Systeme zu einer gemeinsamen Umgebung mit verschiedenen Verbindungen zwischen den Systemen wird. Damit wird die Architektur der Systeme grundlegend verändert. Dies birgt neue Sicherheitsrisiken. So ist es bspw. möglich, dass ein Angreifer durch einen (unberechtigten) Zugang zum ESP auch auf die an diese Komponente angeschlossenen Systemen zugreifen kann.[985]

Davon abgesehen werden durch die Interoperabilität drei neue Datenspeicher geschaffen: der CIR, der BMS sowie der MID. Der MID enthält verschiedene Angaben im Zusammenhang mit einer Verknüpfung. Im CIR und im BMS hingegen werden bestimmte Daten gespeichert, welche im Rahmen der einzelnen Systeme bearbeitet werden. Daten aus den verschiedenen Systemen werden also neu zentral in einem Datenspeicher gespeichert. Damit werden sehr grosse Datenbanken geschaffen. Insbesondere im CIR werden sowohl alphanumerische als auch biometrische Daten von fast allen Drittstaatsangehörigen erfasst, welche die EU-Grenzen bereits überschritten haben, oder dies beabsichtigen. Dies betrifft Millionen von Personen. Hinzu kommt, dass insbesondere biometrische Daten sehr sensibel sind, da sie untrennbar und dauerhaft

983 Art. 33 EU-IOP-VO; BUNDESRAT, Botschaft IOP, 8013 f.
984 Art. 26 Abs. 3 EU-IOP-VO.
985 Siehe dazu EDSB, Reflexionspapier IOP, N 35 f.

mit einer Person verknüpft sind. Eine unrechtmässige Verwendung der Daten im CIR könnte aufgrund der Vielzahl sowie der Art der gespeicherten Daten grundsätzlich vielen Personen einen (schweren) Schaden verursachen.[986]

Bereits während des Entstehungsprozesses der Interoperabilität haben verschiedene Akteure u.a. darauf hingewiesen, dass Hacker an solch gigantischen und zentralen Systemen ein grosses Interesse hätten und die Gefahr des Missbrauchs resp. der über die vorgesehene Nutzung hinausgehende Verwendung bestehe.[987] Insbesondere für kriminelle Organisationen oder Hacker, möglicherweise mit Verbindungen zu Drittstaaten, sind interoperable Datenbanken besonders attraktive Ziele.[988]

Durch die Interoperabilität wird die Datenverwaltungsstruktur also stark verändert. Die Vernetzung der Systeme und insbesondere auch die Schaffung von drei grossen, zentralen Datenspeichern führt dazu, dass das Interesse an unberechtigten Zugriffen auf eben diese steigt. Das Risiko für Datenmissbrauch nimmt durch die Veränderung der Struktur der Informationssysteme grundsätzlich zu.

5.4.1.2 *Bestimmungen zur Datensicherheit*

In den EU-IOP-VO finden sich verschiedene Bestimmungen zur Datensicherheit. So sind eu-LISA, die ETIAS-Zentralstelle, Europol sowie die Schengen/Dublin-Staaten für die Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten zuständig, wobei diese Akteure in Erfüllung ihrer sicherheitsbezogenen Aufgaben zusammenarbeiten. Betreffend die Sicherheit der Interoperabilitätskomponenten sowie der damit verbundenen Kommunikationsinfrastruktur ist eu-LISA grundsätzlich in der Hauptverantwortung und muss die erforderlichen Schutzmassnahmen treffen. Solche sind ebenfalls von den Schengen/Dublin-Staaten, Europol und der ETIAS-Zentralstelle zu ergreifen, sofern das Recht auf Zugang zu Interoperabilitätskomponenten vorhanden ist.[989]

---

986 Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 27 ff.; BUNDESRAT, Botschaft IOP, 7995 ff.; WP29, Opinion proposals IOP, 19 f. Siehe zum Thema Datensicherheit auch PRIVACY INTERNATIONAL, Ziff. 5.

987 Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 28; WP29, Opinion proposals IOP, 19 f. Vgl. dazu auch BUNDESRAT, Botschaft IOP, 7996. Es sind bereits Fälle von unrechtmässigen Zugriffen auf die Systeme oder von der unrechtmässigen Verwendung von Fingerabdruckdaten bekannt. Siehe dazu FRA, biometrics, 61.

988 FRA, biometrics, 63. Dabei stellen insbesondere Datenbanken mit biometrischen Daten ein attraktives Ziel für Hacker dar. Siehe dazu BOSSUNG, 24.

989 Siehe zu den Einzelheiten Art. 42 EU-IOP-VO.

Bei Ereignissen, welche sich auf die Sicherheit der Interoperabilitätskomponenten auswirken (können) und die darin gespeicherten Daten beschädigen oder deren Verlust herbeiführen können, ist eine Meldepflicht vorgesehen. Diese soll sicherstellen, dass bei solchen Ereignissen, sog. Sicherheitsvorfällen, bestimmte Stellen informiert werden. Dabei handelt es sich primär um die Kommission, eu-LISA, den EDSB sowie teilweise noch weitere Akteure.[990]

Davon abgesehen hat eu-LISA nach der Inbetriebnahme der Interoperabilitätskomponenten alle vier Jahre einen Bericht über die technische Funktionsweise der Komponenten einschliesslich ihrer Sicherheit dem Europäischen Parlament, der Kommission sowie dem Rat vorzulegen. Die Kommission hat jeweils innerhalb eines Jahres nach jedem Bericht von eu-LISA eine Gesamtbewertung der Komponenten vorzunehmen. Dieser Bewertungsbericht, welcher u.a. eine Bewertung der Sicherheit der Interoperabilitätskomponenten sowie der Nutzung des CIR zu Zwecken der Identifikation resp. der Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten enthält, wird dem EP, dem Rat, dem EDSB sowie der FRA übermittelt.[991]

In den EU-IOP-VO werden also verschiedene Verantwortlichkeiten im Bereich der Datensicherheit geregelt. Zudem wird festgelegt, wer bei einem Sicherheitsvorfall wie und von wem zu informieren ist. Hinzu kommt eine Pflicht zur Berichterstattung, welche u.a. die Datensicherheit umfasst.

5.4.2. Datenqualität

5.4.2.1 *Allgemeine Problematik*

In Informationssystemen gespeicherte Daten werden grundsätzlich als korrekt und zuverlässig angesehen.[992] Die FRA hat jedoch festgestellt, dass die bereits in Betrieb genommenen Systeme eine grosse Anzahl unrichtiger alphanumerischer Daten enthalten.[993]

---

990 Siehe zu den Einzelheiten Art. 43 EU-IOP-VO. Die genauen Modalitäten der Zusammenarbeit zwischen den verschiedenen Akteuren werden in Durchführungsrechtsakten festgelegt.

991 Art. 78 Abs. 3-4 EU-IOP-VO.

992 FRA, biometrics, 82.

993 FRA, Opinion IOP, 49. Beim VIS wurden sogar zeitweise die Anforderungen an die Qualität der Daten suspendiert, um das Registrierungsverfahren zu beschleunigen. Da die VIS-Daten zwischen 5-10 Jahre gespeichert werden, hat diese Suspendierung noch lange Folgen. Siehe dazu VAVOULA, Deathblow, 152.

Werden Daten durch Menschen erhoben, besteht stets das Risiko von Fehlern. Dies wirkt sich negativ auf die Datenqualität aus.[994] Es gibt verschiedene Gründe, welche die Zuverlässigkeit von alphanumerischen Daten beeinflussen können. Dazu zählen u.a. Rechtschreibfehler, technische Mängel, falsche Transkription in das lateinische Alphabet, Eingabefehler der Daten aufgrund von sprachlichen Schwierigkeiten, Fehler aufgrund kultureller Bräuche bezüglich der Verwendung von Vor- und Nachnamen, Mangel an Kompetenzen und Ausbildung des Personals, erhöhte Arbeitsbelastung und Beanspruchung der MitarbeiterInnen bei der Erfassung und Bearbeitung von Daten sowie nicht ausreichende sprachliche Kenntnisse der BeamtInnen. Des Weiteren wird teilweise das falsche Geschlecht oder die falsche Staatsangehörigkeit registriert oder es werden Geburtsdaten erfasst, obwohl das genaue Datum unbekannt ist. Hinzu kommt, dass Personen, deren Daten erfasst werden sollen, zum Teil kein Ausweisdokument vorweisen können resp. falsche oder unvollständige Daten angeben.[995]

Gemäss der FRA ist das Risiko von Fehlern geringer, wenn die betroffene Person aktiv bei der Erhebung der Daten miteinbezogen wird. Zur Verringerung von Fehlern hilft zudem die Möglichkeit, dass sich die Person zu Widersprüchen äussern kann. Doppelte Kontrollen, Schulungen und der Einsatz elektronischer Lesegeräte zur Minimierung manueller Eingaben sowie ggf. eine automatische Verifizierung mit anderen Dateneingaben können ebenfalls helfen, das Fehlerrisiko gering zu halten.[996]

Biometrische Daten geniessen grundsätzlich eine hohe Glaubwürdigkeit.[997] Deren Zuverlässigkeit hängt jedoch ebenfalls von diversen Faktoren ab. So gibt es z.B. für die Abnahme des Fingerabdrucks verschiedene technische Methoden. Meist werden optische Lesegeräte eingesetzt, welche mittels Beleuchtung den Fingerabdruck erfassen und anschliessend abbilden können.[998] Diese können jedoch leicht getäuscht werden. Weitere Faktoren wie die Temperatur,

994 Siehe dazu HLEG, final report, 10.

995 FRA, biometrics, 84; FRA, borders and security, 30. Insbesondere die Registrierungen bei Eurodac werden häufig unter Zeitdruck vorgenommen. Zudem geben die asylsuchenden Personen oftmals nicht ihre korrekten Daten an, da sie kein Vertrauen in die Behörden haben. Es ist deshalb eine grosse Anzahl von falschen Daten in Eurodac gespeichert. Siehe dazu FRA, Opinion Eurodac 2016, 9.

996 FRA, borders and security, 30.

997 FRA, Opinion IOP, 49.

998 Fingerabdruckdaten können auch mit Hilfe von Tinte und Papier abgenommen werden. Dabei ist es zwar schwierig dieselbe Qualität zu erreichen wie mit dem Lesegerät, dennoch gibt es praktische Vorteile, z.B. keine Verwechslung bei mehreren Versuchen. FRA, biometrics, 90.

Feuchtigkeit, das Vorhandensein von Schmutz sowie auch Verletzungen der Fingerkuppen können die Qualität der Fingerabdruckdaten massgeblich beeinflussen. Gerade im Asylbereich haben phasenweise viele asylsuchende Personen vorsätzlich die Fingerbeeren verletzt, um nicht identifiziert werden zu können. Im Laufe der Zeit können sich die Fingerbeeren zudem verändern. Eine solche Veränderung wirkt sich insbesondere bei Kindern und älteren Personen aus.[999] Für einen zuverlässigen Vergleich von Fingerabdruckdaten sollten deshalb Daten verwendet werden, zwischen deren Abnahme nicht allzu viel Zeit verstrichen ist. Je mehr Zeit zwischen den für einen Vergleich verwendeten Fingerabdruckdaten liegt, desto unzuverlässiger ist das Ergebnis.[1000] Auch die Qualität von Gesichtsbildern hängt von verschiedenen Faktoren ab. So u.a. vom Hintergrund, der Beleuchtung sowie der Lichtreflexion, der Position der Person zur Kamera, der vergangenen Zeit seit der Aufnahme des Bildes, dem Alter, dem Geschlecht sowie dem Zustand der Haut der erfassten Person.[1001]

Abgesehen von diesen zahlreichen Faktoren, welche sich bei der Erhebung von biometrischen Daten negativ auf die Datenqualität auswirken können, ist auch zu berücksichtigen, dass für einen biometrischen Vergleich ein Algorithmus eingesetzt wird. Dieser berechnet Wahrscheinlichkeiten und legt innerhalb festzulegender Grenzwerte fest, ob ein Treffer vorliegt oder nicht. Obwohl dieser Algorithmus eine sehr hohe Genauigkeit der Vergleiche gewährleistet, bleibt ein minimales Restrisiko von falschen Treffern oder falschen Nicht-Treffern bestehen.[1002] Die Festlegung der Grenzwerte der Wahrscheinlichkeiten bedarf einer sorgfältigen Abwägung. Werden die Grenzwerte verschoben, nehmen zwar die falschen Treffer ab, die falschen Nicht-Treffer nehmen jedoch zu resp. umgekehrt. Auch wenn Probleme mit der Qualität von biometrischen Daten nur sehr selten auftreten, so ist aufgrund der immensen Zahl von erfassten Personen in den Systemen dennoch eine grosse Anzahl von Personen betroffen.[1003]

---

999 STADELMANN, 8 f.; BLONSKI, 21 ff.; FRA, biometrics, 92.

1000 Die meisten von der Interoperabilität umfassten Systeme sehen eine Speicherfrist von fünf Jahren vor. Diese Begrenzung hilft, falsche biometrische Treffer zu vermeiden. Bei Eurodac können bestimmte Daten bis zu zehn Jahren gespeichert werden. Siehe zum Ganzen FRA, Opinion IOP, 14; FRA, borders and security, 36.

1001 FRA, biometrics, 90.

1002 Bei Ersterem findet fälschlicherweise eine Zuordnung statt. Bei Letzterem hingegen wird ein Treffer nicht erkannt. Siehe dazu FRA, Gesichtserkennungstechnologien, 9.

1003 Siehe zum Ganzen FRA, biometrics, 88; FRA, Gesichtserkennungstechnologien, 9 f. Siehe dazu auch STADELMANN, 1 ff.; BLONSKI, 11 ff. m.w.H.

Zusammenfassend ist also festzustellen, dass bei der Erhebung von Daten verschiedene Fehlerquellen vorhanden sind. Zudem birgt auch der bei den biometrischen Daten verwendete Algorithmus ein gewisses Risiko, dass ein Treffer nicht korrekt ist resp. nicht erkannt wird. Davon abgesehen besteht eine weitere Fehlerquelle darin, dass die alphanumerischen Daten den falschen biometrischen Daten zugeordnet werden.[1004]

5.4.2.2 *Art und Weise der Erhebung der Daten*

Die Daten, welche im Rahmen der Interoperabilität bearbeitet werden, werden mehrheitlich gemäss der gesetzlichen Grundlage des einschlägigen Informationssystems erhoben. Die Erhebung der Daten erfolgt auf verschiedene Art und Weise. Bei Eurodac, VIS und EES werden die Daten von BeamtInnen erhoben.[1005] Die im SIS und im ECRIS-TCN gespeicherten Daten basieren hingegen auf Daten, welche im Rahmen eines administrativen resp. gerichtlichen Verfahrens erhoben wurden.[1006] Beim ETIAS wiederum werden die Daten in der Regel von der antragstellenden Person selbst angegeben.[1007]

Generell ist es bei all diesen Arten der Datenerhebung möglich, dass Fehler unterlaufen.[1008] Grundsätzlich dürfte es sich bei den ETIAS-Daten um die unzuverlässigsten Daten handeln. Denn diese werden von der betroffenen Person selbst, also ohne Kontrolle durch eine Drittperson, eingegeben. Dies erleichtert es, absichtlich falsche Daten anzugeben. Zudem ist die betroffene Person, anders als z.B. BeamtInnen, nicht bezüglich der Erhebung der Daten geschult. Es dürften deshalb vermehrt Flüchtigkeitsfehler oder sonstige (geläufige) Fehler bei der Dateneingabe auftreten.[1009]

Bei der Datenerhebung durch BeamtInnen dürften solche Fehler weniger häufig auftreten. Die Quelle der Daten, welche von den BeamtInnen erhoben werden, könnte sich jedoch auf die Zuverlässigkeit der Daten auswirken. Werden die Daten einem offiziellen Reisedokument entnommen, dürften die Daten grundsätzlich zuverlässiger sein, als wenn die Angaben von der betroffenen

1004 Beim VIS und bei Eurodac wurde bereits festgestellt, dass biometrische Daten falsch verlinkt wurden. Siehe dazu FRA, biometrics, 90.

1005 Siehe dazu Kapitel III.5.4; III.6.4 und III.7.4.

1006 Siehe dazu Kapitel III.4.4 und III.9.4.

1007 Siehe dazu Kapitel III.8.4. Es ist jedoch auch vorgesehen, dass eine Person für eine andere einen Antrag stellen kann.

1008 Siehe dazu die möglichen Fehlerquellen bei der Datenbearbeitung in Kapitel IV.5.4.2.1.

1009 Vgl. dazu FRA, Opinion IOP, 37 f.

Person selbst gemacht werden. So können nämlich absichtlich falsche Angaben nicht vermieden werden.

Am zuverlässigsten dürften diejenigen Daten sein, die im Zusammenhang mit einem administrativen resp. gerichtlichen Verfahren erhoben wurden. Bei der Erhebung der Daten in solchen Verfahren haben diverse Personen, insbesondere auch die betroffene Person, mitgewirkt. Die Wahrscheinlichkeit ist deshalb gross, dass allfällige Fehler entdeckt worden wären.

Die Art und Weise der Erhebung der Daten indiziert folglich, wie fehleranfällig resp. zuverlässig die Daten grundsätzlich zu werten sind.

5.4.2.3 *Bisherige Sicherheitsmassnahmen*

Um den vorstehend aufgezeigten Fehlerquellen zu begegnen, sind in den gesetzlichen Grundlagen der einzelnen Systeme bereits bestimmte Sicherheitsmassnahmen vorhanden. So ist es bspw. technisch nicht möglich, Eingabefelder leerzulassen oder unerlaubte Zeichen einzufügen. Ausserdem wird eine Überprüfung des Formats vorgenommen und die Daten werden auf Ungereimtheiten geprüft.[1010]

Bei Eurodac stellt die manuelle Überprüfung eines Treffers durch einen Daktyloskopie-Experten eine wichtige Sicherheitsmassnahme dar. Dieser überprüft erweiterte Merkmale wie z.B. Porenstrukturen.[1011] Falsche biometrische Treffer sind eu-LISA zu melden.[1012] Im Jahr 2023 wurden bei Eurodac 212 falsche Treffer registriert.[1013]

Während primär die Schengen/Dublin-Staaten für die Genauigkeit und die Qualität der biometrischen Daten zuständig sind, überwacht eu-LISA die Einhaltung von Qualitätsstandards.[1014] Aufgrund mangelnder Qualität wurden im Jahr 2023 bei Eurodac 2,9 %, absolut knapp 40'000, der Fingerabdruckdaten zurückgewiesen. Im Jahr davon waren es 3,1 %.[1015]

1010 HLEG, final report, 10 f.

1011 In der Schweiz soll die biometrische Abteilung von fedpol nun nicht nur bei Eurodac, sondern bei allen biometrischen Treffern in EU-Informationssystemen eine solche manuelle Überprüfung vornehmen, um falsche Treffer zu vermeiden. Diese Änderung erfolgt dabei unabhängig von einer Schengen/Dublin-Weiterentwicklung. Siehe dazu BUNDESRAT, Botschaft ETIAS Consequential Amendments, 4, 94.

1012 FRA, biometrics, 92.

1013 EU-LISA, Eurodac report 2023, 18.

1014 FRA, biometrics, 88.

1015 EU-LISA, Eurodac report 2023, 19.

Wurden unrichtige Daten erfasst, steht den betroffenen Personen grundsätzlich das Recht zu, die Berichtigung resp. die Löschung derselben zu beantragen.[1016]

5.4.2.4 *Neue Sicherheitsmassnahmen*

Die Thematik der Datenqualität wird in den EU-IOP-VO explizit aufgegriffen. Demnach soll eu-LISA Mechanismen und Verfahren für die automatische Datenqualitätskontrolle einführen.[1017] Ausserdem sollen nur Daten in das EES, das VIS, das ETIAS, das SIS, Eurodac, das ECRIS-TCN, den BMS, den CIR und den MID eingegeben werden können, welche einem gewissen Mindestqualitätsstandard entsprechen. Auch die im BMS gespeicherten Templates werden einer automatischen Qualitätskontrolle unterzogen, ehe sie gespeichert werden. Die IT-Agentur hat zudem regelmässig Berichte über die Datenqualität zuhanden verschiedener Empfänger zu verfassen. Weiter wird die Kommission die Umsetzung der Datenqualität in den Schengen/Dublin-Staaten evaluieren und ggf. Empfehlungen abgeben. In der Folge haben die Schengen/Dublin-Staaten einen Aktionsplan zur Beseitigung der allfällig festgestellten Mängel vorzulegen.[1018]

Ebenfalls zur Verbesserung der Datenqualität trägt die manuelle Verifizierung bei. Die in automatisierter Weise erstellten Verknüpfungen werden bei der Verifizierung einer Prüfung durch eine Person unterzogen. Teilweise wird die manuelle Verifizierung im Beisein der betroffenen Person eingeleitet. Anlässlich dieser Überprüfung können resp. sollten auch allfällige unrichtige Daten erkannt und berichtigt werden können.[1019]

Obwohl im Rahmen der Interoperabilität verschiedene Sicherheitsmassnahmen vorgesehen sind, welche eine hohe Datenqualität gewährleisten sollen, können falsche Treffer resp. falsche Nicht-Treffer nicht ausgeschlossen werden. Da die Interoperabilität u.a. gerade zum Zweck errichtet wurde, Mehrfachidentitäten aufzudecken und Identitätsbetrug zu bekämpfen, besteht die

---

1016 Siehe dazu Kapitel III.4.6.3; III.5.6.3; III.6.6.3; III.7.6.3; III.8.6.3 sowie III.9.6.3.

1017 Der EDSB hat gefordert, dass die automatischen Datenqualitätskontrollen so früh wie möglich eingeführt und davor auch getestet werden (nicht erst nach der Inbetriebnahme der Systeme). Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 108 ff.

1018 Siehe zu den Einzelheiten Art. 37 EU-IOP-VO; Art. 13 Abs. 3 EU-IOP-VO.

1019 Siehe zu den Einzelheiten der manuellen Verifizierung Art. 29 EU-IOP-VO. Ebenfalls können der CRRS sowie das UMF zu einer besseren Datenqualität beitragen. Siehe dazu Art. 38 EU-IOP-VO; Art. 39 EU-IOP-VO. In der vorliegenden Untersuchung wird auf weitere Ausführungen dazu verzichtet. Siehe dazu Kapitel IV.5.3.

Gefahr, dass bei einem Treffer den betroffenen Personen vorgeworfen wird, absichtlich falsche Angaben gemacht zu haben, um unter verschiedenen Identitäten registriert zu werden.[1020]

Die Datenqualität ist von entscheidender Bedeutung für die Wirksamkeit der Interoperabilität. Sie kann nur erfolgreich sein, wenn die gespeicherten Daten zuverlässig sind. Grundsätzlich sollte primär sichergestellt werden, dass die erhobenen Daten schon bei ihrer Eingabe in das entsprechende Informationssystem korrekt sind und nicht nachträglich korrigiert werden müssen.[1021]

Letztlich verbleibt aufgrund der beschriebenen Problematik der Fehleranfälligkeit der Daten immer ein gewisses Restrisiko. Da die Interoperabilität die Aufdeckung von Mehrfachidentitäten sowie die Bekämpfung von Identitätsbetrug bezweckt, sollte bei einem positiven Treffer auch stets berücksichtigt werden, dass es sich (wegen mangelnder Datenqualität) auch um einen falschen Treffer handeln könnte.

5.4.2.5 *Effekt der Interoperabilität auf die Datenqualität*

Bezüglich des Effekts der Interoperabilität auf die Qualität der Daten besteht Uneinigkeit. Einerseits wird die Ansicht vertreten, dass durch die Interoperabilität das Risiko bestehe, dass sich falsche Angaben in anderen Systemen sowie auch auf nationaler Ebene vervielfältigen könnten. Dies hätte zur Folge, dass die Abfrage in den Systemen vermehrt falsche Ergebnisse hervorbringen würde.[1022] Andererseits wird auch die Ansicht vertreten, dass die Interoperabilität eine Chance darstelle, um unrichtige Daten im Abgleich mit anderen Datenbanken besser zu erkennen. Die Interoperabilität schaffe neue Möglichkeiten und könne dazu führen, dass Fehler und Unregelmässigkeiten häufiger von den Behörden entdeckt würden. In der Folge könnten Massnahmen ergriffen werden, um diese zu korrigieren.[1023]

Durch den MID werden verschiedenfarbige Verbindungen zwischen unterschiedlichen Datensätzen hergestellt. Grundsätzlich können dadurch unrichtige Daten entdeckt werden. Ob die Interoperabilität die Datenqualität verbessert oder verschlechtert, hängt davon ab, ob die festgestellten unrichtigen Daten – im Rahmen der manuellen Verifizierung – korrigiert werden und da-

1020 Vgl. dazu FRA, biometrics, 86.
1021 Vgl. dazu VAVOULA, Deathblow, 152 f.
1022 SFH, Vernehmlassungsantwort, 5. Siehe dazu auch FRA, borders and security, 29; QUINTEL, data retention, 15.
1023 FRA, borders and security, 29.

mit die Datenqualität verbessert wird oder ob die festgestellten unrichtigen Daten vielmehr – aufgrund mangelnder Beweise – nicht als solche erkannt werden können. Dies hätte zur Konsequenz, dass falsche Verknüpfungen bestehen bleiben und diese allenfalls negative Folgen für die betroffene Person haben. Es wird sich somit erst nach der Inbetriebnahme der Interoperabilität zeigen, welchen Einfluss die Interoperabilität auf die Datenqualität hat.

5.4.3. Aufsicht

Die durch die Interoperabilität ermöglichte Datenbearbeitung wird von verschiedenen Aufsichtsbehörden überwacht. So einerseits von den nationalen Aufsichtsbehörden. Die Schengen-Staaten haben u.a. sicherzustellen, dass diese die Rechtmässigkeit der Datenbearbeitung, welche ihre Behörden vornehmen, unabhängig überwachen können. Ferner ist auch dafür zu sorgen, dass die nationalen Aufsichtsbehörden über ausreichende Ressourcen sowie Fachkenntnisse zur Wahrnehmung ihrer Aufgaben verfügen. Die nationalen Aufsichtsbehörden haben gewisse statistische Angaben zur Datenbearbeitung zu veröffentlichen und können die Protokolle, welche über die Datenbearbeitungen des ESP, des BMS, des CIR und des MID erstellt werden, einsehen. Des Weiteren haben sie Zugang zu den Begründungen der nationalen Strafverfolgungsbehörden, welche gemäss Art. 22 Abs. 2 EU-IOP-VO keinen Antrag auf vollständigen Zugang zu den Daten beantragen. Ausserdem können sie alle Räumlichkeiten betreten, welche für die Zwecke der Interoperabilität genutzt werden.[1024]

Andererseits übt der EDSB die Aufsicht über die EU-Stellen aus, welche im Rahmen der Interoperabilität Datenbearbeitungen vornehmen. Der EDSB erstellt mindestens alle vier Jahre einen Bericht über die Datenbearbeitungen von eu-LISA, die ETIAS-Zentralstelle und Europol. Er kann die für das ESP, den BMS, den MID und den CIR erstellten Protokolle ebenfalls einsehen und erhält jederzeit Zutritt zu den Räumlichkeiten.[1025]

Der EDSB und die nationalen Aufsichtsbehörden arbeiten aktiv zusammen und stellen eine koordinierte Aufsicht sicher.[1026]

1024 Siehe zu den Einzelheiten Art. 51 EU-IOP-VO.
1025 Siehe zu den Einzelheiten Art. 52 EU-IOP-VO.
1026 Siehe dazu Art. 53 EU-IOP-VO.

5.4.4. Übermittlung an Drittstaaten, internationale Organisationen sowie private Stellen

Grundsätzlich dürfen die im Rahmen der Interoperabilität bearbeiteten Daten nicht an Drittstaaten, internationale Organisationen oder private Stellen übermittelt oder diesen zur Verfügung gestellt werden.[1027]

5.4.5. Rechte der betroffenen Personen

Im Zeitpunkt der Datenerfassung haben die Behörden, welche die Daten erfassen, die im BMS, CIR oder im MID gespeichert werden, den betroffenen Personen bestimmte Informationen zur Verfügung zu stellen. Diese Informationen über die Datenbearbeitung müssen in einer klaren und verständlichen Sprache kommuniziert werden, welche die betroffene Person versteht oder zumindest davon ausgegangen werden kann, dass sie diese versteht. Minderjährige müssen in einer ihrem Alter angemessenen Weise informiert werden.[1028] Unter Vorbehalt von einigen Ausnahmen sind von einer roten Verknüpfung betroffene Personen darüber in Kenntnis zu setzen.[1029]

Ausserdem ist ein Recht auf Auskunft, Berichtigung und Löschung von im MID gespeicherten Daten sowie auf Einschränkung ihrer Verarbeitung vorgesehen.[1030] Die Beschränkung dieser Rechte auf im MID bearbeiteten Daten dürfte darauf zurückzuführen sein, dass im ESP keine Daten gespeichert werden. Bei im CIR gespeicherten Angaben handelt es sich um Daten, welche gemäss den gesetzlichen Grundlagen der einzelnen Systeme erhoben werden. Die im BMS gespeicherten Templates basieren wiederum auf den biometrischen Daten, welche ebenfalls aufgrund der gesetzlichen Grundlagen der einzelnen Systeme erhoben werden. Bezüglich dieser Daten ist in den gesetzlichen Grundlagen der einzelnen Systeme bereits jeweils ein Recht auf Auskunft, Berichtigung und Löschung verankert.[1031] Im MID hingegen wird eine Identitätsbestätigungsdatei angelegt, welche u.a. die Farbe der Verknüpfung, die Angabe der von der Verknüpfung betroffenen Informationssysteme sowie die für das Abrufen der Daten in diesen Systemen notwendige einmalige Kennnum-

1027 Siehe dazu Art. 50 EU-IOP-VO. Dort werden auch die Ausnahmen von diesem Grundsatz aufgeführt.

1028 Art. 47 EU-IOP-VO; BUNDESRAT, Botschaft IOP, 8016.

1029 Siehe dazu Art. 32 Abs. 4 EU-IOP-VO.

1030 Siehe zu den Einzelheiten Art. 48 EU-IOP-VO.

1031 Siehe dazu Art. 53 SIS-Grenze-VO; Art. 67 SIS-Polizei-VO; Art. 29 Abs. 4-15 Eurodac-VO; Art. 38 VIS-VO; Art. 14 VIS-Beschluss; Art. 52 EES-VO; Art. 64 ETIAS-VO; Art. 25 ECRIS-TCN-VO.

mer enthält. Nur bei den im MID gespeicherten Verknüpfungen handelt es sich demnach um durch die Interoperabilität neu geschaffene Daten. Folglich muss nur für die im MID gespeicherten Daten ein Recht auf Auskunft, Berichtigung und Löschung in den EU-IOP-VO vorgesehen werden.

Zur Erleichterung der Ausübung dieser Rechte wird ein Web-Portal eingerichtet. Dieses informiert u.a. über die zur Verfügung stehenden Rechte der betroffenen Personen sowie die Verfahren zur Geltendmachung dieser Rechte.[1032]

5.4.6. Haftung und Sanktionen

Personen resp. Schengen-Staaten, welchen durch eine gegen die EU-IOP-VO verstossende Handlung durch einen anderen Staat, Europol, eu-LISA resp. Frontex ein materieller oder immaterieller Schaden entstanden ist, können Schadenersatz verlangen. Eine (teilweise) Befreiung von der Haftung ist möglich, wenn der Nachweis gelingt, dass hinsichtlich des eingetretenen Schadens keine Verantwortung übernommen werden muss. Für Schäden an den Komponenten, welche durch eine Pflichtverletzung entstanden sind, haften die Schengen-Staaten zudem, sofern sowohl eu-LISA als auch ein anderer Schengen-Staat es versäumt haben, Massnahmen zur Verhinderung resp. Verringerung des Schadens zu ergreifen. Hinsichtlich der Geltendmachung von Schadenersatzansprüchen sind je nach dem gegen wen sich diese richten, entweder das nationale Recht des beklagten Schengen-Staats oder die in den Verträgen vorgesehenen Voraussetzungen einschlägig.[1033]

Davon abgesehen haben die Schengen-Staaten wirksame, verhältnismässige und abschreckende Sanktionen gegen die missbräuchliche Bearbeitung von Daten vorzusehen.[1034]

1032 Siehe zu den Einzelheiten zum Webportal Art. 49 EU-IOP-VO.
1033 Siehe dazu Art. 46 EU-IOP-VO.
1034 Art. 45 EU-IOP-VO.

6. Beteiligung der Schweiz

6.1. Übernahme und Umsetzung der EU-IOP-VO

Die EU-IOP-VO wurden der Schweiz am 21. Mai 2019 als Weiterentwicklungen des Schengen-Besitzstands notifiziert.[1035] Die entsprechenden Notenaustausche sind am 16. Juli 2021 in Kraft getreten.[1036]

Die EU-IOP-VO enthalten sowohl direkt anwendbare Bestimmungen als auch solche, welche auf nationaler Ebene zu konkretisieren sind. Bspw. sind die Zwecke der Datenbearbeitung, die Zugriffsrechte sowie die Weitergabe von Daten als auch die Sanktionen formell-gesetzlich zu regeln. Auf Gesetzesstufe mussten insbesondere das AIG sowie das BPI geändert werden, da dort die der Interoperabilität zugrunde liegenden Informationssysteme geregelt sind.[1037] Eine Vielzahl der Neuerungen betrifft das Verordnungsrecht, welches entsprechend anzupassen resp. neu zu schaffen ist.[1038]

Insbesondere wird eine neue Verordnung geschaffen (die N-IOP-Verordnung). Diese ist noch nicht in Kraft. Sie soll u.a. die Zugriffsberechtigungen genauer festlegen, die Zugriffsberechtigungen gemäss Art. 20-22 EU-IOP-VO präzisieren, das Verfahren der manuellen Verifizierung von MID-Verknüpfungen regeln und die Rechte der betroffenen Personen näher ausführen.[1039]

6.2. Ausgestaltung der Interoperabilität in der Schweiz

Zwar stellen die EU-IOP-VO Weiterentwicklungen des Schengen-Besitzstands dar, welche die Schweiz übernommen hat. Die Interoperabilität beschränkt sich jedoch nicht auf diese beiden Verordnungen. So sind primär sechs Informationssysteme von der Interoperabilität betroffen. Diese haben jeweils eine eigene gesetzliche Grundlage. Hinzu kommt, dass auch verschiedene EU-Akteure in die Interoperabilität involviert sind. Aufgrund dieser Umstände wird

1035 Bundesrat, Botschaft IOP, 7991 f.

1036 Siehe dazu Notenaustausch IOP-Grenze-VO; Notenaustausch IOP-Polizei-VO.

1037 Im BPI, in welchem die polizeilichen Informationssysteme des Bundes geregelt werden, mussten dem AIG sehr ähnliche Bestimmungen zu bestimmten Interoperabilitätskomponenten aufgenommen werden. Siehe zu den Einzelheiten Bundesrat, Botschaft IOP, 8022 f. Siehe zu den konkreten gesetzlichen Anpassungen Bundesbeschluss IOP.

1038 Bundesrat, Botschaft IOP, 8020.

1039 Siehe dazu Vorentwurf N-IOP-Verordnung; Bundesamt für Polizei, Erläuternder Bericht N-IOP-Verordnung.

sich die Ausgestaltung der Interoperabilität in der Schweiz von derjenigen in den Mitgliedstaaten – in mehr oder weniger grossem Ausmass – unterscheiden.[1040]

Die ECRIS-TCN-VO stellt keine Weiterentwicklung des Schengen/Dublin-Besitzstands dar. Zwar wird aktuell eine mögliche Teilnahme der Schweiz – auf freiwilliger Basis – geprüft. Sollte jedoch kein entsprechendes Abkommen abgeschlossen werden, wird sich die Schweiz nicht am ECRIS-TCN beteiligen.[1041] In diesem Fall sowie auch falls die Interoperabilität vor dem ECRIS-TCN in Betrieb genommen würde, könnte sich dies folgendermassen auf die Ausgestaltung der Interoperabilität in der Schweiz auswirken: Beim ESP ist explizit festgehalten, dass Treffer nur angezeigt werden, wenn auf die von diesem Treffer betroffenen Systeme gemäss deren gesetzlichen Grundlagen resp. des nationalen Rechts ein Zugriffsrecht besteht. Es dürfte deshalb davon ausgegangen werden, dass allfällige Treffer im ECRIS-TCN den nationalen Behörden der Schweiz, welche das ESP abfragen dürfen, nicht angezeigt würden.

Bei den drei Abfragetypen des CIR gemäss Art. 20-22 EU-IOP-VO ist hingegen festgehalten, dass die nationalen Stellen das ESP gemäss den in den EU-IOP-VO festgelegten Zugriffsrechten nutzen dürfen.[1042] Bei den Abfragen des CIR zu Identifizierungszwecken gemäss Art. 20 EU-IOP-VO sowie bei der Abfrage des CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten gemäss Art. 21 EU-IOP-VO werden nationale Behörden teilweise berechtigt, auf Daten zuzugreifen, auf welche sie gemäss den gesetzlichen Grundlagen der einzelnen Systeme nicht zugreifen dürfen. Mit Art. 20 EU-IOP-VO wird den nationalen Polizeibehörden in bestimmten Fällen ein Abfragerecht auf die im CIR gespeicherten Daten zugestanden, sofern sie das nationale Recht dazu ermächtigt. Es handelt sich damit um eine neue Abfrage. Auch bei der in Art. 21 EU-IOP-VO vorgesehenen Abfrage wird bestimmten Behörden, sofern gewisse Voraussetzungen vorliegen, zu definierten Zwecken beim Vorliegen einer gelben resp. roten Verknüpfung ein neues Zugriffsrecht gewährt.

Es stellt sich deshalb bei diesen Abfragetypen die Frage, ob diese neuen Zugriffsrechte beim Vorliegen eines Treffers mit ECRIS-TCN-Daten auch den nationalen Behörden eines Staats gewährt werden, welcher sich nicht an diesem

1040 Die Ausgestaltung der Interoperabilität kann sich auch in den Mitgliedstaaten unterscheiden. So bei Mitgliedstaaten, welche sich nicht vollumfänglich an der Schengener Zusammenarbeit beteiligen. Z.B. verfügt Irland über keinen Zugriff zum SIS und wird deshalb den MID nicht nutzen können. Siehe dazu BUNDESRAT, Botschaft IOP, 7992.

1041 Siehe dazu BUNDESRAT, Botschaft IOP, 8001.

1042 Art. 7 Abs. 2 EU-IOP-VO.

System beteiligt. Schliesslich ist denkbar, dass diese neuen Zugriffsrechte nur unter der Annahme gewährt wurden, weil sich die involvierten Staaten jeweils an allen betroffenen Informationssystemen beteiligen. Andererseits hätte dies u.a. zur Folge, dass wenn eine nationale Behörde der Schweiz für die manuelle Verifizierung einer gelben Verknüpfung zuständig ist, möglicherweise nicht auf alle involvierten Daten zugreifen kann. Dies würde die Effektivität der Interoperabilität einschränken. Wie dies gehandhabt wird, dürfte sich erst in der Praxis zeigen, sofern sich die Schweiz letztlich nicht am ECRIS-TCN beteiligt resp. die Inbetriebnahme dieses Systems nach derjenigen der Interoperabilität in der Schweiz erfolgt.

Bei der Abfrage des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten gemäss Art. 22 EU-IOP-VO werden keine ECRIS-TCN-Daten abgefragt.[1043] Der Zugriff der nationalen Strafverfolgungsbehörden auf Eurodac-Daten stellt jedoch kein Dublin-Besitzstand dar. Gemäss dem Eurodac-Protokoll wird diese Zugriffsmöglichkeit zwar zukünftig auch in der Schweiz eingeführt.[1044] Für den Fall, dass die Interoperabilität vor der Einführung dieser Zugriffsberechtigung in Betrieb genommen wird, stellt sich auch hier die Frage, ob den nationalen Behörden der Schweiz allfällige Treffer mit Eurodac-Daten angezeigt würden. Dies müsste verneint werden, weil mit Art. 22 EU-IOP-VO kein neues Zugriffsrecht geschaffen wurde, sondern diese Bestimmung lediglich das Verfahren einer bereits bestehenden Zugangsberechtigung ändert.

Der Vollständigkeit halber sei des Weiteren erwähnt, dass die Schweiz derzeit über keinen direkten Zugriff auf Europol-Daten verfügt. Es besteht zwar die Möglichkeit, dass Daten zwischen der Schweiz und Europol übermittelt werden.[1045] Die Schweiz strebt einen direkten Zugriff auf Europol-Daten an.[1046] Da auch Europol-Daten teilweise in die Interoperabilität involviert werden, könnten sich aufgrund des Zugriffsrechts der Schweiz auf solche Daten allfällige Auswirkungen auf die Ausgestaltung der Interoperabilität ergeben.[1047]

1043 Siehe dazu Kapitel IV.5.3.3.3.
1044 Siehe dazu Kapitel III.5.3.
1045 Siehe dazu Art. 8 und Art. 9 Abkommen CH-Europol.
1046 Siehe dazu BUNDESRAT, Botschaft IOP, 8001 f. m.w.H.
1047 Hierzu erübrigen sich jedoch weitere Ausführungen, weil die Europol-Daten nicht Gegenstand der vorliegenden Untersuchung sind. Siehe zu dieser Ausklammerung Kapitel III.1.

7. Fazit

Der Begriff der Interoperabilität wird nicht ausschliesslich im Zusammenhang mit dem EU-Projekt, welches im Fokus der vorliegenden Untersuchung steht, verwendet. Im Allgemeinen wird darunter ein Verknüpfen resp. Verbinden verstanden. Im Rahmen der Interoperabilität der EU-Informationssysteme ist der Begriff dahingehend zu verstehen, dass die betroffenen Informationssysteme befähigt werden sollen, Daten miteinander auszutauschen und Informationen gemeinsam zu nutzen. Das bisher geschlossene Umfeld der einzelnen Informationssysteme wird dadurch zu einer gemeinsamen Umgebung.

Bereits vor der Entwicklung der Interoperabilität der EU-Informationssysteme gab es Bestrebungen, Informationssysteme interoperabel auszugestalten. Letztlich wurden diese jedoch nie realisiert. Im Zuge der steigenden Anzahl von illegalen Grenzübertritten im Jahr 2015 sowie von verschiedenen Terroranschlägen in Europa wurde die Idee von interoperablen Datenbanken wieder aufgegriffen und letztlich umgesetzt. Auffällig ist, dass in der Entwicklungs- resp. Umsetzungsphase der Interoperabilität die gesetzlichen Grundlagen der von der Interoperabilität betroffenen Informationssysteme entweder erst neu geschaffen oder erneut revidiert wurden.[1048]

Mit der Interoperabilität wird ein verbesserter Informationsaustausch zwischen bestimmten Informationssystemen angestrebt. Dieser soll durch einen gezielteren Zugang zu den betroffenen Informationssystemen ermöglicht werden. Die zugriffsberechtigten Behörden sollen über jegliche für sie relevanten Informationen verfügen und somit schnell und effizient ein umfassendes Bild einer Person erhalten können. Weiter soll die Interoperabilität die korrekte Identifizierung der in den Informationssystemen erfassten Personen erleichtern. Der Zugang von Strafverfolgungsbehörden soll ebenso erleichtert wie auch vereinfacht werden. Davon abgesehen soll die Interoperabilität insbesondere auch die Aufdeckung von Mehrfachidentitäten ermöglichen, wobei dadurch Identitätskontrollen von Personen mit rechtmässigen Mehrfachidentitäten erleichtert werden können und Identitätsbetrug bekämpft werden

[1048] Dies wurde vom EDSB kritisiert, da es von zentraler Bedeutung sei, Kohärenz zwischen den beteiligten Rechtssetzungsprojekten zu schaffen. Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 24. Auch aus den Diskussionen der Expertengruppe ging hervor, dass die bereits bestehenden Systeme und Praktiken zuerst verbessert werden sollten, bevor neue entwickelt werden. Siehe dazu HLEG, Interim Report, 3.

kann. Mit diesen Bestrebungen wird primär das Ziel, die Sicherheit im Schengen-Raum zu erhöhen, verfolgt.[1049]

Die Interoperabilität wird insbesondere durch die Einführung von vier Komponenten (ESP, BMS, CIR und MID) ermöglicht. Diese bearbeiten sowohl alphanumerische als auch biometrische Daten. Anders als die Komponenten CIR, BMS und MID speichert das ESP keine Daten. Dieses erfüllt vielmehr die Funktion eines Suchportals. Durch die Speicherung von gewissen Daten schaffen die anderen drei Komponenten jeweils einen zentralisierten, EU-weiten Speicher. So werden die biometrischen Templates nicht mehr einzeln in den jeweiligen Informationssystemen gespeichert, sondern zentral im BMS. Der CIR ersetzt die betroffenen Informationssysteme insofern, als dass dieser bestimmte Angaben zur Person, zu den Reisedokumenten sowie bestimmte biometrische Daten an einem Ort speichert. Im MID werden in den Identitätsbestätigungsdateien einmalige Kennnummern gespeichert, anhand welcher die verknüpften Daten abgerufen werden können. Die Komponenten ergänzen sich gegenseitig und sind voneinander abhängig. So wird bspw. mit dem BMS und den darin gespeicherten Templates die Abfrage von biometrischen Daten im CIR und im SIS ermöglicht. Ausserdem ist der CIR mit den jeweils anderen Komponenten mit einer Kommunikationsinfrastruktur verbunden.

Das ESP gewährt die in den gesetzlichen Grundlagen der betroffenen Informationssysteme vorgesehenen Zugriffsrechte. Durch den CIR werden jedoch auch neue Zugriffsrechte geschaffen. So u.a. wenn Daten mit einer gelben oder roten Verknüpfung gekennzeichnet werden. In diesen Fällen dürfen die für die manuelle Verifizierung zuständigen Behörden resp. diejenigen Behörden, welche auf ein von einer roten Verknüpfung betroffenes Informationssystem zugreifen dürfen, auch auf die verknüpften Daten zugreifen. Auch die Zugangsmöglichkeiten der Polizeibehörden auf den CIR gemäss Art. 20 EU-IOP-VO sind nicht in den gesetzlichen Grundlagen der einzelnen Systeme vorgesehen, weshalb es sich dabei ebenfalls um eine neue Zugriffsgewährung handelt. Insofern erweist sich die zu Beginn der Entwicklung der Interoperabilität von der Kommission geäusserte Aussage, dass durch die Interoperabilität die bestehenden Zugriffsberechtigungen nicht geändert werden, als trügerisch.[1050] Davon abgesehen wird den Strafverfolgungsbehörden zwar bereits in den be-

[1049] Zur Verwirklichung der Ziele der Interoperabilität hat zudem auch beigetragen, dass der Umfang der gespeicherten Daten in den einzelnen Systemen stetig zugenommen hat (siehe dazu Kapitel III.10). So stehen nun mehr und insbesondere auch biometrische Daten für die Zwecke der Interoperabilität zur Verfügung.

[1050] Siehe dazu Kapitel IV.4.

stehenden gesetzlichen Grundlagen der betroffenen Informationssysteme Zugriff gewährt. Die Zugangsbedingungen dieser Behörden werden durch die Interoperabilität jedoch insofern verändert, als ein zweistufiges Verfahren vorgesehen wird, welches die Abfrage vereinheitlichen sowie erleichtern soll.

Da die EU-IOP-VO eine Weiterentwicklung des Schengen-Besitzstands darstellen, hat die Schweiz diese beiden Verordnungen übernommen. Aufgrund der Tatsache, dass die Schweiz kein Mitgliedstaat ist, sondern sich als ein an Schengen und Dublin assoziierter Staat an der Interoperabilität beteiligt, könnte sich deren Ausgestaltung in der Schweiz von derjenigen in einem Mitgliedstaat unterscheiden (z.B. im Hinblick auf das ECRIS-TCN).

Mit der Interoperabilität wird also die bestehende Struktur der betroffenen Informationssysteme aufgebrochen. Zudem werden neue Funktionen eingeführt und neue Zugriffsberechtigungen geschaffen. Im Hinblick auf den Datenschutz wurde aus diesem Kapitel ersichtlich, dass in den EU-IOP-VO verschiedene Sicherheitsmassnahmen vorgesehen sind. Inwiefern die Interoperabilität mit dem grundrechtlich geschützten Datenschutz vereinbar ist, wird im folgenden Kapitel vertieft untersucht. Im Fokus stehen dabei vor allem die vier Komponenten sowie die neuen Zugriffsmöglichkeiten.

V. Vereinbarkeit der Interoperabilität mit dem Grundrecht auf Datenschutz

1. Einleitung

In den vorangehenden Kapiteln wurde ausführlich erklärt, was mit der Interoperabilität bezweckt wird, wie sie ausgestaltet ist und welche Informationssysteme von diesem Projekt betroffen sind.[1051] Des Weiteren wurde der Schutzbereich des grundrechtlich geschützten Datenschutzes dargelegt, wie dieser von der EMRK, der GRC und der BV definiert wird und aufgezeigt, unter welchen Voraussetzungen ein Eingriff in den Schutzbereich gerechtfertigt werden kann.[1052]

Im vorliegenden Kapitel wird nun untersucht, inwiefern die Interoperabilität mit dem Grundrecht auf Datenschutz vereinbar ist.

Unter der Bezeichnung «*Grundrecht auf Datenschutz*» wird der (datenschutzrechtliche) Gehalt von Art. 8 EMRK, Art. 8 GRC sowie Art. 13 Abs. 2 BV verstanden. Wie das Kapitel II gezeigt hat, sind sich diese Grundrechte sehr ähnlich. Deshalb werden diese Grundrechte für die folgende Untersuchung als *ein* Grundrecht behandelt. Nur wenn auf Spezialitäten eines Grundrechts eingegangen wird, welche die jeweils anderen Grundrechte nicht aufweisen, wird das betreffende Grundrecht explizit genannt.[1053]

Die Prüfung der Vereinbarkeit der Interoperabilität mit dem Grundrecht auf Datenschutz wird wie folgt vorgenommen: Wie bereits in Kapitel II aufgezeigt, wird für die Prüfung einer Rechtfertigung eines Eingriffs in Art. 8 EMRK, Art. 8 GRC resp. Art. 13 Abs. 2 BV jeweils ein eigenes Prüfschema verwendet, wobei die dafür verwendeten Kriterien zumindest grösstenteils identisch sind.[1054] Da die vorliegende Untersuchung den Fokus auf die Schweiz legt, werden diejenigen Kriterien verwendet, welche bei Eingriffen in Art. 13 Abs. 2 BV geprüft werden. Es wird deshalb – nachdem festgestellt wird, dass ein Eingriff in den Schutzbereich des Grundrechts auf Datenschutz vorliegt – im Rahmen der

---

1051 Siehe zur Interoperabilität ausführlich Kapitel IV. Siehe zu den Informationssystemen Kapitel III.4; III.5; III.6; III.7; III.8 und III.9.

1052 Siehe dazu ausführlich Kapitel II.

1053 Siehe zum «*Grundrecht auf Datenschutz*» Kapitel I.2.

1054 Siehe dazu Kapitel II.7.3.

Rechtfertigung geprüft, ob eine gesetzliche Grundlage vorhanden ist, ein öffentliches Interesse verfolgt wird, in den Kerngehalt des Grundrechts eingegriffen wird und die Massnahme verhältnismässig ist.[1055]

Geprüft wird die Interoperabilität. Dieses Projekt stellt also gewissermassen die – wie nachfolgend noch dargelegt wird – in das Grundrecht auf Datenschutz eingreifende Massnahme dar. Wie bereits aus Kapitel IV hervorgegangen ist, umfasst die Interoperabilität verschiedene Datenbearbeitungen. Im Zentrum stehen dabei insbesondere die vier Interoperabilitätskomponenten. Aber auch die neu geschaffenen Zugriffsberechtigungen, also der Zugriff der Polizeibehörden auf den CIR gemäss Art. 20 EU-IOP-VO und der Zugang zum CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten gemäss Art. 21 EU-IOP-VO, stellen einen wesentlichen Teil der Interoperabilität dar. Mit Art. 22 EU-IOP-VO werden zudem die bisher festgelegten Zugangsbedingungen für die Abfrage zwecks Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten wesentlich verändert.[1056] Auch dabei handelt es sich um einen zentralen Aspekt der Interoperabilität. Diese verschiedenen Datenbearbeitungen stellen für sich genommen grundsätzlich je einen eigenständigen Eingriff in das Grundrecht auf Datenschutz dar, welcher rechtfertigungsbedürftig ist. Wie sich jedoch gezeigt hat, sind insbesondere die einzelnen Interoperabilitätskomponenten voneinander abhängig und unterstützen sich gegenseitig.[1057] Insofern ist die Interoperabilität als ein gesamtes Projekt zu verstehen. Bereits im Entstehungsprozess der Interoperabilität wurde festgehalten, dass nur mit der Einführung von allen vier Komponenten die Zielsetzung der Interoperabilität erreicht werden kann.[1058] Um die Eigenständigkeit der Datenbearbeitungen dennoch zu würdigen, wird bei der Prüfung der Verhältnismässigkeit sowohl auf die Interoperabilitätskomponenten sowie auf die Abfragen gemäss Art. 20-22 EU-IOP-VO einzeln eingegangen.[1059]

Die Festlegung der Interoperabilität als eingreifende Massnahme hat ausserdem zur Folge, dass ausschliesslich die damit anvisierte Verknüpfung der Datenbanken auf die Vereinbarkeit mit dem Grundrecht auf Datenschutz untersucht wird. Inwiefern die von der Interoperabilität betroffenen Informationssysteme im Ein-

1055 Bei der Beurteilung der Verhältnismässigkeit werden zudem auch die Subkriterien, also die Geeignetheit, die Erforderlichkeit sowie die Zumutbarkeit untersucht.

1056 Siehe zu diesen Datenbearbeitungen Kapitel IV.5.3.

1057 So bedient sich z.B. der MID für den automatisierten Abgleich auf Mehrfachidentitäten der Komponenten ESP und BMS. Siehe dazu Kapitel IV.5.3.4.

1058 Siehe dazu Kapitel IV.4.

1059 Siehe dazu Kapitel V.3.4.

zelnen mit dem Grundrecht auf Datenschutz vereinbar sind, ist nicht Gegenstand der vorliegenden Untersuchung.[1060]

2. Schutzbereich und Eingriff

Aus den Erwägungsgründen der EU-IOP-VO geht explizit hervor, dass die Interoperabilität neue Datenbearbeitungsverfahren einführt und dass diese in die Grundrechte gemäss Art. 7 und 8 GRC eingreifen.[1061]

Dass die Interoperabilität in das Grundrecht auf Datenschutz eingreift, wird nachfolgend ausführlich dargelegt und bestätigt. Gefolgt wird dabei primär den in Art. 8 GRC sowie Art. 13 Abs. 2 BV statuierten Anforderungen für einen Eingriff. Demnach wird verlangt, dass der Grundrechtsadressat personenbezogene Daten von den Grundrechtsträgern bearbeitet.[1062]

2.1. Persönlicher Schutzbereich

Geschützt werden primär natürliche Personen.[1063] Von den bei der Interoperabilität vorgesehenen Datenbearbeitungen sind diejenigen Personen betroffen, deren Daten in den von der Interoperabilität umfassten Informationssystemen bearbeitet werden.[1064] Primär sind also Drittstaatsangehörige betroffen.[1065] Zum Teil werden aber auch Daten von anderen Personengrup-

---

1060 Siehe zu dieser Eingrenzung Kapitel I.2. Einzig im Zusammenhang mit Art. 22 EU-IOP-VO wird auf die gesetzlichen Grundlagen der Informationssysteme, welche einen solchen Zugang vorsehen, eingegangen, da dort der entsprechende Zugriff bisher geregelt ist. Die einzelnen Informationssysteme bergen für sich selbst betrachtet jeweils Risiken und Gefahren. So erscheint bspw. die bei Eurodac vorgesehene zehnjährige Speicherfrist für gewisse Daten aus datenschutzrechtlicher Perspektive nicht unbedenklich. Siehe dazu STÄMPFLI, 189; VAVOULA, EU immigration databases, 223. Siehe zur Entstehung der Systeme SIS, Eurodac, VIS, EES und ETIAS mit kritischer Würdigung ausserdem VAVOULA, EU immigration databases.

1061 ErwG. 40 EU-IOP-VO.

1062 Bei Art. 8 EMRK grenzt der EGMR den Schutzbereich nicht immer klar vom Eingriff ab. Zudem nimmt der EGMR stets eine Einzelfallbeurteilung vor. Es sind deshalb keine allgemeingültigen Kriterien vorhanden, wann der Schutzbereich eröffnet ist resp. wann ein Eingriff vorliegt. Siehe dazu Kapitel II.4.3.

1063 Siehe dazu Kapitel II.7.1.

1064 Siehe dazu auch ErwG. 12 EU-IOP-VO.

1065 Der Begriff «*Drittstaatsangehörige*» wird in den EU-IOP-VO nicht definiert. Das SIS sowie das EES sehen jedoch eine entsprechende Definition vor. Gemäss dieser sind unter dem Begriff Personen zu verstehen, welche keine UnionsbürgerInnen sind. Ausgenommen davon sind jedoch Personen, welche von einem Abkommen profitieren, welches ihnen ein

pen, wie z.B. UnionsbürgerInnen oder Schweizer Staatsangehörigen, bearbeitet.[1066] *In casu* sind demnach stets natürliche Personen von den Datenbearbeitungen betroffen.[1067] Der persönliche Schutzbereich ist somit eröffnet.

2.2. Sachlicher Schutzbereich

Der sachliche Schutzbereich des Grundrechts auf Datenschutz ist betroffen, wenn personenbezogene Daten bearbeitet werden.[1068]

2.2.1. Personenbezogene Daten

Als personenbezogene Daten gelten alle Daten, welche sich auf eine bestimmte oder zumindest bestimmbare Person beziehen.[1069]

Im Zusammenhang mit der Interoperabilität werden verschiedene personenbezogene Daten – sowohl alphanumerische als auch biometrische Daten – bearbeitet. Bei den alphanumerischen Daten handelt es sich insbesondere um verschiedene Angaben zur Person resp. zu deren Reisedokument(en). Unter die biometrischen Daten fallen im Zusammenhang mit der Interoperabilität ausschliesslich Fingerabdruckdaten und Gesichtsbilder.[1070] Diese enthalten einzigartige Informationen einer bestimmten natürlichen Person, welche insbesondere dazu benutzt werden können, sie zu identifizieren.[1071] Aber auch die verwendeten alphanumerischen Daten beziehen sich jeweils auf eine bestimmte natürliche Person und erlauben (mitunter) deren Identifikation. Auf

gleichwertiges Recht auf Freizügigkeit gewährleistet (Art. 3 Ziff. 4 SIS-Grenze-VO; Art. 3 Abs. 1 Ziff. 6 EES-VO). Für die vorliegende Untersuchung bedarf es keiner abschliessenden Definition dieses Begriffs. Aufgrund des gewählten Fokus ist jedoch explizit festzuhalten, dass Staatsangehörige der Schweiz keine Drittstaatsangehörige darstellen.

1066 Siehe dazu Kapitel III.10.

1067 Unerheblich ist, dass die Mehrheit der betroffenen Personen nicht über die Staatsangehörigkeit eines Schengen/Dublin-Staates verfügt. Siehe zur GRC Kapitel II.6.2. Siehe zur EMRK VILLIGER, N 24, wonach es nicht erforderlich ist, dass die beschwerdeführende Person im eingeklagten EMRK-Staat wohnt noch über dessen Staatsangehörigkeit verfügt.

1068 Dies geht zumindest eindeutig bei Art. 8 GRC sowie Art. 13 Abs. 1 BV hervor. Art. 8 EMRK lassen sich keine solchen allgemeinen Aussagen entnehmen, da der Gerichtshof stets im Einzelfall urteilt. Siehe dazu Kapitel II.7.1.

1069 Siehe dazu Kapitel II.5.3 und II.6.3.

1070 Siehe dazu Art. 4 Ziff. 10 und Ziff. 11 EU-IOP-VO.

1071 Siehe bezüglich den Fingerabdrücken EuGH, Urteil v. 17.10.2013, *Schwarz*, ECLI:EU:C:2013:670, Rz. 27, wonach Fingerabdruckdaten personenbezogene Daten darstellen, «*da sie objektiv unverwechselbare Informationen über natürliche Personen enthalten und deren genaue Identifizierung ermöglichen*».

die Klassifizierung sämtlicher im Rahmen der Interoperabilität bearbeiteten Daten wird vorliegend verzichtet, da der Personenbezug zweifelsfrei vorliegt. Nachfolgend werden lediglich einige ausgewählte Daten im Einzelnen qualifiziert, da bei diesen teilweise die Meinung vertreten wird, dass es sich nicht um personenbezogene Daten handelt.

2.2.1.1 *Templates*

Die Erstellung von Templates ist notwendig, damit biometrische Abfragen vorgenommen werden können. Diese Templates werden auf der Grundlage der Original-Daten erstellt, enthalten aber weniger Informationswert als die Originale.[1072] Zur Frage, ob diese Templates personenbezogene Daten darstellen, werden unterschiedliche Ansichten vertreten.[1073] Dieser Frage kommt insofern Bedeutung zu, als nur personenbezogene Daten vom Grundrecht auf Datenschutz geschützt werden.[1074]

Die WP29 vertritt z.B. die Ansicht, dass die Templates zwar weniger personenbezogene Informationen als die biometrischen Daten im Original enthielten und zudem in kodierter Form bestünden. Dennoch könne damit eine Identifizierung in einem automatisierten Verfahren vorgenommen werden. Die Einzigartigkeit der biometrischen Daten liege in deren Fähigkeit als universeller Identifikator, womit Informationen aus verschiedenen Informationsquellen zur gleichen Person verlinkt werden könnten. Dies sei genau die beabsichtigte Verwendung des BMS, weshalb die biometrischen Templates als biometrische Daten zu werten seien.[1075]

Im Gegenteil dazu wird in der Schweiz davon ausgegangen, dass es sich bei den Templates nicht um personenbezogene Daten handelt.[1076]

1072 Siehe zu den biometrischen Templates Kapitel IV.5.3.2.

1073 Siehe dazu SFH, Vernehmlassungsantwort, 8 m.w.H. Grundsätzlich können personenbezogene Daten anonymisiert werden. Dadurch entfällt der Personenbezug. Kann die Anonymisierung nur mit einem unverhältnismässig grossen Aufwand rückgängig gemacht werden, fallen solche Daten aus dem Schutzbereich des Grundrechts. Siehe dazu BLONSKI, 50 ff. Siehe zur Anonymisierung sowie zur Abgrenzung zur Pseudonymisierung auch PROBST, 13 ff.

1074 Siehe dazu Kapitel II.7.1.

1075 WP29, Opinion proposals IOP, 8. Vgl. im Zusammenhang mit der Datenschutzrichtlinie auch WP29, Biometrics, 5. Der EDSB spricht im Zusammenhang mit den vom BMS gespeicherten Daten von «*biometrischen Templates*». Diese Bezeichnung lässt ebenfalls darauf schliessen, dass darunter biometrische Daten zu verstehen sind. Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 77 f.

1076 Siehe dazu BUNDESRAT, Botschaft IOP, 8022.

Würden die Templates keine personenbezogenen Daten darstellen, hätte dies zur Konsequenz, dass der grundrechtliche Datenschutz bei der Bearbeitung dieser Daten nicht greifen würde. Bei den Original-Daten, aus welchen die Templates erstellt werden, hingegen schon. Es stellt sich die Frage, ob es für die betroffenen Personen von Bedeutung ist, ob auch die Templates personenbezogene Daten darstellen.

Die automatisch generierten Templates könnten – bspw. aufgrund technischer Mängel – fehlerhaft sein. Dies wiederum könnte im Rahmen der biometrischen Abgleiche zu falschen Ergebnissen führen. Eine dadurch verursachte falsche Identifizierung könnte für die betroffene Person schwerwiegende negative Konsequenzen haben (so könnte z.B. im Anwendungsbereich von Art. 22 EU-IOP-VO eine Person fälschlicherweise mit einer terroristischen oder sonstigen schweren Straftat in Verbindung gebracht werden). Gelten Templates nicht als personenbezogene Daten, kann kein Auskunftsrecht – und in der Folge auch kein Recht auf Berichtigung oder Löschung – geltend gemacht werden. Insofern kommt der Klassifizierung der Templates als (keine) personenbezogene Daten doch eine gewisse Relevanz zu.

Die im BMS gespeicherten Templates sind zwar so ausgestaltet, dass eine Rückführung in die ursprüngliche biometrische Datei ausgeschlossen ist.[1077] Dennoch bleiben sie – wie auch die Original-Daten – einzigartig. Wie bereits die WP29 aufführte, enthalten die Templates nicht so viele Informationen wie die Originale. Die besondere Funktion der biometrischen Daten, nämlich die zuverlässige Identifikation von Personen, bleibt jedoch erhalten. Die Templates stammen von biometrischen Daten einer bestimmten Person und werden eigens zum Zweck erstellt, deren Identifizierung zu ermöglichen. Insofern erscheint es – gemäss der hier vertretenen Ansicht – angezeigt, die im BMS gespeicherten Templates als personenbezogene Daten zu qualifizieren.[1078]

2.2.1.2 *Einmalige Kennnummer der Identitätsbestätigungsdatei*

Im MID werden Identitätsbestätigungsdateien gespeichert, welche u.a. auch eine einmalige Kennnummer umfassen, die das Abrufen der verknüpften Daten aus den entsprechenden Informationssystemen erlaubt.[1079] Bezüglich die-

1077 EU-LISA, Feasibility Study sBMS, 20.
1078 Siehe dazu zustimmend Vavoula, Deathblow, 141.
1079 Siehe für die Einzelheiten Art. 34 EU-IOP-VO.

sen im MID enthaltenen Daten wird die Ansicht vertreten, dass es sich dabei nicht um personenbezogene Daten handelt.[1080]

Aus der Definition der personenbezogenen Daten geht hervor, dass sich diese auch auf eine bestimmbare Person beziehen können. Bestimmbar ist eine Person, wenn diese direkt oder indirekt identifiziert werden kann.[1081] Eine Identifizierung kann u.a. mittels einer Kennnummer erfolgen. So werden z.B. das Autokennzeichen[1082], die IP-Adresse[1083] sowie auch die Telefonnummer als personenbezogene Daten angesehen.[1084]

Die im MID gespeicherte Identitätsbestätigungsdatei enthält zwar keine Informationen betreffend die Identität einer Person, deren Reisedokumente oder deren biometrische Daten. Jedoch dient insbesondere die in der Identitätsbestätigungsdatei gespeicherte einmalige Kennnummer dazu, Verknüpfungen herzustellen und dem zugriffsberechtigten Nutzer die von der Verknüpfung betroffenen Datensets von bestimmten Personen preiszugeben. Anhand dieser Referenz können die entsprechenden Personen identifiziert werden. Es handelt sich demnach also um eine Kennnummer, welche die Identifizierung einer Person ermöglicht. Folglich muss es sich zumindest bei dieser im MID gespeicherten Angabe um personenbezogene Daten handeln.

2.2.2. Datenbearbeitungen

Für die Eröffnung des sachlichen Schutzbereichs wird des Weiteren verlangt, dass die personenbezogenen Daten bearbeitet werden.[1085] Wie vorstehend in Kapitel IV ausführlich dargelegt, sind im Rahmen der Interoperabilität verschiedene Datenbearbeitungen vorgesehen.[1086]

Im Zusammenhang mit der Interoperabilität werden also verschiedene Bearbeitungen von personenbezogenen Daten vorgenommen. Der sachliche Schutzbereich ist somit eröffnet.

1080 Siehe dazu VAVOULA, Deathblow, 140.

1081 Siehe dazu Kapitel II.6.3.

1082 Vgl. dazu FRA/EUROPARAT/EDSB, Handbuch, 107 f.

1083 Siehe dazu z.B. BGE 136 II 508, E. 3.1; EuGH, Urteil v. 19.10.2016, *Patrick Breyer gegen Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, Rz. 49.

1084 Siehe dazu EDPS, necessity, 10. Vgl. dazu auch die Definition der personenbezogenen Daten in Art. 4 Ziff. 1 DSGVO.

1085 Siehe dazu Kapitel II.7.1.

1086 Siehe dazu insbesondere Kapitel IV.5.3.

2.3. Eingriff

2.3.1. Vorliegen eines Eingriffs

Ein Eingriff in den Schutzbereich des Grundrechts auf Datenschutz liegt vor, wenn die jeweiligen Grundrechtsadressaten eine Bearbeitung personenbezogener Daten vornehmen. Die Grundrechtsadressaten der BV und der EMRK sind die staatlichen Behörden. Bei der GRC sind es hingegen die Stellen der EU resp. die Mitgliedstaaten, sofern EU-Recht betroffen ist.[1087] Dass die EU-IOP-VO EU-Recht darstellen, geht aus diesen Verordnungen selbst hervor.[1088] Ebenso wurde bereits erläutert, dass die EU-Grundrechte nach dem Verständnis des EuGH nicht nur bei der Vollziehung von Verordnungen anwendbar sind, sondern auch bei einem allfällig gewährten Handlungsspielraum, sofern keine Verpflichtung zu einem bestimmten Tun vorgesehen ist.[1089] Die EU-Grundrechte sind also bezüglich den EU-IOP-VO zu beachten, wobei dies auch allfällig gewährte Handlungsspielräume einschliesst.[1090]

Bei der Interoperabilität sind verschiedene Akteure berechtigt, Datenbearbeitungen vorzunehmen. So z.B. verschiedene nationale Behörden der Schengen/Dublin-Staaten, welche u.a. die Daten im CIR eingeben, Abfragen im ESP vornehmen oder manuelle Verifizierungen durchführen. Zudem überwachen nationale Kontrollstellen die im Rahmen der Interoperabilität vorgenommenen Datenbearbeitungen.[1091]

Abgesehen von den nationalen Behörden nehmen auch verschiedene EU-Stellen, insbesondere die IT-Agentur eu-LISA, Datenbearbeitungen vor. Diese ist u.a. in der Umsetzung, im Betrieb aber auch im Monitoring der Datenbearbeitungen aktiv. Bestimmte Datenbearbeitung werden von weiteren Stellen der EU, wie z.B. Europol, vorgenommen.[1092]

Dementsprechend werden die mit der Interoperabilität vorgenommenen Datenbearbeitungen von den Grundrechtsadressaten der BV, der EMRK sowie

---

1087 Siehe dazu Kapitel II.4.2 und II.5.2.

1088 Siehe dazu die vollständige Bezeichnung der beiden Verordnungen.

1089 Siehe dazu Kapitel II.6.2.

1090 Ein solcher Handlungsspielraum gewähren die EU-IOP-VO z.B. bei Art. 20 EU-IOP-VO. Siehe dazu Kapitel IV.5.3.3.1 sowie V.3.4.4.

1091 Siehe dazu die Ausführungen zu den Interoperabilitätskomponenten sowie zu den ausgewählten Sicherheitsmassnahmen in Kapitel IV.5.3 und IV.5.4.

1092 Siehe dazu z.B. in Kapitel IV.5.3 (betreffend eu-LISA) sowie IV.5.3.3.3 (betreffend Europol).

der GRC vorgenommen. Die Interoperabilität stellt folglich einen Eingriff in das Grundrecht auf Datenschutz dar.[1093]

2.3.2. Schwere des Eingriffs

Grundsätzlich wird die Schwere von Eingriffen anhand verschiedener Kriterien im Einzelfall beurteilt, wobei im Bereich des Datenschutzes insbesondere die Art der bearbeiteten Daten eine entscheidende Rolle spielen kann.[1094]

In allgemeiner Weise ist festzuhalten, dass bei der Interoperabilität alphanumerische (gewisse Personalien sowie ggf. Angaben zum Reisedokument) sowie auch biometrische Daten bearbeitet werden. Letztere sind von besonderer Natur, da sie bei jeder Person einzigartig sind. Im Vergleich mit alphanumerischen Daten stellt die Bearbeitung von biometrischen Daten einen schwereren Eingriff dar, weshalb höhere Anforderungen an den Datenschutz zu stellen sind.[1095]

Die im Rahmen der Interoperabilität bearbeiteten Daten stammen von einem umfassenden Personenkreis. Die Anwendungsbereiche der von der Interoperabilität betroffenen Informationssysteme sind nämlich so ausgelegt, dass sie insbesondere die Daten von allen Drittstaatsangehörigen erfassen, welche in den Schengen-Raum einreisen (möchten).[1096] Aus der Rechtsprechung des

---

1093 Vgl. dazu auch FRA, Opinion IOP, 8; ErwG. 40 EU-IOP-VO.

1094 Siehe dazu Kapitel II.4.5; II.5.5 und II.6.5. Die Schwere eines Eingriffs wird von den Gerichten an unterschiedlicher Stelle geprüft, so z.B. bei der gesetzlichen Grundlage. Siehe dazu BGE 122 I 360, E. 5b. Auch wird die Schwere eines Eingriffs u.a. im Vorfeld zu den Ausführungen einer Rechtfertigung eines Eingriffs erörtert. Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 37. Dies rührt daher, dass die Schwere bei verschiedenen Kriterien der Rechtfertigung eine Rolle spielt. Vorliegend wird die Schwere des Eingriffs direkt nach der Prüfung, ob ein Eingriff vorliegt, thematisiert. Die Rechtsprechung zeigt, dass die Beurteilung der Intensität eines Eingriffs bei ähnlichen Sachverhalten von verschiedenen Gerichten sehr unterschiedlich bewertet werden kann. Siehe zur Rechtsprechung des EuGH, dem BGer sowie dem EGMR im Bereich der Vorratsdatenspeicherung MATTER, 257 ff. Ein anderes Beispiel stellt die Bearbeitung von DNA-Profilen dar. Das BGer sieht darin einen leichten Eingriff. Siehe dazu z.B. in BGE 128 II 259, E. 3.3. Obwohl die Lehre diese Rechtsprechung von Anfang an kritisierte, hielt das BGer seither daran fest. Siehe dazu BGE 147 I 372, E. 2. Der EGMR geht dabei hingegen von einem schweren Eingriff aus. Siehe dazu EGMR, Urteil v. 04.12.2008, S. *and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 72 ff.

1095 EDPS, Opinion EES, N 16. Vgl. dazu auch Art. 5 lit. c Ziff. 4 DSG und Art. 9 DSGVO.

1096 So werden in Eurodac asylsuchende Personen erfasst. Im VIS die visumpflichtigen und in ETIAS die visumbefreiten Drittstaatsangehörigen. Die Ein- und Ausreisen dieser Personen werden zudem im EES erfasst. Dazu kann eine Ausschreibung im SIS kommen oder bei

BGer geht zwar hervor, dass der individuelle Grundrechtseingriff grundsätzlich nicht schwerer wiegt, bloss weil eine grosse Anzahl von Personen betroffen ist.[1097] In der Rechtsprechung des EuGH zeigt sich jedoch, dass dieser Aspekt durchaus in die Bewertung der Schwere eines Eingriffs miteinfliessen kann.[1098] Des Weiteren ist zu berücksichtigen, dass gewisse Datenbearbeitungen systematisch und automatisiert erfolgen (beispielsweise die vom MID vorgenommene Prüfung auf Mehrfachidentitäten).[1099]

Regelmässig wird in der Rechtsprechung von einem schweren Eingriff ausgegangen, wenn anhand der durch die Datenbearbeitungen gewonnenen Daten von einer Person ein Profil erstellt werden kann.[1100] Es stellt sich demnach die Frage, ob die Interoperabilität die Profilbildung begünstigt. In die Datenbearbeitung bei der Interoperabilität sind grundsätzlich verschiedene Stellen involviert. Diese haben jeweils gemäss ihren Funktionen Zugang zu den Daten. Je nach dem über welche Zugriffsrechte der Endnutzer verfügt, kann dieser – bei einem Treffer – verschiedene Arten von Daten einsehen und daraus Rückschlüsse auf das Privatleben der betroffenen Person ziehen. So kann ein Endnutzer z.B. an Informationen zur Reisetätigkeit im Schengen-Raum oder allfälligen strafrechtlichen Verurteilungen der betroffenen Person in Mitgliedstaaten gelangen. Ob sich daraus ein Profil der betroffenen Person erstellen lässt, dürfte wohl einerseits davon abhängen, wie häufig die Daten dieser Person in den EU-Informationssystemen erfasst sind sowie andererseits vom Umfang der Zugriffsberechtigung des Endnutzers.

Bezogen auf eine konkrete Datenbearbeitung ist bspw. bezüglich der Abfrage des CIR gemäss Art. 20 EU-IOP-VO festzustellen, dass dadurch bereits erhobene Daten für einen weiteren Zweck bearbeitet werden dürfen. Dies hat zur Folge, dass der Anwendungsbereich der im Rahmen der EU-Informationssysteme erhobenen Daten erweitert wird. Primär erfolgt die Abfrage anhand von biometrischen Daten. Diese werden mit Daten abgeglichen, welche in verschiedenen Informationssystemen gespeichert sind. Nicht zuletzt auch unter

einer strafrechtlichen Verurteilung eine Erfassung im ECRIS-TCN. Siehe zu diesen Systemen Kapitel III.4; III.5; III.6; III.7; III.8 und III.9.

1097 Siehe dazu BGE 133 I 77, E. 5.3.

1098 Siehe dazu z.B. EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 97; EuGH, Urteil v. 21.06.2022, *Ligue des droits humains*, ECLI:EU:C:2022:491, Rz. 111.

1099 Siehe dazu Art. 27 EU-IOP-VO. Vgl. zur automatisierten Datenbearbeitung auch ErwG. 26 IOP-Polizei-VO.

1100 Siehe zu (schweren) Eingriffen aufgrund der Erstellung eines Profils EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 99; EuGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 128; EuGH, Urteil v. 21.06.2022, *Ligue des droits humains*, ECLI:EU:C:2022:491, Rz. 100. Siehe dazu z.B. auch BGE 143 I 253, E. 3.2.

Berücksichtigung des ursprünglichen Zwecks der erhobenen Daten dürfte mit Art. 20 EU-IOP-VO (zumindest bezüglich der Möglichkeit von Polizeibehörden, Identifizierungen auf dem Hoheitsgebiet der Schengen/Dublin-Staaten vorzunehmen) ein schwerer Eingriff verbunden sein.

Es zeigt sich somit, dass mit der Interoperabilität ein System von Datenbearbeitungen geschaffen wird, welches neue, systematische und teilweise automatisierte Bearbeitungen von Daten von allen Drittstaatsangehörigen vorsieht, welche einen Bezug zum Schengen-Raum aufweisen.[1101] Ohne näher auf jede einzelne Datenbearbeitung einzugehen, wird festgehalten, dass aufgrund der Natur der bearbeiteten Daten, des Umfangs des davon betroffenen Personenkreises sowie der Art der Datenbearbeitungen zumindest gewisse Datenbearbeitungen, welche im Zusammenhang mit der Interoperabilität vorgenommen werden, schwerwiegend in das Grundrecht auf Datenschutz eingreifen dürften.[1102]

3. Rechtfertigung des Eingriffs

Nachdem vorstehend ein Eingriff in das Grundrecht auf Datenschutz festgestellt wurde, wird nun die Rechtfertigung dieses Eingriffs untersucht. Geprüft werden die Kriterien der gesetzlichen Grundlage, des öffentlichen Interesses, des Kerngehalts sowie der Verhältnismässigkeit.[1103]

3.1. Gesetzliche Grundlage

Das Grundrecht auf Datenschutz verlangt, dass die gesetzliche Grundlage zugänglich und genügend bestimmt ist, so dass die Betroffenen die Konsequenzen des eigenen Verhaltens vorhersehen können.[1104]

Die gesetzliche Grundlage der Interoperabilität stellen primär die EU-IOP-VO dar. Darin finden sich verschiedene Bestimmungen zu den Interoperabili-

---

1101 Siehe aus der Rechtsprechung zu grossangelegten Datenbearbeitungen, welche systematisch und teilweise auch automatisiert vorgenommen werden, wobei ein relativ umfassender Personenkreis davon betroffen ist z.B. EuGH, Urteil v. 21.06.2022, *Ligue des droits humains*, ECLI:EU:C:2022:491, Rz. 111; EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 97. Vgl. dazu auch BGE 122 I 360, E. 5c-d.

1102 Siehe zu einem Überblick über verschiedene Beurteilungen des EuGH in Bezug auf die Schwere des Eingriffs EDPS, proportionality, 25 ff.

1103 Siehe dazu Kapitel V.1.

1104 Siehe dazu Kapitel II.7.3.

tätskomponenten sowie auch zu den Abfragen gemäss Art. 20-22 EU-IOP-VO. Diese beiden Verordnungen wurden im Amtsblatt der EU veröffentlicht und sind somit öffentlich zugänglich.[1105]

Fraglich erscheint, ob die EU-IOP-VO genügend bestimmt sind, so dass die Konsequenzen dieser Rechtsakte für die Betroffenen vorhersehbar sind. Die EU-IOP-VO sind mit ihren jeweils 80 resp. 84 Erwägungsgründen und 75 resp. 79 eher ausführlichen Bestimmungen für sich allein bereits umfassend. Hinzu kommt, dass der Kommission in den EU-IOP-VO an diversen Stellen Delegationsbefugnisse übertragen wurden. Auf dieser Grundlage hat die Kommission zahlreiche Durchführungsrechtsakte erlassen. Des Weiteren enthalten die EU-IOP-VO eine grosse Anzahl an Verweisen auf andere EU-Rechtsakte. Mitunter wird auf die gesetzlichen Grundlagen der EU-Informationssysteme verwiesen.[1106] Diese werden regelmässig revidiert, was es zusätzlich erschwert einen Überblick über die jeweils geltenden gesetzlichen Grundlagen zu wahren.[1107] Zudem wird auch vielfach auf die relevanten datenschutzrechtlichen Bestimmungen des EU-Sekundärrechts, welche im Rahmen der Datenbearbeitungen zu beachten sind, verwiesen.[1108] Davon abgesehen gewähren die EU-IOP-VO den Schengen/Dublin-Staaten zum Teil einen gewissen Gestaltungsspielraum, weshalb auch nationales Recht zu beachten ist.[1109] Die EU-IOP-VO und deren Verhältnis zu den gesetzlichen Grundlagen der einzelnen Systeme wurde deshalb auch als «*gesetzgeberischer Albtraum*» bezeichnet.[1110]

Um die Ausgestaltung der Interoperabilität im Einzelnen zu erfassen, sind also zahlreiche und umfassende gesetzliche Grundlagen zu konsultieren. Aufgrund

1105 Siehe dazu das Urteil *Leander*. Dort wurde die Zugänglichkeit bejaht, da die «*Ordinance*» publiziert worden war. Siehe dazu EGMR, Urteil v. 26.03.1987, *Leander vs. Sweden*, Beschwerde Nr. 9248/81, Rz. 53.

1106 So z.B. hinsichtlich der Speicherdauer (Art. 23 EU-IOP-VO), den Ausnahmen von dem grundsätzlichen Verbot des Weiterleitens an Dritte (Art. 50 EU-IOP-VO) sowie dem effektiven Zugang der nationalen Strafverfolgungsbehörden zu den Daten von Eurodac, VIS, EES und ETIAS (22 Abs. 3 EU-IOP-VO).

1107 Siehe dazu MOHLER, Herausforderung, 38 f.

1108 Siehe dazu z.B. Art. 47 Abs. 1 EU-IOP-VO. Problematisch ist, dass nicht immer eindeutig ist, welches Datenschutz-Regime einschlägig ist. Vgl. dazu BROUWER, A point of no return.

1109 Siehe dazu insbesondere Art. 20 EU-IOP-VO. Die genaue Ausgestaltung der beiden in dieser Bestimmung geregelten Abfragemöglichkeiten durch die Polizeibehörden ist grösstenteils durch nationales Recht festzulegen. Es ist mit einer unterschiedlichen Ausgestaltung dieser Abfragemöglichkeiten in den Schengen/Dublin-Staaten zu rechnen. Vgl. dazu BROUWER, A point of no return.

1110 GROENENDIJK. Siehe dazu auch BROUWER, Interoperability of Databases, wonach sich diese Komplexität auch negativ auf die Geltendmachung der Rechte der betroffenen Personen auswirken könne.

dieser sehr komplexen gesetzlichen Regelung ist ernsthaft in Frage zu stellen, ob es diese den Betroffenen im Sinne der Vorhersehbarkeit ermöglicht, ihr Verhalten danach zu richten. Selbst für erfahrene JuristInnen dürfte die Ausgestaltung der Interoperabilität nicht ganz einfach zu erfassen sein.[1111]

Die Komplexität der Interoperabilität ergibt sich u.a. durch den Einbezug verschiedener EU-Informationssysteme. Ausserdem sind vier Komponenten notwendig, um die Informationssysteme interoperabel zu machen. Deren Funktion, Zweck sowie auch das gegenseitige Verhältnis mussten geklärt werden. Da die Interoperabilität verschiedene Datenbearbeitungen vorsieht, mussten auch zahlreiche Aspekte dazu geregelt werden. So werden in den EU-IOP-VO u.a. die Speicherung der Daten[1112], der Zugang von Drittparteien[1113], die Verfahren zur Wahrung der Integrität und Vertraulichkeit der Daten[1114] sowie die Löschung[1115] der Daten geregelt. Wäre die gesetzliche Grundlage der Interoperabilität weniger umfassend ausgefallen, hätte die Gefahr bestanden, dass diese als zu wenig hinreichend bestimmt deklariert worden wäre.

Die Rechtsprechung zum Grundrecht auf Datenschutz verlangt ferner, dass klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Massnahme vorgesehen sind. Es müssen Mindestanforderungen festgelegt werden, so dass den von der Datenbearbeitung betroffenen Personen ausreichende Garantien zur Verfügung gestellt werden, welche einen wirksamen Schutz vor Missbrauch ermöglichen.[1116] Diese Anforderungen werden teilweise beim Kriterium der gesetzlichen Grundlage, teilweise aber auch erst bei der Prüfung der Verhältnismässigkeit untersucht. Der Rechtsprechung ist zu entnehmen, dass diese Kriterien insbesondere dann bei der gesetzlichen Grund-

1111 Vgl. dazu ein Urteil des BGer, in welchem das Gericht eine detaillierte Auflistung der zu speichernden Daten als nicht «*stufen- und sachgerecht*» einstufte, aufgrund der damit einhergehenden Komplexität. Eine solche Aufzählung wäre sehr technisch und für Laien wohl kaum verständlich. Siehe dazu BGer 1C_598/2016 vom 2. März 2018, E. 6.2.

1112 Siehe zur Speicherfrist der im BMS, CIR und MID gespeicherten Daten die Art. 15, 23 sowie 35 EU-IOP-VO. Im ESP werden keine Daten gespeichert.

1113 Die EU-IOP-VO statuieren ein grundsätzliches Verbot der Übermittlung von Daten an Drittstaaten, internationale Organisationen sowie private Stellen, wobei einige in anderen gesetzlichen Grundlagen vorgesehene Ausnahmen vorbehalten sind. Siehe dazu Art. 50 EU-IOP-VO.

1114 Siehe dazu z.B. die Art. 42-44 EU-IOP-VO, welche den Agenturen sowie den Schengen/Dublin-Staaten gewisse Pflichten hinsichtlich der Sicherheit der Daten auferlegen und auch ein Verfahren vorsehen im Falle eines Sicherheitsvorfalls. Ausserdem tragen die Schengen/Dublin-Staaten für die eigenen Behörden die Verantwortung.

1115 Die Vernichtung der Daten geht aus der Regelung zur Speicherdauer hervor. Die Löschung erfolgt jeweils automatisch. Siehe dazu die Art. 15, 23 und 35 EU-IOP-VO.

1116 Siehe dazu Kapitel II.7.3.

lage evaluiert werden, wenn keine Regeln zu gewissen Aspekten – z.B. dem Zweck oder der Löschung der Daten – vorhanden sind.[1117] Da solche Aspekte, wie soeben aufgezeigt, grundsätzlich in den EU-IOP-VO geregelt werden, werden diese Anforderungen in der vorliegenden Untersuchung im Rahmen der Verhältnismässigkeit abschliessend geprüft.[1118]

Aufgrund der vorstehenden Diskussion wird davon ausgegangen, dass die gesetzliche Grundlage zugänglich sowie auch grundsätzlich hinreichend bestimmt ist, auch wenn die Komplexität der gesetzlichen Regelung es den Betroffenen erschweren dürfte, ihr Verhalten danach auszurichten.[1119] Einzig die Regelung zur Abfrage des CIR gemäss Art. 20 EU-IOP-VO wirft ernsthafte Fragen bezüglich dem Erfordernis einer gesetzlichen Grundlage auf. Wie sich noch zeigen wird, ist die Abfragemöglichkeit nur sehr oberflächlich auf EU-Ebene geregelt. Die genauere Ausgestaltung dieser Abfrage wird vielmehr den Schengen/Dublin-Staaten überlassen. Insbesondere die fehlende Festlegung eines genauen Zwecks der Abfrage stellt in Frage, ob die gesetzliche Grundlage genügend bestimmt ist, sodass die Konsequenzen für die Betroffenen vorhersehbar sind.[1120] Da sich die Abfragemöglichkeit gemäss Art. 20 EU-IOP-VO im Folgenden (auch) in anderer Hinsicht als nicht gerechtfertigt erweisen wird, muss diese Frage vorliegend nicht abschliessend beurteilt werden.[1121]

1117 Siehe dazu *Rotaru*, wonach die rumänische Regelung als nicht genügend bewertet wurde, da keine ausreichende Beschränkung der Befugnisse vorgesehen war und nicht festgelegt wurde, welche Informationen überhaupt gespeichert werden dürfen resp. wem der Zugriff zu den Daten gestattet war. Ausserdem fehlten Zweckbestimmungen und Löschungsregeln. Siehe dazu EGMR, Urteil v. 04.05.2000, *Rotaru v. Romania*, Beschwerde Nr. 28341/95, Rz. 56 ff. Siehe dazu auch BGE 122 I 360, E. 5c-d, wo die gesetzliche Grundlage der Registrierung von Mitgliedern einer bestimmten Gruppe verneint wurde, da nicht klar geregelt war, unter welchen Voraussetzungen und zu welchem Zweck eine Registrierung vorgenommen werden darf, welcher Personenkreis erfasst werden darf, wer die Informationen erhalten darf sowie unter welchen Voraussetzungen eine Löschung möglich ist.

1118 Ebenso prüfte der EuGH diese Anforderungen bei der Verhältnismässigkeit in EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 54; EuGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 140 f.

1119 Die WP29 befand die beiden Vorschläge der EU-IOP-VO ohne Zweifel als ausreichende gesetzliche Grundlage. Geprüft wurden deshalb nur die Notwendigkeit und Verhältnismässigkeit der Vorschläge. Siehe dazu WP29, Opinion proposals IOP, 3.

1120 Siehe dazu FRA, Opinion IOP, 28.

1121 Art. 20 EU-IOP-VO wird sowohl beim Kerngehalt (siehe Kapitel V.3.3) als auch bei der Verhältnismässigkeit (siehe Kapitel V.3.4.4) diskutiert.

3.2. Öffentliches Interesse

Die Hintergründe der Entstehung der Interoperabilität zeigen auf, dass dieses Projekt auf der Grundlage eines Bedürfnisses nach Sicherheit entstanden ist. Aufgrund von verschiedenen Bedrohungen sollte die innere Sicherheit mit der Interoperabilität gestärkt werden.[1122]

Aus den Erwägungsgründen der EU-IOP-VO geht hervor, dass die mit der Interoperabilität neu eingeführten Datenbearbeitungsverfahren die korrekte Identifizierung der betroffenen Personen sicherstellen sollen. Diese sei notwendig, damit die von der Interoperabilität umfassten Informationssysteme wirksam genutzt werden können. Die Interoperabilität sei deshalb aufgrund der von den einzelnen Informationssystemen verfolgten Ziele gerechtfertigt. Dabei handelt es sich um das wirksame Management der Unionsgrenzen, die Wahrung der inneren Sicherheit der Union sowie die wirksame Umsetzung der Asyl- und der Visapolitik der Union.[1123]

Des Weiteren findet sich in Art. 2 EU-IOP-VO eine als «*Ziele*» genannte Bestimmung. Diese nennt in Abs. 1 sieben Ziele und in Abs. 2 sieben Massnahmen, mit welchen die in Abs. 1 genannten Ziele erreicht werden sollen. Der Begriff «*Ziel*» wird im Zusammenhang mit der Interoperabilität nicht einheitlich verwendet. Je nach Kontext wird darunter das öffentliche Interesse oder der Zweck der Datenbearbeitung verstanden.[1124] Mit den in Art. 2 Abs. 1 EU-IOP-VO aufgeführten Zielen dürften die öffentlichen Interessen gemeint sein. Diese dort genannten Aspekte lassen sich – zumindest mehrheitlich – unter die drei vorhin genannten Hauptinteressen subsumieren, mit welchen die Zielsetzung der einzelnen Informationssysteme beschrieben wurde.[1125]

1122 Siehe dazu Kapitel IV.3 und IV.4.

1123 ErwG. 40 EU-IOP-VO. Siehe dazu auch BUNDESRAT, Botschaft IOP, 7991, wonach die Interoperabilität das Ziel verfolgt, die Sicherheit im Schengen-Raum zu verstärken, schnellere und wirksamere Kontrollen an den Schengen-Aussengrenzen zu ermöglichen sowie einen Beitrag zur Bekämpfung der irregulären Migration zu leisten. Bereits in der Folgenabschätzung wurde die Verbesserung des Managements der Schengen-Aussengrenzen sowie die Leistung eines Beitrags zur inneren Sicherheit als allgemeine Zielsetzungen der Interoperabilität definiert. Siehe dazu EUROPEAN COMMISSION, Impact assessment IOP Part 1, 15.

1124 Vgl. dazu z.B. EDSB, Reflexionspapier IOP, N 12 ff.

1125 Dabei wird davon ausgegangen, dass sich das Ziel des Beitrags zur Verhinderung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten unter das öffentliche Interesse der inneren Sicherheit subsumieren lässt. Siehe dazu auch BGE 144 I 126, E. 7 (mit Hinweisen auf die Rechtsprechung des EGMR), wonach ein Beitrag zur Strafverfolgung der öffentlichen Sicherheit und Ordnung dient. Vgl. dazu auch EUGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 82. Der Beitrag zur Verhinderung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten dient dabei nicht

Insgesamt ergibt sich, dass mit der Interoperabilität verschiedene öffentliche Interessen verfolgt werden.[1126]

3.3. Kerngehalt

Der Kerngehalt des Grundrechts auf Datenschutz wurde bis anhin (noch) nicht klar definiert. Im Folgenden wird deshalb versucht, anhand der einschlägigen Hinweise, welche sich in der Rechtsprechung und der Lehre zum Kerngehalt finden, zu erörtern, ob der Kerngehalt durch die Interoperabilität tangiert sein könnte.[1127]

Der Rechtsprechung des EuGH ist zu entnehmen, dass im Urteil *Digital Rights* Bestimmungen zum Datenschutz und zur Datensicherheit von zentraler Bedeutung waren, dass *in casu* der Kerngehalt als nicht betroffen erachtet wurde.[1128] Insgesamt fordert die Rechtsprechung des EuGH ein gewisses Mass an Sicherheitsmassnahmen, damit die Daten effektiv geschützt werden können.[1129]

---

nur der öffentlichen Ordnung und Sicherheit, sondern schützt auch die Rechte und Freiheiten von Dritten. Siehe dazu BGE 144 I 126, E. 7 (jeweils mit Hinweisen auf die Rechtsprechung des EGMR). Vgl. dazu auch EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 41. Nur beim in Art. 2 Abs. 1 Bst. g EU-IOP-VO genannten Ziel («*Erleichterung der Identifizierung von unbekannten Personen, welche sich nicht ausweisen können, oder von nicht identifizierten sterblichen Überresten bei Naturkatastrophen, Unfällen oder terroristischen Anschlägen*») ist unklar, ob es sich dabei um ein eigenständiges öffentliches Interesse handeln soll. Aufgrund der Formulierung erscheint die Festlegung eines solches nicht eindeutig. Siehe zu dieser Problematik Kapitel V.3.4.4.

1126 Das öffentliche Interesse der Interoperabilität wurde in den Dokumenten der WP29, dem EDSB oder der FRA kaum diskutiert. Zum Teil wurde auch ohne nähere Ausführungen dazu davon ausgegangen, dass ein solches gegeben sei (ohne dieses genauer zu bestimmen). Siehe dazu z.B. WP29, Opinion proposals IOP, 3. Der EDSB führte lediglich aus, dass das allgemeine Ziel der beiden Vorschläge darin bestehe, das Grenzmanagement an den Schengen-Aussengrenzen zu verbessern und einen Beitrag zur inneren Sicherheit der Europäischen Union zu leisten. Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, Rz. 8. In der Folgenabschätzung wurde die Verbesserung des Managements der Schengen-Aussengrenzen sowie der Beitrag zur inneren Sicherheit der EU als allgemeine Zielsetzungen definiert. Abgesehen davon wurden auch spezifische Ziele definiert. Siehe dazu European Commission, Impact assessment IOP Part 1, 15 f.

1127 Siehe zum Kerngehalt Kapitel II.5.6.4; II.6.6.2 sowie II.7.3.

1128 Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 40. Vgl. dazu auch EuGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 150.

1129 Siehe dazu Kapitel II.6.6.2.

In den EU-IOP-VO wird dem Datenschutz ein ganzes Kapitel gewidmet. Dort werden u.a. verschiedene Verantwortlichkeiten, die Rechte der betroffenen Personen sowie die Aufsicht geregelt. Abgesehen von diesen allgemeinen Sicherheitsmassnahmen werden auch für die in den Interoperabilitätskomponenten vorgenommenen Datenbearbeitungen weitere Sicherheitsmassnahmen vorgesehen. So z.B. die Protokollierungspflicht der Datenbearbeitungen.[1130] Es ist also davon auszugehen, dass die von der Rechtsprechung des EuGH geforderten minimalen Sicherheitsmassnahmen vorliegen.

Davon abgesehen ist es den abfragenden Behörden möglich, im Rahmen ihrer Zugriffsrechte an gewisse Informationen zu gelangen. Auch wenn sich durch diese Informationen ein mehr oder weniger umfangreiches Bild von einer Person ergeben kann, so beschränken sich diese Angaben auf die Personalien einer Person, deren Reisetätigkeit im Schengen-Raum sowie auf ein allfälliges kriminelles Verhalten. Die Informationen beschränken sich somit auf gewisse Aspekte des Privatlebens der betroffenen Person.[1131] Da im *Gutachten 1/15* die Informationen, in welche eingesehen werden konnte, ebenfalls nur einen bestimmten Teil des Privatlebens betrafen, wurde von keinem Eingriff in den Kerngehalt ausgegangen.[1132]

Im selben Gutachten wurde bei der Verneinung einer Verletzung des Kerngehalts zudem ausgeführt, dass die Zwecke der Datenbearbeitungen begrenzt wurden.[1133] Der Lehre ist zu entnehmen, dass das im Sekundärrecht verankerte Prinzip der Zweckbestimmung zum Kerngehalt gehören soll.[1134] In den EU-IOP-VO wird insbesondere für die einzelnen Interoperabilitätskomponenten jeweils ein Zweck definiert.[1135] Hinsichtlich dem mit dem CIR verfolgten Zweck, welcher mit den beiden Abfragemöglichkeiten gemäss Art. 20 EU-IOP-VO erreicht werden soll, fällt jedoch auf, dass dieser sehr vage gehalten ist. Bezweckt wird die Erleichterung und Unterstützung der korrekten Identifizierung von im EES, im VIS, im ETIAS, in Eurodac und im ECRIS-TCN erfassten Personen. In Art. 20 Abs. 5 EU-IOP-VO werden die Schengen/Dublin-Staaten zudem bezüglich der Abfragemöglichkeit, welche im Rahmen von Polizeikontrollen durchgeführt werden darf, explizit aufgefordert die «*genauen Zwecke*» im na-

1130 Die verschiedenen Sicherheitsmassnahmen werden ausführlich bei der Beurteilung der Verhältnismässigkeit besprochen. Siehe dazu Kapitel V.3.4.

1131 Siehe dazu auch EuGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 150.

1132 Siehe dazu Kapitel II.6.6.2.

1133 EuGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 150.

1134 Siehe dazu Kapitel II.6.6.2.

1135 Siehe zum ESP Art. 6 Abs. 1 EU-IOP-VO; zum BMS Art. 12 Abs. 1 EU-IOP-VO; zum CIR Art. 17 Abs. 1 EU-IOP-VO sowie zum MID Art. 25 Abs. 1 EU-IOP-VO.

tionalen Recht näher festzulegen. Immerhin wird festgelegt, dass die Identifizierungen für die Verhinderung sowie Bekämpfung illegaler Einwanderung resp. der Gewährleistung eines hohen Masses an Sicherheit zu erfolgen haben.

Bereits in seiner Stellungnahme zu den Vorschlägen der EU-IOP-VO hat der EDSB ausgeführt, dass es sich bei der Identifizierung einer Person nicht um einen Selbstzweck handeln dürfe. Es müsse stets ein konkretes Ziel mit der Identifizierung verfolgt werden, also z.B. um zu ermitteln, ob eine Person polizeilich gesucht werde oder sich rechtmässig in der EU aufhalte.[1136] Indem der EU-Gesetzgeber lediglich auf die übergeordneten Begriffe verweist, im Rahmen welcher die Abfragen zu erfolgen haben, kann diesem Erfordernis nicht entsprochen werden. Denn diese Begriffe sind derart weit gefasst, dass sich letztlich ein ziemlich umfassendes Spektrum der Polizeitätigkeit darunter subsumieren lässt.[1137] Insofern wird dadurch keine Begrenzung vorgenommen. Das «*konkrete Ziel*» der Abfrage kann dadurch nicht eruiert werden. Dazu hätte im EU-Recht eingehender festgelegt werden müssen, welche konkreten Zwecke die Abfragen verfolgen müssen.

Bezüglich der anderen Abfragemöglichkeit gemäss Art. 20 EU-IOP-VO ist der Zweck der Identifizierung ebenso unklar. Die Abfragemöglichkeit sieht die Identifizierung von unbekannten Personen, welche sich nicht ausweisen können, resp. von menschlichen Überresten im Zusammenhang mit Unfällen, Naturkatastrophen sowie Terroranschlägen vor. Aufgrund der Formulierung sowie unter Berücksichtigung der aufgeführten Ereignisse könnte mit dieser Abfragemöglichkeit die Identifizierung von Opfern beabsichtigt sein. Klar geht dies jedoch nicht aus dem EU-Recht hervor. Anders als bei der Abfragemöglichkeit, welche im Rahmen von Polizeikontrollen vorgenommen werden darf, ist zudem weder festgelegt, dass die «*genaueren Zwecke*» im nationalen Recht zu definieren sind, noch wird versucht diese Identifizierung anhand von übergeordneten Zielen zu begrenzen.

Da der EU-Gesetzgeber es unterlassen hat, die genauen Zwecke dieser beiden Abfragemöglichkeiten festzulegen, stellt sich die Frage, ob dadurch der Kerngehalt als verletzt angesehen werden könnte. Dies könnte durchaus diskutiert werden. Da sich diese beiden Abfragemöglichkeiten gemäss Art. 20 EU-IOP-

1136 Vgl. dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 39.

1137 So hatte auch schon die FRA zu den Vorschlägen der EU-IOP-VO bemerkt, dass damit jegliche Abfragen ermöglicht werden, welche ein sicherheitsbezogenes Ziel verfolgen. Siehe dazu FRA, Opinion IOP, 27.

VO nachfolgend jedoch als unverhältnismässig erweisen werden, wird vorliegend auf eine abschliessende Diskussion zum Kerngehalt verzichtet.[1138]

Abgesehen davon wurde zum Kerngehalt der informationellen Selbstbestimmung in der Lehre dargelegt, dass dieser betroffen sein könnte, wenn die betroffenen Personen durch die Datenbearbeitung «*gläsern*» erscheinen würden. Da sich das Bild, welches sich den abfragenden Behörden zu einer Person im Rahmen der Interoperabilität ergeben kann, lediglich auf bestimmte Aspekte des Privatlebens beschränkt, erscheint dies *in casu* nicht zutreffend zu sein. Des Weiteren wurde in der Lehre die These aufgestellt, dass der Kern betroffen sein könnte, wenn der Zugang zu den eigenen Daten gänzlich verwehrt würde. Aufgrund der den betroffenen Personen bei der Interoperabilität zugestandenen Rechte, ist dies ebenfalls nicht einschlägig.[1139] In der Lehre wird ebenfalls ausgeführt, dass eine Verletzung der Menschenwürde den Kerngehalt betreffen könnte. Inwiefern durch die Interoperabilität die Menschenwürde beeinträchtigt werden könnte, ist jedoch nicht ersichtlich.[1140]

Unter Berücksichtigung der Rechtsprechung des EuGH sowie den in der Lehre vertretenen Ansichten zum Kerngehalt sind keine Hinweise ersichtlich, welche darauf schliessen lassen, dass mit der Interoperabilität in den Kerngehalt eingegriffen wird. Auf eine abschliessende Diskussion bezüglich der beiden Abfragemöglichkeiten gemäss Art. 20 EU-IOP-VO wurde explizit verzichtet.

3.4. Verhältnismässigkeit

Bei der Prüfung der Verhältnismässigkeit werden die einander gegenüberstehenden Interessen gegeneinander abgewogen, wobei im Einzelfall jeweils verschiedene Aspekte berücksichtigt werden.[1141]

Vorliegend stehen auf der einen Seite die mit der Interoperabilität verfolgten öffentlichen Interessen, wobei insbesondere das Interesse an der Wahrung der inneren Sicherheit im Vordergrund steht.[1142] Auf der anderen Seite stehen die

1138 Siehe dazu die Ausführungen in Kapitel V.3.4.4.

1139 Siehe dazu insbesondere Art. 47 EU-IOP-VO (Recht auf Information) sowie Art. 48 EU-IOP-VO (Recht auf Auskunft, Berichtigung und Löschung betreffend MID-Daten). Der Zugang zu den Daten ist also gewährleistet. Siehe dazu insbesondere Kapitel V.3.4.8.1.b).

1140 Siehe zu den Ausführungen zum Kerngehalt bei der informationellen Selbstbestimmung Kapitel II.5.6.4.

1141 Siehe dazu Kapitel II.7.3.

1142 Siehe zum öffentlichen Interesse der Interoperabilität Kapitel V.3.2. Vgl. dazu auch die Entstehungsgeschichte der Interoperabilität in Kapitel IV.3 und IV.4.

Interessen der Betroffenen am Schutz ihrer im Rahmen der Interoperabilität bearbeiteten Daten.

Die Wahrung der öffentlichen Ordnung und Sicherheit stellt gemäss der Rechtsprechung zwar ein erhebliches Interesse dar. Dennoch vermag auch dieses öffentliche Interesse nicht jeglichen Eingriff in die Grundrechte zu rechtfertigen.[1143]

Mit dem Schutz der Daten soll insbesondere ein selbstbestimmtes Entscheiden resp. Handeln der Personen gewährleistet werden, indem sie Kenntnis darüber haben oder zumindest abschätzen können, wer welche Daten über die eigene Person in Erfahrung bringen kann. Insofern soll damit der Privatsphären- resp. der Persönlichkeitsschutz sichergestellt werden.[1144] Insbesondere weil bei der Interoperabilität bestimmte alphanumerische und auch biometrische Daten systematisch und teilweise automatisiert bearbeitet werden und sich – durch die missbräuchliche resp. falsche Bearbeitung von Daten – allfällige negative Konsequenzen für die betroffenen Personen ergeben können, ist das Interesse der betroffenen Personen am Schutz ihrer Daten (ebenfalls) grundsätzlich hoch zu gewichten.

Die Festlegung des gerichtlichen Massstabs bestimmt zudem, wie streng die Verhältnismässigkeit der Massnahme überprüft wird resp. wie viel Gestaltungsspielraum dem Grundrechtsadressat zugestanden wird. Dabei werden u.a. der betroffene Bereich, die Art des betroffenen Grundrechts, die Art und Schwere des Eingriffs sowie das Ziel desselben berücksichtigt.[1145] Vorliegend ist in Anbetracht der systematischen und teilweise automatisierten Bearbeitung der Daten aller Drittstaatsangehöriger, welche einen Bezug zum Schengen-Raum haben sowie der Schwere des mit der Interoperabilität verbundenen Eingriffs in das Grundrecht auf Datenschutz – trotz der damit verfolgten erheblichen öffentlichen Interessen – eine strikte Kontrolle der Verhältnismässigkeit vorzunehmen.

Für die Beurteilung der Verhältnismässigkeit der Interoperabilität wird insbesondere auf die vier Interoperabilitätskomponenten sowie die drei Abfragen des CIR einzeln eingegangen. Da bei diesen Komponenten resp. den Abfragen jeweils unterschiedliche (und teilweise sehr umfassende) Datenbearbeitungen

1143 Siehe dazu BGE 144 I 126, E. 8.3.1 mit Hinweisen auf die einschlägige Rechtsprechung des EGMR.

1144 Siehe dazu Kapitel II.2.

1145 Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 47. Vgl. dazu auch EGMR, Urteil v. 04.12.2008, *S. and Marper v. The United Kingdom*, Beschwerde Nr. 30562/04 und 30566/04, Rz. 102.

vorgenommen werden, werden dort die drei Subkategorien der Verhältnismässigkeit, wie sie von der Rechtsprechung der BGer herausgearbeitet wurden, explizit untersucht. Es handelt sich dabei um die Kriterien der Geeignetheit, der Erforderlichkeit sowie der Zumutbarkeit.[1146] Die Prüfung dieser Kriterien soll es erlauben für die Interoperabilitätskomponenten sowie die Abfragen jeweils festzustellen, ob diese verhältnismässig sind. Im Anschluss werden noch ausgewählte Sicherheitsmassnahmen, welche bei sämtlichen im Zusammenhang mit der Interoperabilität vorgenommenen Datenbearbeitungen Geltung beanspruchen, diskutiert, bevor eine Bewertung der Verhältnismässigkeit der Interoperabilität vorgenommen wird.

3.4.1. Europäisches Suchportal

3.4.1.1 *Geeignetheit*

Das ESP soll den zugriffsberechtigten Stellen einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang u.a. zu den EU-Informationssystemen zur Wahrnehmung ihrer Aufgaben im Einklang mit den Zielen und Zwecken des EES, VIS, ETIAS, ECRIS-TCN, SIS sowie von Eurodac erleichtern.[1147]

Durch den mit dem ESP verfolgten Zweck kann den Zielen der betroffenen Systeme besser entsprochen werden. Mit diesen Systemen werden insbesondere das wirksame Management der Schengen-Aussengrenzen, die Wahrung der inneren Sicherheit sowie die wirksame Umsetzung der Asyl- und Visapolitik verfolgt.[1148] Das ESP ist also geeignet, zur Verfolgung von verschiedenen öffentlichen Interessen beizutragen.[1149]

3.4.1.2 *Erforderlichkeit*

Der Folgenabschätzung ist zu entnehmen, dass die mit der Einführung von neuen Systemen steigende Zahl der Zentralsysteme zu einer Belastung für die beteiligten Staaten führe. Mit dem ESP könne ermöglicht werden, dass die Zentralsysteme nicht mehr jeweils über eine eigene, sondern über eine gemeinsame Schnittstelle abgerufen werden können. Dadurch wären weniger

1146 Siehe zu diesen Kriterien Kapitel II.5.6.3.

1147 Art. 6 Abs. 1 EU-IOP-VO. In der Machbarkeitsstudie zum ESP wurden verschiedene Varianten geprüft. Siehe dazu EUROPEAN COMMISSION, Impact assessment IOP Part 2, 18 ff.

1148 Siehe dazu ErwG. 40 EU-IOP-VO.

1149 Siehe zum öffentlichen Interesse der Interoperabilität Kapitel V.3.2.

Verbindungen zwischen den Systemen nötig. Im Sinne der Datensicherheit sei dadurch nur ein Kontrollpunkt zu überprüfen.[1150] Die Gefahr einer Datenpanne oder von Datenverlust wurde mit der Funktion des ESP geringer eingeschätzt als ohne.[1151] Ebenfalls wurde in der Folgenabschätzung darauf hingewiesen, dass das ESP von Zentralsystemen auch zur Abfrage von anderen Systemen benutzt werden könne. Eine solche Funktion sei zwischen den Systemen EES und VIS sowie auch bei ETIAS vorgesehen. Falls das ESP nicht entwickelt werden würde, müsste für ETIAS sowieso eine Funktion errichtet werden, welche die Aufgaben des ESP simuliere, damit das System funktionieren könne.[1152]

In der Folgenabschätzung wurden verschiedene Varianten einer möglichen Ausgestaltung des ESP geprüft: Mit und ohne SIS, mit und ohne Interpol-Datenbanken und Europol-Daten, mit und ohne ECRIS-TCN sowie mit und ohne biometrischer Abfragemöglichkeit. Letztlich wurde die umfangreichste Version zur Umsetzung empfohlen. Der Anschluss von Eurodac, VIS, EES und ETIAS an das ESP wurde in der Folgenabschätzung als Minimum aufgeführt, ohne dies genauer zu begründen.[1153]

Die Erforderlichkeit des ESP wird also u.a. mit der Einführung von neuen Systemen begründet. Dies erscheint nicht überzeugend.[1154] Zudem fehlt auch eine Begründung, wieso von den geprüften Varianten gerade die umfangreichste Form des ESP umgesetzt wurde. Davon abgesehen scheint sich die Notwendigkeit jedoch aus technischer Perspektive zu ergeben. So führen zu viele Verbindungen zwischen den Systemen zu einer Belastung. Dieser kann mit dem ESP begegnet werden. Auch unter Berücksichtigung, dass das ESP lediglich eine technische Neuerung darstellt und damit keine neuen Zugriffsrechte geschaffen werden oder mehr Datenbearbeitungen damit verbunden sind, kann die Erforderlichkeit des ESP bejaht werden.

3.4.1.3 *Zumutbarkeit*

Grundsätzlich ist davon auszugehen, dass das ESP keine grossen Auswirkungen auf die Datenbearbeitung mit sich bringt. So ist das ESP derart ausgestaltet, dass nur die Ergebnisse derjenigen Datenbanken angezeigt werden, für die der Endnutzer über eine Zugangsberechtigung verfügt. Des Weiteren ist das

1150 European Commission, Impact assessment IOP Part 2, 18 ff. m.w.H.
1151 European Commission, Impact assessment IOP Part 2, 41.
1152 European Commission, Impact assessment IOP Part 1, 37.
1153 Siehe dazu European Commission, Impact assessment IOP Part 2, 39 ff.
1154 Vgl. dazu auch WP29, Opinion proposals IOP, 4.

ESP ein Suchportal. Es werden also grundsätzlich keine Daten erzeugt, aktualisiert, gespeichert oder gelöscht. Davon ausgenommen sind lediglich die verschiedenen Nutzerprofile sowie die zu erstellenden Protokolle der im ESP vorgenommenen Abfragen.[1155]

Die Nutzerprofile stellen dabei sicher, dass lediglich auf diejenigen Systeme resp. Daten zugegriffen werden kann, auf welche der Endnutzer gemäss den gesetzlichen Bestimmungen der einzelnen Systeme auch tatsächlich zugreifen darf. Diese Profile hat eu-LISA regelmässig – mindestens einmal im Jahr – zu überprüfen und ggf. zu aktualisieren.[1156]

Die zu erstellenden Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, insbesondere der Prüfung der Zulässigkeit einer Abfrage sowie der Rechtmässigkeit der Datenbearbeitung als auch der Sicherstellung der Datensicherheit und -integrität verwendet werden.[1157] Die in den Protokollen zu erfassenden Angaben sind für die Protokolle von eu-LISA klar vorgeschrieben. Für die Schengen/Dublin-Staaten, resp. die Stellen der Union sind hingegen keine expliziten Vorgaben vorgesehen. Damit die mit den Protokollen verfolgte datenschutzrechtliche Kontrolle gewährleistet werden kann, erscheint es angezeigt, dass auch die Schengen/Dublin-Staaten sowie die Stellen der Union mindestens diejenigen Angaben erfassen, welche eu-LISA zu protokollieren hat. Werden nämlich zu wenige oder nicht relevante Angaben erhoben, kann auf der Grundlage dieser Protokolle keine effektive Kontrolle der Datenbearbeitung vorgenommen werden.

Da im ESP keine Daten gespeichert werden und die Nutzerprofile sicherstellen, dass die bestehenden Zugriffsberechtigungen eingehalten werden, erscheint das ESP aus datenschutzrechtlicher Perspektive zumutbar.[1158]

1155 Vgl. dazu European Commission, Impact assessment IOP Part 1, 37; European Commission, Impact assessment IOP Part 2, 46. Siehe dazu auch Europäische Kommission, Vorschlag IOP-Grenze, 15 f.

1156 Siehe dazu Art. 8 EU-IOP-VO.

1157 Siehe zu den Einzelheiten Art. 10 EU-IOP-VO. Siehe zum Zugang zu diesen Protokollen Art. 40 Abs. 4 EU-IOP-VO.

1158 Siehe dazu auch Jones, 19 f. Siehe dazu auch Quintel, data retention, 15.

3.4.2. Gemeinsamer Dienst für den Abgleich biometrischer Daten

3.4.2.1 *Geeignetheit*

Mit dem BMS wird ein Speicher für biometrische Templates geschaffen. Die Schaffung dieses Speichers ermöglicht es, biometrische Abgleiche systemübergreifend vorzunehmen. Damit trägt der BMS zur Verwirklichung der Ziele des EES, VIS, Eurodac, SIS und ECRIS-TCN bei. Ausserdem unterstützt der BMS den CIR und den MID.[1159]

Wie auch das ESP bezweckt der BMS also, die Verwirklichung der Ziele der von dieser Interoperabilitätskomponente betroffenen Informationssysteme zu unterstützen. Diese zielen insbesondere auf ein wirksames Management der Schengen-Aussengrenzen, der Wahrung der inneren Sicherheit sowie auf eine wirksame Umsetzung der Asyl- und Visapolitik ab.[1160]

Davon abgesehen unterstützt der BMS auch das Funktionieren des CIR und des MID. Mit diesen beiden Interoperabilitätskomponenten werden u.a. systemübergreifende biometrische Abfragen vorgenommen. Diese können nur ermöglicht werden, weil im BMS die biometrischen Templates von verschiedenen Informationssystemen gespeichert werden. Der BMS ist also geeignet, die mit dem CIR und dem MID sowie die mit den vorgenannten Systemen verfolgten öffentlichen Interessen zu begünstigen.[1161]

3.4.2.2 *Erforderlichkeit*

In der Folgenabschätzung wird die Errichtung des BMS dahingehend begründet, dass biometrische Daten einzigartig sind und deshalb gegenüber alphanumerischen Daten als zuverlässiger gelten. Mit dem BMS kann ausfindig gemacht werden, ob von einer Person bereits biometrische Daten in einem anderen System erfasst sind. Damit kann einerseits Identitätsbetrug entdeckt und bekämpft werden. Andererseits können auch Verwechslungen von Personen mit ähnlichen Profilen vermieden werden. Ausserdem geht aus der Folgenabschätzung hervor, dass ein einziger Speicher – im Vergleich mit jeweils

---

1159 Art. 12 Abs. 1 EU-IOP-VO. In der Machbarkeitsstudie zum BMS wurden verschiedene Optionen geprüft. Vgl. dazu EU-LISA, Feasibility Study sBMS.

1160 Siehe zum ESP Kapitel V.3.4.1. Siehe zu den öffentlichen Interessen der Interoperabilität Kapitel V.3.2.

1161 Siehe zu diesen Komponenten Kapitel V.3.4.6 und V.3.4.7.

einem pro System – vorteilhaft für die Sicherheit, die Kosten, die Wartung sowie den Betrieb ist.[1162]

Da biometrische Abfragen bereits für das Funktionieren der einzelnen Systeme vorgesehen sind, erscheint der BMS – abgesehen von den Vorteilen für die Sicherheit, Kosten, Wartung resp. den Betrieb – auf den ersten Blick nicht erforderlich. Systemübergreifende Abfragen von biometrischen Daten können jedoch erst ermöglicht werden, wenn die Templates an einem einzigen Ort gespeichert werden. Um systemübergreifende Abfragen vornehmen zu können, ist der BMS also erforderlich.

Im Sinne einer milderen Massnahme wurde vorgeschlagen, dass der BMS – wie auch das ESP – ohne Speicherfunktion ausgestaltet werden könnte.[1163] Die Speicherung von Templates wird jedoch nicht erst durch die EU-IOP-VO ermöglicht. Vielmehr speichern die bereits in Betrieb genommenen Systeme Templates, um biometrische Abfragen vorzunehmen.[1164] Aus datenschutzrechtlicher Perspektive wäre ein BMS ohne Speicherfunktion zu bevorzugen, da dies mit einer geringeren Datenbearbeitung einhergeht. Aktuell werden die Templates in den einzelnen Systemen gespeichert. Ob ein biometrischer Abgleich ganz ohne Speicherung von Templates (technisch) möglich wäre, erscheint fraglich.[1165] Grundsätzlich werden durch den BMS keine Daten geschaffen, welche nicht schon im Rahmen der einzelnen Informationssysteme erstellt werden.[1166] Die Interoperabilität bewirkt lediglich, dass diese Templates in einem gemeinsamen Speicher und nicht mehr in den einzelnen Systemen separat gespeichert werden. Ebenfalls unverändert bleibt, dass die Daten an einem einzigen Ort gespeichert werden. Sie werden also nicht dupliziert. In der Annahme, dass die Erforderlichkeit der Speicherung der Templates bereits bei den einzelnen Informationssystemen beurteilt und bejaht wurde, wird vorliegend davon ausgegangen, dass ein systemübergreifender Abgleich von biometrischen Daten ohne Speicherfunktion (technisch) nicht möglich ist. Insofern dürfte die Erforderlichkeit des BMS vorliegen.

1162 EUROPEAN COMMISSION, Impact assessment IOP Part 1, 38.

1163 FRA, borders and security, 24. Siehe dazu auch WP29, Opinion proposals IOP, 8 f.

1164 Siehe dazu FRA, Opinion IOP, 21.

1165 In der Machbarkeitsstudie des BMS wurde keine Variante ohne Speicherfunktion geprüft. Siehe dazu EU-LISA, Feasibility Study sBMS, 7.

1166 WP29, Opinion proposals IOP, 7. Siehe dazu auch EUROPEAN COMMISSION, Impact assessment IOP Part 1, 39.

3.4.2.3 *Zumutbarkeit*

Mit dem BMS wird – wie auch mit dem CIR – eine (biometrische) Datenbank geschaffen. Damit verbunden sind grundsätzlich Risiken von unerlaubten Zugriffen sowie der missbräuchlichen Verwendung der Daten.[1167]

Der BMS geht im Vergleich mit dem CIR insofern weniger weit, als der BMS nur Templates – nicht jedoch die Original-Daten – speichert. Im Gegensatz zum CIR, welcher keine SIS-Daten speichert, umfasst der BMS auch die Templates der im SIS gespeicherten Fingerabdruckdaten und Gesichtsbilder.[1168] Da ein Template grundsätzlich nicht wieder in die darin abgebildeten Original-Daten zurückverwandelt werden kann, darf davon ausgegangen werden, dass das Interesse von nicht zugriffsberechtigten Personen an diesen Daten – im Vergleich zum Interesse an den Original-Daten – geringer ausfällt.[1169] Wie auch bei den anderen Interoperabilitätskomponenten sind beim BMS zudem verschiedene Bestimmungen zur Datensicherheit vorgesehen.[1170]

Zur Gefahr der missbräuchlichen Verwendung ist festzustellen, dass nicht die Endnutzer auf den BMS zugreifen, sondern sich der CIR und das SIS dem BMS bedienen, um biometrische Abfragen vorzunehmen.[1171] Deshalb ist keine direkte Verbindung zwischen dem BMS und den Endnutzern vorhanden. Insofern besteht kein Risiko von unrechtmässigen resp. missbräuchlichen Zugriffen durch die Endnutzer. Wohl kann sich aber eine missbräuchliche Verwendung einer Abfrage des CIR resp. des SIS ergeben.[1172]

Die Speicherdauer der Templates im BMS orientiert sich an derjenigen der im CIR und im SIS gespeicherten Original-Daten. Dies stellt sicher, dass die Templates nur so lange für die systemübergreifenden biometrischen Abgleiche zur

---

1167 Siehe dazu Kapitel IV.5.4.1.1.

1168 WP29, Opinion proposals IOP, 8. Ursprünglich hätten auch die Templates der im SIS erhobenen DNA-Profile und Handflächenabdrücke im BMS gespeichert werden sollen. Die FRA bemerkte jedoch zu Recht, dass diese Daten nicht für systemübergreifende Abfragen benutzt werden können, da diese ausschliesslich im SIS erhoben werden. Siehe dazu FRA, Opinion IOP, 22. Fraglich erscheint, wieso das Foto des VIS-Antragstellers in Art. 13 Abs. 1 Bst. b IOP-Grenze-VO nicht erwähnt wird, obwohl in Art. 18 Abs. 1 Bst. b IOP-Grenze-VO festgelegt ist, dass ein solches Foto im CIR zu speichern ist. Der EDSB hatte diesen Hinweis bereits in seiner Stellungnahme zu den Vorschlägen der EU-IOP-VO vorgebracht. Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 78.

1169 Siehe zur Rückwandlung von Fingerabdruckdaten EU-LISA, Feasibility Study sBMS, 20.

1170 Siehe dazu Kapitel IV.5.4.1.2.

1171 Siehe dazu Art. 14 EU-IOP-VO.

1172 Siehe zu den Abfragen des CIR Kapitel V.3.4.3; V.3.4.4 sowie V.3.4.5.

Verfügung stehen, wie die Original-Daten für den Zweck des jeweiligen Informationssystems. Die Löschung erfolgt automatisch.[1173]

Des Weiteren ist die Datenbearbeitung im BMS von eu-LISA, jeder Stelle der EU sowie den Schengen/Dublin-Staaten zu protokollieren.[1174] Wie auch bei den Protokollen, welche von der Datenbearbeitung im ESP zu erstellen sind, sind die von den Schengen/Dublin-Staaten sowie den Stellen der EU zu erfassenden Angaben nicht explizit genannt. Damit die Protokolle die datenschutzrechtliche Kontrolle gewährleisten können, sollten zumindest diejenigen Angaben protokolliert werden, welche von eu-LISA zu erfassen sind.[1175]

Zusammenfassend ist festzuhalten, dass die Speicherung der biometrischen Templates im BMS erforderlich ist, um systemübergreifende biometrische Abfragen durchführen zu können. Die Schaffung einer solch grossen Datenbank ist mit gewissen Risiken verbunden. Aufgrund der Art der gespeicherten Daten, der vorgesehenen Begrenzung der Datenbearbeitung sowie der getroffenen Sicherheitsmassnahmen erscheint die Datenbearbeitung durch den BMS jedoch insgesamt zumutbar.

3.4.3. Abfrage des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten

In den gesetzlichen Grundlagen von Eurodac, VIS, EES und ETIAS ist eine indirekte Zugangsberechtigung von nationalen Strafverfolgungsbehörden resp. Europol vorgesehen. Diese ist an bestimmte Voraussetzungen geknüpft, welche teilweise zwar sehr ähnlich sind, sich aber dennoch voneinander unterscheiden.[1176]

Bis anhin muss eine berechtigte nationale Strafverfolgungsbehörde resp. Europol einen Antrag bei der zuständigen Stelle stellen, um Einsicht in die Daten aus dem EES, ETIAS, VIS oder Eurodac zu erhalten. Diese unabhängige Behörde prüft, ob der beantragte Zugang für die Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerwiegender Straftaten er-

1173 Siehe dazu Art. 15 EU-IOP-VO.

1174 Siehe zu den Einzelheiten Art. 16 EU-IOP-VO. Siehe zum Zugang zu diesen Protokollen Art. 40 Abs. 4 EU-IOP-VO.

1175 Siehe dazu Kapitel V.3.4.1.3. Es dürfte jedoch Art. 16 Abs. 1 Bst. b EU-IOP-VO entfallen, da eu-LISA für die Erstellung und Speicherung der Templates zuständig ist. Bst. a derselben Bestimmung müsste dahingehend abgeändert werden, als die Behörde resp. Stelle konkret zu benennen ist, welche die Abfrage durchführt.

1176 Siehe dazu Kapitel III.5.5.2; III.6.5.2; III.7.5.2 und III.8.5.3.

forderlich ist, ob der Zugriff im Einzelfall erforderlich ist und ob berechtigte Gründe betreffend die Annahme vorliegen, dass die Abfrage einen wesentlichen Beitrag zur Verhütung, Aufdeckung oder Untersuchung der betreffenden Straftaten leisten kann.[1177]

Bei Eurodac sowie teilweise auch beim EES sind die nationalen Strafverfolgungsbehörden abgesehen von diesen Zugangsbedingungen gehalten, vorgängig noch andere Systeme abzufragen.[1178] Wird in einem dieser Systeme ein Treffer angezeigt, beendet dies das Verfahren um Einsichtnahme. Diese Pflicht zur vorgängigen Abfrage anderer Systeme wird als «*Kaskadenmechanismus*» bezeichnet.[1179]

Ergibt sich bei der Abfrage der Kaskade kein Treffer resp. wird – wie beim VIS, ETIAS und teilweise EES – keine solche Abfrage vorausgesetzt, erhält die ersuchende Behörde Zugang zu den Daten des Treffers, sofern die unabhängige Behörde das Vorliegen der benötigten Voraussetzungen geprüft und bejaht hat. In bestimmten Situationen wird das Vorliegen der Zugangsbedingungen auch erst nach der Zugriffsgewährung geprüft. Insofern handelt es sich um ein indirektes Zugriffsrecht.[1180]

Bei den bereits in Betrieb genommenen Systemen zeigt sich, dass der Zugang zu Eurodac-Daten deutlich strenger und eingehender geregelt ist als derjenige zu VIS-Daten. Diese strengen Anforderungen sind zum Teil auch für die Abfragen im EES und ETIAS übernommen worden.[1181]

Die EU-IOP-VO sehen nun insofern eine Abänderung dieser Zugangsbedingungen vor, als neu ein zweistufiges Verfahren geschaffen wird. Die erste Stufe ist in Art. 22 EU-IOP-VO geregelt. Für die zweite Stufe verweist diese Bestim-

---

1177 Auf die Begriffe «*berechtigte Gründe*» sowie «*wesentlicher Beitrag*» wird noch genauer eingegangen. Siehe dazu Kapitel V.3.4.3.3.b). Siehe zu diesen Zugangsbedingungen Kapitel III.5.5.2; III.6.5.2; III.7.5.2 und III.8.5.3.

1178 Es handelt sich dabei um nationale Datenbanken und Abfragen gemäss der Prümer Zusammenarbeit. Bei Eurodac wird auch eine vorgängige Abfrage im VIS vorausgesetzt.

1179 Vgl. dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 60 f.

1180 Davon ausgenommen ist lediglich der Zugang von Europol zum VIS. Siehe zu den einzelnen Abfragen der betroffenen Systeme Kapitel III.5.5.2; III.5.5.3; III.6.5.2; III.6.5.3; III.7.5.2; III.7.5.3; III.8.5.3 und III.8.5.4. Siehe für eine Übersicht zu diesen Abfragen auch VAVOULA, Assessment, 148 ff.

1181 Dies ist einerseits auf die intensiven Verhandlungen im Zusammenhang mit der Revision der Eurodac-VO sowie andererseits auf die Entstehung der Systeme EES und ETIAS im Nachgang zu den Urteilen *Digital Rights*, *Tele2* sowie dem *Gutachten 1/15* zurückzuführen. In diesen Urteilen resp. in diesem Gutachten wurden den staatlichen Überwachungsmassnahmen signifikante Beschränkungen auferlegt. Siehe dazu VAVOULA, Assessment, 163.

mung auf die gesetzliche Grundlage des Informationssystems, in welchem ein Treffer erfolgte. Der Umfang der Einsicht in die Daten bleibt dadurch unverändert, d.h. es kann nicht in mehr und auch nicht in weniger Daten eingesehen werden. Geändert wird mit den EU-IOP-VO das Verfahren zur Einsichtnahme von den nationalen Strafverfolgungsbehörden sowie Europol in Daten aus Eurodac, VIS, EES und ETIAS.[1182] Dieses soll im Rahmen der Interoperabilität erleichtert und einheitlich geregelt werden.[1183] Die Gewährung des Zugangs als solcher wird im Folgenden nicht näher geprüft, da dieser durch die gesetzlichen Grundlagen von Eurodac, VIS, EES und ETIAS ermöglicht wird. Die nachfolgende Prüfung konzentriert sich ausschliesslich auf die mit der Interoperabilität angestrebte Erleichterung sowie einheitliche Regelung dieses Verfahrens.[1184]

Neu können die abfrageberechtigten Behörden in der ersten Stufe der Abfrage anhand einer Abfrage im CIR in Erfahrung bringen, ob in Eurodac, VIS, EES oder ETIAS Daten zur gesuchten Person vorhanden sind. Beim Ergebnis handelt es sich um eine sog. «*Treffer/kein Treffer*» Antwort.[1185] Solche Abfragen dürfen nur vorgenommen werden, wenn im konkreten Einzelfall vernünftige Hinweise vorliegen, dass die Abfrage zur Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten beitragen kann. Wird ein Treffer angezeigt, muss die abfragende Behörde im Rahmen der zweiten Stufe bei der zuständigen Stelle um Zugang zu diesen Daten ersuchen, wobei dabei die Voraussetzungen desjenigen Informationssystems erfüllt sein müssen, in welchem der Treffer erfolgte.[1186]

Die Erleichterung besteht darin, dass die nationalen Strafverfolgungsbehörden resp. Europol ohne vorgängige Kontrolle einer anderen Stelle in Erfahrung bringen können, ob und falls ja in welchem System resp. in welchen Systemen Daten zur gesuchten Person vorhanden sind. Dies stellt eine Erleichterung im Vergleich zur aktuellen Situation dar, da kein «*blinder Antrag*» auf Einsicht mehr gestellt werden muss. Damit eine solche Abfrage vorgenommen werden kann, sind zwar bestimmte Voraussetzungen einzuhalten. Eine Kontrolle, ob

1182 Siehe dazu Kapitel IV.5.3.3.3.

1183 Siehe dazu Art. 17 Abs. 1 EU-IOP-VO.

1184 Die Gewährung des Zugangs von nationalen Strafverfolgungsbehörden resp. Europol auf Datenbanken aus dem Migrationsbereich ist nicht unbedenklich. Siehe dazu FRA, biometrics, 65; FRA, Opinion Eurodac 2016, 40. Vgl. dazu auch Mitsilegas/Vavoula, 505 ff.

1185 Daraus ist ersichtlich, ob Daten in den abgefragten Systemen vorliegen oder nicht. Die Daten selbst werden jedoch nicht preisgegeben, sondern nur der Verweis auf das einschlägige System. Siehe dazu Art. 22 Abs. 2 EU-IOP-VO.

1186 Siehe zu den Einzelheiten Art. 22 EU-IOP-VO.

diese Voraussetzungen eingehalten wurden, ist jedoch nicht vorgesehen. Diese Voraussetzungen sind denjenigen, welche von den gesetzlichen Grundlagen der einzelnen Systeme verlangt werden, ähnlich. Die Kontrolle des Vorliegens dieser Voraussetzungen erfolgt jedoch erst auf der zweiten Stufe, also nachdem die abfrageberechtigten Behörden bereits den CIR abgefragt haben.

Letztlich wird also eine für alle Informationssysteme identische erste Stufe dem bereits vorgesehenen Abfrageverfahren vorgeschoben. Dies erleichtert den Behörden eine erste Abfrage. Die mit der Interoperabilität angestrebte einheitliche Regelung des Verfahrens wird hingegen insofern relativiert, als für die zweite Stufe des Zugangs auf die jeweiligen Bestimmungen der einzelnen Systeme verwiesen wird. Dadurch soll wohl den Besonderheiten der einzelnen Systeme Rechnung getragen werden.

3.4.3.1 *Geeignetheit*

Der CIR verfolgt das Ziel, den Zugang der nationalen Strafverfolgungsbehörden sowie Europol zum EES, VIS, ETIAS und Eurodac für die Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer und anderer schwerer Straftaten zu erleichtern und einheitlich zu regeln. Dies wird in Art. 22 EU-IOP-VO geregelt.[1187]

Die Erleichterung sowie einheitliche Regelung der bereits bestehenden Zugriffsmöglichkeit soll die Verfolgung der sekundären Ziele der Systeme Eurodac, VIS, EES und ETIAS, also der Zugang zwecks Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten, verbessern. Insofern ist Art. 22 EU-IOP-VO geeignet, einen Beitrag zur Verhinderung, Aufdeckung sowie Untersuchung terroristischer oder sonstiger schwerer Straftaten zu leisten. Damit wird insbesondere zur Wahrung der inneren Sicherheit beigetragen.[1188]

3.4.3.2 *Erforderlichkeit*

Aus der Folgenabschätzung geht hervor, dass die bestehenden Zugangsbedingungen und Sicherheitsmassnahmen die Effizienz sowie der berechtigte Gebrauch der Abfrage von Systemen zu Strafverfolgungszwecken einschränken.[1189] An der bisherigen Regelung wurde insbesondere der Kaskadenmecha-

1187 Siehe dazu Art. 17 Abs. 1 EU-IOP-VO.
1188 Siehe zum öffentlichen Interesse der Interoperabilität Kapitel V.3.2.
1189 European Commission, Impact assessment IOP Part 1, 11 f.

nismus kritisiert. Demnach müsse die Abfrage beendet werden, sobald ein Treffer in einem System, welches gemäss diesem Mechanismus abzufragen sei, vorliege. Dabei bleibe unberücksichtigt, dass andere Systeme noch weitere hilfreiche Informationen liefern könnten. Deshalb sollten alle verfügbaren Systeme abgefragt werden können.[1190] Die Konsultation von anderen Datenbanken stelle zudem einen hohen administrativen Aufwand dar. Die Stellung eines Antrags auf Einsicht in die Daten sei mit Verzögerungen verbunden.[1191] Die Informationen müssten jedoch schnell zugänglich sein. Insofern seien deshalb Kaskaden-Abfragen zu vermeiden.[1192]

Die Erforderlichkeit eines vereinfachten und einheitlich geregelten Zugangs der nationalen Strafverfolgungsbehörden sowie Europol wird also damit begründet, dass die bisherigen Zugangsbedingungen, insbesondere das Erfordernis der Kaskade, zu kompliziert und träge seien.

Den von eu-LISA erstellten Statistiken ist zu entnehmen, dass im VIS im Jahr 2020 rund 16'000, im Jahr 2021 rund 12'000, im Jahr 2022 knapp 14'000 und im Jahr 2023 bis und mit dem Monat September rund 15'000 Abfragen von nationalen Strafverfolgungsbehörden vorgenommen wurden. Die grosse Mehrheit dieser Abfragen wird jeweils von wenigen Schengen-Staaten durchgeführt.[1193] Bei Eurodac erfolgten solche Abfragen viel weniger häufig. Im Jahr 2023 wurden knapp 1600 Abfragen von nationalen Strafverfolgungsbehörden vorgenommen.[1194] Dies ist wenig überraschend. Schliesslich sind die Zugangsbedingungen bei Eurodac viel höher angesetzt als beim VIS (u.a. wird auch eine Abfrage im VIS vorausgesetzt).

Diese Statistiken veranschaulichen, dass die Abfrage bisher nur von nationalen Strafverfolgungsbehörden weniger Schengen/Dublin-Staaten benutzt wird. Aufgrund dieses unterschiedlichen Abfrageverhaltens stellt sich die Frage, ob eine Anpassung des Verfahrens überhaupt erforderlich erscheint.[1195]

Die niedrige Anzahl der Abfragen könnte einerseits darauf zurückzuführen sein, dass die Ergebnisse der Abfragen für die abfrageberechtigten Behörden nicht nützlich sind. Andererseits könnte der Grund dafür auch sein, dass – wie dies in der Folgenabschätzung propagiert wurde – die Zugangsbedingungen

1190 European Commission, Impact assessment IOP Part 1, 25, 43; HLEG, final report, 15 f.
1191 European Commission, Impact assessment IOP Part 1, 25.
1192 HLEG, final report, 53.
1193 eu-LISA, VIS report 2022, 26 f., 31; eu-LISA, VIS report 2024, 22, 25.
1194 Siehe dazu eu-LISA, Eurodac report 2023, 12.
1195 Vgl. dazu Vavoula, Deathblow, 150 f. Aufgrund der überschaubaren Anzahl der Abfragen wird der Zugang zu Eurodac-Daten in Frage gestellt. Siehe dazu Guerra.

zu hoch angesetzt sind. Aus dem Umstand, dass doch einige Staaten Gebrauch von diesen Abfragen machen, lässt sich schliessen, dass diese die (strengen) Zugangsbedingungen in Anbetracht der Ergebnisse in Kauf nehmen. Leider wird statistisch nicht erfasst, wie viele falsche positive Treffer bei solchen Abfragen hervorgehen. Auch finden sich keine Hinweise dazu, wie nützlich diese Daten für die abfragenden Behörden sind, also z.B. wie viele Verurteilungen dank dieser Daten vorgenommen werden konnten. Informationen zu allfälligen Verweigerungen des Zugangs zu den Daten fehlen ebenfalls.[1196] Aus den erhobenen Statistiken lassen sich demnach keine verlässlichen Schlüsse zur Erforderlichkeit einer Erleichterung und Vereinheitlichung des Zugangs zu Strafverfolgungszwecken ziehen.[1197]

Dem Argument, dass die Antragstellung zu Verzögerungen führe, kann entgegengehalten werden, dass bereits gemäss der bisherigen Regelung in dringenden Fällen die grundsätzlich vor der Zugriffsgewährung vorgenommene Kontrolle der Zugangsbedingungen auch erst nach der Einsicht in die Daten erfolgen kann. Auch führt das Erfordernis der Kaskade zu keinen nennenswerten Verzögerungen, da nationale Datenbanken grundsätzlich in kurzer Zeit abgefragt werden können. Bei der Abfrage im Rahmen der Prümer Zusammenarbeit ist die Abfragezeit offenbar davon abhängig, wie der Mechanismus in den jeweiligen Mitgliedstaaten ausgestaltet ist.[1198]

Die in der Folgenabschätzung aufgeführte Begründung der Erforderlichkeit einer Erleichterung sowie einer einheitlichen Regelung der Abfrage zu Strafverfolgungszwecken überzeugt deshalb nicht. Insbesondere fehlt es an entsprechenden Belegen, welche die Erforderlichkeit untermauern würden.[1199] Die Erforderlichkeit, das Verfahren für den Zugang der nationalen Strafverfolgungsbehörden sowie Europol zu Daten aus dem VIS, Eurodac, EES und ETIAS zwecks Verhütung, Aufdeckung sowie Untersuchung von terroristischen und sonstigen schweren Straftaten zu erleichtern und einheitlich zu regeln, erscheint insgesamt nicht ausreichend begründet und belegt.

1196 Vgl. dazu zum VIS Vavoula, Assessment, 157. Es wird nur erfasst, wie viele dringende Anträge eingereicht wurden und wie viele davon im Nachhinein als nicht dringend beurteilt wurden. Siehe dazu eu-LISA, VIS report 2022, 31.

1197 Zum Nutzen von PNR-Daten für die Identifizierung von Personen, die einer terroristischen oder sonstigen schweren Straftat verdächtig werden, scheint es hingegen entsprechende Statistiken zu geben. Siehe dazu EuGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 56.

1198 FRA, Opinion IOP, 33 f.

1199 Vgl. dazu auch EDSB, Reflexionspapier IOP, N 16.

Bereits die aktuelle Gewährung des Zugriffs der nationalen Strafverfolgungsbehörden erfolgte auf der Basis von wenig überzeugenden Argumenten. Eine solche Zugriffsmöglichkeit wurde zuerst beim VIS, später bei Eurodac und schliesslich auch beim EES und ETIAS vorgesehen. Beim VIS wurde dies damit begründet, dass den nationalen Strafverfolgungsbehörden möglichst viele Daten zur Verfügung stehen sollten.[1200] Bei Eurodac war der Zugang insofern problematischer, als in diesem System Daten von Personen gespeichert sind, welche schutzbedürftig sind. Mehrere Legislativvorschläge der Kommission, welche einen Zugang der nationalen Strafverfolgungsbehörden auf Eurodac-Daten vorsahen, sind gescheitert ehe schliesslich dennoch ein Zugriffsrecht gewährt wurde. Die Begründung der Erforderlichkeit dieser Zugriffsgewährung ist dabei nicht überzeugender als beim VIS.[1201] Beim EES liess der erste Vorschlag der Kommission die Gewährung eines entsprechenden Zugangs noch offen. Ein solcher wurde letztlich gewährt, weil die Schengen-Staaten geltend gemacht haben, dass der Zugang zu VIS-Daten für die Aufklärung verschiedener Straftaten hilfreich gewesen sei.[1202] Bei der Erarbeitung der gesetzlichen Grundlagen des ETIAS wurde schliesslich einfach angenommen, dass auch die ETIAS-Daten für die Strafverfolgung hilfreich sein könnten.[1203]

Diese Entwicklung zeigt, dass der Zugang von nationalen Strafverfolgungsbehörden zu Systemen aus dem Migrationsbereich zunehmend normal wurde. Dies obwohl die Erforderlichkeit eines solchen Zugangs nicht überzeugend dargelegt wurde und die Effektivität des Zugangs nur rudimentär mit effektiven Zahlen belegt werden kann. Die Prävention von Straftaten dürfte nur schwer messbar sein.[1204] Im Bereich der Strafverfolgung dürfte es hingegen

1200 Siehe dazu VAVOULA, Assessment, 156 f.

1201 Siehe dazu ErwG. 8 Eurodac-VO. Offenbar spielte bei der Zugriffsgewährung die Umsetzung des automatisierten Fingerabdruckidentifizierungssystems (AFIS) in den Mitgliedstaaten eine Rolle. So konnte ein Mitgliedstaat bei einer Prüm-Abfrage ebenfalls Eurodac-Daten abfragen, wenn diese Daten ebenfalls im AFIS gespeichert waren. Im umgekehrten Fall war dies damals nicht möglich. Siehe dazu VAVOULA, Assessment, 157 ff.

1202 VAVOULA, Assessment, 159; EUROPÄISCHE KOMMISSION, Vorschlag EES, 6. Die Kommission hatte dabei zwar festgestellt, dass die Verwendung der im EES gespeicherten Daten in Anbetracht der Nützlichkeit dieser Daten für die Strafverfolgung nicht verhältnismässig sei. Unter Druck sowie unter Berücksichtigung der Terroranschläge in Europa, erarbeitete die Kommission schliesslich doch einen Vorschlag für das EES, welcher einen Zugang der nationalen Strafverfolgungsbehörden vorsah. Siehe dazu MITSILEGAS/VAVOULA, 514.

1203 EUROPÄISCHE KOMMISSION, ETIAS-Vorschlag, 11; VAVOULA, Assessment, 160.

1204 VAVOULA, Assessment, 160.

möglich sein, Zahlen zur Wirksamkeit des Zugriffs von den nationalen Strafverfolgungsbehörden auf Systeme aus dem Migrationsbereich zu erheben.[1205]

Um die Gewährung des Zugriffs der nationalen Strafverfolgungsbehörden sowie Europol überhaupt rechtfertigen zu können, mussten (immerhin) strenge Zugangsbedingungen aufgestellt werden. Es wurde den abfrageberechtigten Stellen explizit kein direkter Zugriff auf Daten gewährt, da diese primär für andere Zwecke erhoben werden.[1206]

3.4.3.3 *Zumutbarkeit*

a) Funktion des Kaskadenmechanismus

Ein Kaskadenmechanismus ist aktuell bei Eurodac vorgesehen.[1207] Ebenso beim EES, sofern die Abfrage für die Identifizierung von unbekannten Verdächtigen, Straftätern oder mutmasslichen Opfern terroristischer oder sonstiger schwerer Straftaten erfolgt.[1208] Dieser Mechanismus ist jedoch in den beiden Systemen nicht genau gleich ausgestaltet. Er verlangt grundsätzlich, dass bevor auf Eurodac-Daten resp. EES-Daten zugegriffen werden darf, vorgängig andere Datenbanken abgefragt werden müssen.[1209] Nur wenn diese vorgängige Abfrage ohne Treffer verlaufen ist, darf auf die entsprechenden Daten aus den Systemen Eurodac resp. EES zugegriffen werden. Die Informationssysteme VIS und ETIAS sehen hingegen keinen Kaskadenmechanismus vor.[1210]

1205 Bei den PNR-Daten ist dies zumindest möglich. Siehe dazu EuGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 56.

1206 Vgl. dazu Lobsiger/Gloor Scheidegger, 320 ff. Siehe dazu ausserdem BGE 144 I 126, E. 8.3.2 ff., wobei das BGer ebenfalls berücksichtigte, dass die Strafverfolgungsbehörden keinen direkten und uneingeschränkten Zugriff auf die Daten hätten, sondern dass dieser «*strengen Anforderungen*» unterworfen sei. Ausserdem seien angemessene Schutzvorkehrungen vorgesehen worden, um Missbräuche zu vermeiden.

1207 Art. 20 Abs. 1 Eurodac-VO.

1208 Art. 32 Abs. 2 EES-VO.

1209 Dies betrifft die nationalen Datenbanken sowie die Abfragen gemäss der Prümer Zusammenarbeit. Bei Eurodac wird zudem eine vorgängige Abfrage des VIS verlangt.

1210 Beim ETIAS war im Vorschlag der Verordnung zwar ein Kaskadenmechanismus sowohl für die nationalen Strafverfolgungsbehörden als auch für Europol vorgesehen (siehe dazu Europäische Kommission, ETIAS-Vorschlag, 61 ff.). Dieser wurde jedoch nicht in die ETIAS-VO überführt. Grundsätzlich wäre es konsequenter gewesen auch beim VIS und bei ETIAS einen Kaskadenmechanismus vorzusehen. Im EES werden ebenfalls die Daten der im VIS erfassten visumpflichtigen Personen sowie den im ETIAS erfassten visumbefreiten Personen gespeichert. Die aktuelle Regelung führt nun dazu, dass für den Zugang zu den Daten im VIS und ETIAS keine Kaskade vorliegt. Für die Daten der gleichen Person, welche im EES gespeichert sind, u.U. jedoch schon. Vgl. dazu Vavoula, Assessment, 166.

Aus der Eurodac-VO geht hervor, dass der Kaskadenmechanismus – basierend auf den Prinzipien der Verhältnismässigkeit sowie der Zweckbestimmung – eine Sicherheitsmassnahme darstellt. Die Einführung dieses Mechanismus spiegelt die spezielle Sensitivität der in den Systemen gespeicherten Daten wider. Demnach soll die Hürde für die Behörden, welche für die innere Sicherheit zuständig sind, bei einer Abfrage in Eurodac signifikant höher sein, als die Hürde bei einer Abfrage in strafrechtlichen Datenbanken.[1211] Insbesondere da es sich bei den in Eurodac erfassten Daten um Daten vulnerabler Personen handelt, welche um internationalen Schutz ersuchen und grundsätzlich keinen Zusammenhang mit kriminellen Aktivitäten oder anderen Sicherheitsrisiken aufweisen, müssen robuste Sicherheitsmassnahmen beim Zugriff von nationalen Strafverfolgungsbehörden vorgesehen werden.[1212]

Der Kaskadenmechanismus stellt also ein zentrales Element für die Verhältnismässigkeit des Zugangs der nationalen Strafverfolgungsbehörden zu Informationssystemen aus dem Migrationsbereich dar.[1213]

Aufgrund der Wichtigkeit dieses Elements bei der Gewährung des Zugriffs, erscheint es erstaunlich, dass insbesondere der Kaskadenmechanismus in der im Zuge der Interoperabilität vorgenommenen Folgenabschätzung kritisiert wurde.[1214] Dem Vorschlag zur IOP-Polizei-VO sind sogar Hinweise zu entnehmen, dass der Kaskadenmechanismus hätte abgeschafft werden sollen.[1215]

Der Kaskadenmechanismus ist in den gesetzlichen Grundlagen von Eurodac und dem EES geregelt. Solange diese Rechtsakte nicht entsprechend angepasst werden, bleibt dieses Erfordernis bestehen. Diese Bedingung wird jedoch mit der Inbetriebnahme der Interoperabilität auf die zweite Stufe des Zugangsverfahrens verschoben.[1216]

Dies erscheint aus praktischen Gründen wenig sinnvoll. So kann eine zugriffsberechtigte Behörde zwar im Rahmen der ersten Zugangsstufe in Erfahrung bringen, dass Daten z.B. in Eurodac vorhanden sind. Erfolgt dann, im Rah-

1211 Siehe dazu ErwG. 10 Eurodac-VO.

1212 Siehe dazu ErwG. 15 Eurodac-VO.

1213 Siehe zum Ganzen FRA, biometrics, 67.

1214 Siehe dazu Kapitel V.3.4.3.2.

1215 Siehe dazu Europäische Kommission, Vorschlag IOP-Polizei, 11. Teilweise wurde dies auch so aufgefasst, dass der Kaskadenmechanismus wegfallen sollte. Siehe dazu FRA, Opinion IOP, 30. Dies wurde auch bereits in der Folgenabschätzung so propagiert. Siehe dazu European Commission, Impact assessment IOP Part 1, 43.

1216 Siehe dazu Art. 22 Abs. 3 EU-IOP-VO. Die gesetzliche Grundlage von Eurodac wurde mittlerweile revidiert. Siehe dazu Kapitel III.5.7.

men der zweiten Zugangsstufe, aber bei der Abfrage der Kaskade ein Treffer, darf die abfragende Behörde letztlich keinen Zugriff auf die Eurodac-Daten erhalten, da die Zugangsvoraussetzungen nicht erfüllt sind. Ob diese Verweigerung des Zugangs in der Praxis konsequent durchgeführt werden würde, ist zu bezweifeln. Schliesslich konnte die abfragende Behörde bereits in Erfahrung bringen, dass für die Verhütung, Untersuchung oder Verhinderung von terroristischen oder sonstigen schweren Straftaten nützliche Informationen in einem Informationssystem vorhanden sind.[1217]

Der EDSB hatte deshalb vorgeschlagen, die Kaskade auf der ersten Stufe vorzusehen. Insbesondere mit der Prümer Zusammenarbeit sei schliesslich ein spezifisches System geschaffen worden, welches den Austausch polizeilicher Informationen inkl. Fingerabdruckdaten erleichtern soll. Nur weil die Prümer Zusammenarbeit bislang noch nicht vollständig von den Mitgliedstaaten umgesetzt worden sei, solle dies nicht zur Folge haben, dass den nationalen Strafverfolgungsbehörden stattdessen Zugriff auf andere Systeme anderer Behörden gewährt werden solle.[1218] Wäre dieser Empfehlung des EDSB Folge geleistet worden, wären die bisherigen Zugangsbedingungen der nationalen Strafverfolgungsbehörden zu Daten aus dem VIS, ETIAS und teilweise auch dem EES verschärft worden, da diese Informationssysteme bis anhin keinen resp. nur einen beschränkten Kaskadenmechanismus vorsehen. Wie die FRA jedoch gemäss der hier vertretenen Ansicht überzeugend vorbrachte, handelt es sich insbesondere bei den Prüm-Daten, welche im Rahmen des Kaskadenmechanismus abzufragen sind, um sehr umfangreiche Informationen über kriminelle Aktivitäten, Verdächtige und Straftäter. Eine solche Abfrage dürfte also die grössten Chancen bieten, dass hilfreiche Informationen für den Kampf gegen Terrorismus sowie schwerer Kriminalität erhältlich gemacht werden können.[1219]

Es erscheint vor diesem Hintergrund nicht ersichtlich, weshalb nicht primär zuerst diejenigen Systeme zu konsultieren sind, welche einen strafrechtlichen Fokus aufweisen. Bei den Informationssystemen, bei welchen eine Abfrage von nationalen Strafverfolgungsbehörden resp. Europol vorgesehen ist, handelt es sich hingegen um Systeme, welche primär migrationsrechtliche Zwecke verfolgen. Die Personen, deren Daten in diesen Systemen gespeichert werden,

1217 Vgl. dazu VAVOULA, Assessment, 175. Vgl. dazu auch JONES, 26. Vielleicht gerade deshalb wird nun zukünftig das Erfordernis der Kaskade bezüglich Eurodac-Daten nicht mehr vorausgesetzt. Siehe dazu Kapitel III.5.7.

1218 EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 65 ff.

1219 FRA, Opinion IOP, 34.

weisen grundsätzlich keinen Bezug zu einem kriminellen Verhalten auf. Diese Daten sollten demnach nur sehr zurückhaltend für die Strafverfolgung verwendet werden dürfen.[1220]

b) Zugangsbedingungen

Art. 22 Abs. 1 EU-IOP-VO sieht drei Voraussetzungen vor, damit eine Abfrage im CIR zwecks Verhütung, Verfolgung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten vorgenommen werden darf. So müssen im konkreten Einzelfall vernünftige Gründe vorliegen, dass eine Abfrage der Systeme zur Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger Straftaten beitragen kann.[1221] Diese Voraussetzungen sind – abgesehen vom Erfordernis der Kaskade – ziemlich ähnlich wie diejenigen, welche gemäss den gesetzlichen Grundlagen der Systeme Eurodac, VIS, EES und ETIAS gefordert werden.[1222]

Ein Vergleich des Kriteriums der «*vernünftigen Gründe*» mit den gesetzlichen Grundlagen der einzelnen Systeme zeigt, dass bei Eurodac[1223] «*hinreichende Gründe*», beim VIS[1224] «*berechtigte Gründe*» und beim EES[1225] und ETIAS[1226] «*Beweise oder hinreichende Gründe*» vorausgesetzt werden. Fraglich erscheint, ob trotz der unterschiedlichen Wortwahl dasselbe Kriterium gemeint ist. In der englischen Sprachversion werden jeweils derselbe oder zumindest sehr ähnliche Begriffe verwendet.[1227] Insofern dürfte den unterschiedlichen Begriffen in der deutschen Sprachfassung nicht allzu grosses Gewicht zugemessen

---

1220 Vgl. dazu auch FRA, Opinion IOP, 32 ff.

1221 In den Vorschlägen zu den EU-IOP-VO fehlte die Voraussetzung, dass hinreichende Gründe vorliegen müssen. Dies hatte die FRA bemängelt. Siehe dazu FRA, Opinion IOP, 31 f.

1222 Siehe Kapitel III.5.5.2; III.6.5.2; III.7.5.2 und III.8.5.3.

1223 Art. 20 Abs. 1 Bst. c Eurodac-VO. Bezüglich der Abfrage von Europol Art. 21 Abs. 1 Bst. c Eurodac-VO.

1224 Art. 3 Abs. 1 VIS-VO; Art. 5 Abs. 1 Bst. c VIS-Beschluss. Bezüglich der Abfrage von Europol Art. 7 VIS-Beschluss. Gemäss dieser Bestimmung können Daten entweder zu Analysezwecken oder in anonymisierter Form verwendet werden, weshalb dieses Kriterium nicht verwendet wird.

1225 Art. 32 Abs. 1 Bst. c EES-VO. Bezüglich der Abfrage von Europol Art. 33 Abs. 1 Bst. c EES-VO.

1226 Art. 52 Abs. 1 Bst. c ETIAS-VO. Bezüglich der Abfrage von Europol Art. 53 Abs. 2 Bst. d ETIAS-VO.

1227 So wird bei Eurodac der Begriff «*reasonable grounds*», beim EES und ETIAS «*evidence or reasonable grounds*» und beim VIS «*reasonable grounds*» benutzt. Letzterer Begriff wird auch in Art. 20 Abs. 1 EU-IOP-VO verwendet.

werden. Vorliegend wird deshalb davon ausgegangen, dass es sich bei diesen Begriffen um Synonyme handelt.

Des Weiteren muss die Abfrage gemäss Art. 22 Abs. 1 EU-IOP-VO zur Verhütung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten beitragen. Eine zumindest ähnliche Formulierung wird auch in den gesetzlichen Grundlagen des EES[1228] und des ETIAS[1229] verwendet. Bei Eurodac wird jedoch ein «*wesentlicher*» Beitrag[1230] und beim VIS ein «*erheblicher*» Beitrag[1231] gefordert. Diese Wortwahl könnte darauf schliessen lassen, dass die Hürde hinsichtlich dieses Kriteriums beim VIS und Eurodac deutlich höher angesetzt ist.[1232] Auch die Wortwahl in der englischen Sprachfassung lässt darauf schliessen.[1233] Ausgehend vom Verständnis, dass bei Eurodac und dem VIS ein wesentlicher resp. erheblicher Beitrag verlangt wird, hätte dies zur Folge, dass bei einem Antrag auf Einsicht in Daten aus Eurodac resp. dem VIS für die erste Stufe des Zugangs zwar auch ein Beitrag ausreicht, welcher weder «*wesentlich*» noch «*erheblich*» ist. Für den effektiven Zugang zu den Daten – also die zweite Stufe des Zugangs – wäre jedoch ein «*wesentlicher*» resp. «*erheblicher*» Beitrag erforderlich. Dies erscheint wenig sinnvoll. Denn so könnten die nationalen Strafverfolgungsbehörden zwar in Erfahrung bringen, dass Daten in Eurodac resp. im VIS vorhanden sind. Sie könnten aber nicht auf diese zugreifen, da der Zugriff nicht die nötige Wesentlichkeit resp. Erheblichkeit im Zusammenhang mit der Verhinderung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren Straftat herbeiführen könnte.

Insgesamt ergibt sich aus den Zugangsbedingungen von Art. 22 EU-IOP-VO, dass diese Abfrage auf bestimmte Fälle beschränkt werden soll. Die Voraussetzungen für eine Abfrage des CIR sind, abgesehen von einem allfälligen Er-

1228 Art. 32 Abs. 1 Bst. c EES-VO. Bezüglich der Abfrage von Europol Art. 33 Abs. 1 Bst. c EES-VO.

1229 Art. 52 Abs. 1 Bst. c ETIAS-VO. Bezüglich der Abfrage von Europol Art. 53 Abs. 2 Bst. d ETIAS-VO.

1230 Art. 20 Abs. 1 Bst. c Eurodac-VO. Bezüglich der Abfrage von Europol Art. 21 Abs. 1 Bst. c Eurodac-VO.

1231 Art. 3 Abs. 1 VIS-VO; Art. 5 Abs. 1 Bst. c VIS-Beschluss. Bezüglich der Abfrage von Europol Art. 7 VIS-Beschluss. Gemäss dieser Bestimmung können Daten entweder zu Analysezwecken oder in anonymisierter Form verwendet werden, weshalb dieses Kriterium nicht verwendet wird.

1232 Vgl. dazu auch FRA, biometrics, 66.

1233 So wird in den EU-IOP-VO sowie in den gesetzlichen Grundlagen des EES sowie ETIAS das Wort «*contribute*» verwendet. Bei Eurodac sowie dem VIS hingegen «*substantially contribute*».

fordernis einer Abfrage der Kaskade, sehr ähnlich ausgestaltet wie diejenigen, welche die gesetzlichen Grundlagen der einzelnen Systeme vorsehen. Da jedoch zum Teil andere Formulierungen verwendet wurden, stellt sich die Frage, ob der EU-Gesetzgeber damit zum Ausdruck bringen wollte, dass es sich um unterschiedliche Voraussetzungen handelt. Grundsätzlich dürfte es wohl nur sinnvoll sein, wenn eine den CIR abfragende Behörde bei einem Treffer letztlich auch um Einsicht in diese Daten ersuchen kann. Insofern dürfte es kontraproduktiv sein, wenn die Zugangsbedingungen der zweiten Zugangsstufe höher angesetzt sind als bei der ersten, da so die Behörden zwar in Erfahrung bringen könnten, dass Daten vorhanden sind, aber letztlich keine Einsicht in diese erhalten.

c) Weitere Sicherheitsmassnahmen

Die durch die EU-IOP-VO veränderten Zugangsbedingungen führen dazu, dass auf der ersten Stufe nicht kontrolliert wird, ob die Zugangsbedingungen für die Abfrage des CIR erfüllt sind. Erst während der zweiten Zugangsstufe prüft die zuständige Stelle, ob die Zugangsbedingungen, welche die gesetzlichen Grundlagen des einschlägigen Informationssystems verlangen, vorliegen. Eine Kontrolle durch die unabhängige Behörde findet also erst statt, nachdem die abfragende Behörde bereits erfahren hat, in welchem System Daten der betroffenen Person gespeichert sind (aber immerhin vor dem effektiven Zugang zu den Daten). Diese Systematik hat zur Folge, dass die Zugangsbedingungen gemäss Art. 22 Abs. 1 EU-IOP-VO nicht explizit überprüft werden. Wie bereits erläutert, ist unklar, ob diese Zugangsbedingungen deckungsgleich mit denjenigen in den gesetzlichen Grundlagen der einzelnen Systeme sind. Sie weisen jedoch zumindest grosse Ähnlichkeiten auf.[1234] Wird davon ausgegangen, dass diese Zugangsbedingungen identisch sind, impliziert eine Gutheissung eines Einsichtsgesuchs durch die unabhängige Kontrolle, welche die Zugangsbedingungen gemäss den gesetzlichen Grundlagen der Systeme prüft, auch, dass die Voraussetzungen gemäss Art. 22 Abs. 1 EU-IOP-VO erfüllt sind.

Der Umstand, dass eine Kontrolle erst stattfindet, nachdem die abfrageberechtigten Behörden eine Abfrage im CIR vorgenommen haben, birgt die Gefahr von missbräuchlichen Abfragen. Denn grundsätzlich ist es möglich, Abfragen im CIR vorzunehmen, auch wenn die Voraussetzungen gemäss Art. 22 Abs. 1 EU-IOP-VO nicht vorliegen. Dadurch können die abfragenden Behörden

[1234] Siehe dazu Kapitel V.3.4.3.3.b).

zumindest in Erfahrung bringen, ob Daten in den Systemen vorhanden sind.[1235] Auch wenn es sich bei der Angabe, ob ein Treffer vorliegt oder nicht um ein vermeintlich banales Ergebnis handelt, können auch aus dieser Information Schlüsse gezogen werden. So sagt ein Treffer in der Eurodac-Datenbank z.B. aus, dass es sich bei der betroffenen Person um einen Drittstaatsangehörigen handelt, welcher um Asyl ersucht hat.[1236] Folglich handelt es sich auch bei der «*Treffer/kein Treffer Angabe*» um personenbezogene Daten.[1237] Aus der Folgenabschätzung geht zwar hervor, dass diese Informationen ohne die zusätzlichen Informationen in den Systemen keinen praktischen Nutzen hätten.[1238] Es kann jedoch nicht ausgeschlossen werden, dass in Einzelfällen genau diese Information von entscheidender Bedeutung ist.

Als Garantie gegen eine mögliche missbräuchliche Verwendung des Zugangs durch die abfrageberechtigten Behörden darf die Treffer/kein Treffer Antwort ausschliesslich für den Antrag auf Einsicht in das System resp. zumindest eines der Systeme, in welchem ein Treffer erzielt wurde, benutzt werden. Eine Nichtbeantragung auf Einsicht in die Daten muss begründet werden.[1239] Dies wird von der zuständigen Aufsichtsbehörde resp. dem EDSB anhand der zu erstellenden Protokolle spätestens alle sechs Monate überprüft.[1240] Nicht ersichtlich ist jedoch, was die Folgen einer missbräuchlichen Abfrage sind. So sind keine Sanktionen vorgesehen, welche verhängt werden können, sollte ein Zugang einer abfrageberechtigten Behörde nicht rechtmässig erfolgt sein. Zumindest hätte explizit in den EU-IOP-VO verankert werden sollen, dass die aus dem CIR gezogenen Daten wieder zu löschen sind, wenn sich herausstellt, dass der Zugang nicht gerechtfertigt gewesen war.[1241]

Abgesehen davon sind sowohl eu-LISA, Europol als auch die Schengen/Dublin-Staaten gehalten, Protokolle von den vorgenommenen Abfragen zu erstellen. Diese Zugangsprotokolle werden von der zuständigen Aufsichtsbehörde

1235 Siehe dazu FRA, Opinion IOP, 32. Die FRA hatte deshalb vorgeschlagen, einen unabhängigen Mechanismus einzuführen, damit auch die Voraussetzungen gemäss Art. 22 Abs. 1 EU-IOP-VO – zumindest in nicht systematischer Weise – kontrolliert werden könnten.

1236 Auch das Resultat, dass kein Treffer gefunden wurde, kann Rückschlüsse ermöglichen. Siehe dazu VAVOULA, Interoperability, 187.

1237 EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 58; WP29, Opinion proposals IOP, 13.

1238 Vgl. dazu EUROPEAN COMMISSION, Impact assessment IOP Part 1, 44.

1239 Art. 22 Abs. 2 EU-IOP-VO.

1240 Siehe zu den Einzelheiten Art. 24 Abs. 4-6 EU-IOP-VO.

1241 Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 68. Zumindest in Art. 31 Abs. 3 EES-VO sowie Art. 51 Abs. 4 UAbs. 2 ETIAS-VO ist ausdrücklich festgehalten, dass die Daten zu löschen sind, wenn diese durch einen unrechtmässigen Zugriff resp. eine unrechtmässige Abfrage erlangt wurden.

resp. dem EDSB spätestens alle sechs Monate dahingehend geprüft, ob die Verfahren und Bedingungen eingehalten wurden.[1242] Das Protokollieren der Abfragen ist zwar wichtig, kann jedoch nicht die Möglichkeit der vorgängigen oder zumindest parallelen Kontrolle der Zugangsbedingungen ersetzen.[1243]

Des Weiteren haben die Schengen/Dublin-Staaten sowie Europol Jahresberichte über die Wirksamkeit des Zugangs zum CIR gemäss Art. 22 EU-IOP-VO zu erstellen, wobei diesen Berichten u.a. Informationen und Statistiken zum genauen Zweck der Abfrage oder die Anzahl und die Art von Fällen, in denen die Identität einer Person festgestellt werden konnte, zu entnehmen sind.[1244] Die Pflicht zur Erstellung von solchen Jahresberichten ist zu begrüssen.

d) Für die Abfrage verwendete Daten

In Art. 22 EU-IOP-VO wird nicht festgelegt, mit welchen Daten die Abfrage vorgenommen werden darf. Aus den gesetzlichen Grundlagen der betroffenen Informationssysteme geht hervor, dass bei Eurodac nur anhand von biometrischen Daten (bisher Fingerabdruckdaten) abgefragt werden darf.[1245] Beim VIS[1246] und beim EES[1247] kann die Abfrage hingegen auch mit alphanumerischen Daten vorgenommen werden. Da ETIAS[1248] keine biometrischen Daten enthält, ist die Abfrage nur mit alphanumerischen Daten möglich.

Für eine Abfrage mit alphanumerischen Daten können verschiedene Angaben verwendet werden, so bspw. beim VIS der Reisegrund, beim EES das Datum und der Ort der Einreise und beim ETIAS z.B. die IP-Adresse. Wird eine solche Angabe in den CIR eingegeben, ist damit zu rechnen, dass eine Vielzahl von Treffern angegeben wird. Durch die Eingabe von solchen Angaben ist die Suchabfrage nicht individualisiert.[1249] Die Möglichkeit der Abfrage des CIR anhand von alphanumerischen Daten führt also dazu, dass mit grosser Wahrscheinlichkeit eine grosse Anzahl von Daten von Personen angezeigt wird, welche nicht auf dem Radar der abfragenden Behörde sind. Durch deren Aufführung als (vermeintlicher) Treffer der Suchabfrage besteht das Risiko, dass diese Personen Nachteile erleiden können. Sie könnten z.B. mit einem Straf-

1242 Siehe zu den Einzelheiten Art. 24 Abs. 4-6 EU-IOP-VO.
1243 Vgl. dazu FRA, Opinion IOP, 32.
1244 Art. 78 Abs. 9 IOP-Grenze-VO; Art. 74 Abs. 9 IOP-Polizei-VO.
1245 Siehe dazu Art. 20 Abs. 2 Eurodac-VO.
1246 Siehe dazu Art. 5 Abs. 2 VIS-Beschluss.
1247 Siehe dazu Art. 32 Abs. 4-5 EES-VO. Gemäss dieser Bestimmung darf die Abfrage zu Identifizierungszwecken nur mit biometrischen Daten erfolgen.
1248 Siehe dazu Art. 52 ETIAS-VO.
1249 FRA, biometrics, 66.

verfahren in Verbindung gebracht werden. Das Risiko von falschen Treffern ist bei einer Abfrage mit solchen Daten sehr hoch. Zudem erscheint die Nützlichkeit einer solchen Antwort für die abfragenden Behörden beschränkt.

e) Umsetzung in der Schweiz

In der Schweiz sind verschiedene Behörden i.S.v. Art. 22 EU-IOP-VO abfrageberechtigt. Dabei handelt es sich um verschiedene Abteilungen insbesondere von fedpol, dem NDB, der Bundesanwaltschaft, sowie die kantonalen Polizei- und Strafverfolgungsbehörden und die Polizeibehörden der Städte Zürich, Winterthur, Lausanne, Chiasso und Lugano.[1250] Diese Behörden haben bei der EZ fedpol einen Antrag auf Einsicht in die Daten zu stellen. Da fedpol auch als abfrageberechtigte Behörde aufgeführt ist, ist sicherzustellen, dass die EZ fedpol als Kontrollbehörde ihre Tätigkeit objektiv wahrnehmen kann und bei der Prüfung der Gesuche über die nötige Unabhängigkeit verfügt.[1251]

f) Bewertung

Die neue Regelung des Zugangs der nationalen Strafverfolgungsbehörden resp. Europol gemäss Art. 22 EU-IOP-VO mag zwar zu einer gewissen Vereinfachung resp. Vereinheitlichung des Verfahrens führen. Fraglich ist jedoch, ob diese Neuerung verhältnismässig ist.

Die Erforderlichkeit einer Erleichterung sowie einheitlichen Regelung des Verfahrens wurde in der Folgenabschätzung nur ungenügend begründet. Die erhobenen Statistiken zeigen, dass die Abfrage zu Zwecken der Verhinderung, Aufdeckung sowie Untersuchung terroristischer oder sonstiger schwerer Straftaten von den abfrageberechtigten Behörden eher restriktiv und sehr einseitig verwendet wird. Wieso nur sehr wenige Schengen/Dublin-Staaten bis anhin solche Abfragen vornehmen, ist unklar. Dass die Abfrage von gewissen Staaten häufig genutzt wird, zeigt jedoch, dass der Nutzen einer solchen Abfrage die teilweise hohen Zugangsbedingungen überwiegt. Die Tatsache, dass die Mehrheit der Schengen/Dublin-Staaten keinen resp. einen geringen Gebrauch von dieser Abfrage machen, muss nicht *per se* bedeuten, dass die Zugangsbedingungen zu hoch angesetzt sind. Insgesamt lässt sich aus den erhobenen Daten kein Bedarf einer Erleichterung resp. Vereinheitlichung der bisherigen Zugangsbedingungen ableiten.

1250 Botschaft IOP, 8033 f.

1251 Vgl. dazu VAVOULA, Right to Private Life, 263. Siehe dazu auch FRA, Opinion IOP, 31.

Zudem kann das in der Folgenabschätzung vorgebrachte Argument, dass mit den bisherigen Zugangsverfahren Verzögerungen verbunden sind, insofern entkräftet werden, als bereits in den bestehenden gesetzlichen Grundlagen vorgesehen ist, dass in Ausnahmefällen die Überprüfung des Vorliegens der Zugriffsvoraussetzungen auch erst nach der Einsicht in die Daten erfolgen kann. Weiter können die gemäss dem Kaskadenmechanismus vorgeschriebenen Abfragen in anderen Systemen – zumindest teilweise – auch innert kurzer Frist vorgenommen werden. Die Erforderlichkeit einer Erleichterung sowie einheitlichen Regelung des bestehenden Verfahrens für den Zugang der nationalen Strafverfolgungsbehörden sowie Europol zum VIS, Eurodac, EES und ETIAS ist somit nicht ausreichend begründet.

Die Erleichterung sowie Vereinheitlichung der Abfrage der nationalen Strafverfolgungsbehörden sowie Europol wirkt sich zudem auf die Funktion des Kaskadenmechanismus aus. Diese Sicherheitsmassnahme wurde eingesetzt, um der besonderen Sensibilität der Daten Ausdruck zu verleihen. Das Erfordernis der Kaskaden-Abfragen wird durch die Interoperabilität auf die zweite Zugangsstufe verschoben. Da die abfragende Behörde bereits bei der ersten Zugangsstufe in Erfahrung bringen kann, dass Daten vorhanden sind, stellt sich die Frage, ob der effektive Zugang zu den Daten von der unabhängigen Kontrollstelle verwehrt werden würde, sollte bei einer Kaskaden-Abfrage ein Treffer erfolgen. Unter der Berücksichtigung, dass die abfragende Behörde bereits weiss, dass für sie relevante Daten für die Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten in einem System vorhanden sind, ist dies zweifelhaft. Dadurch wird nicht nur die Unabhängigkeit und Objektivität der Kontrollstelle in Frage gestellt, sondern auch das effektive Vorhandensein einer Kontrollbehörde als solche.[1252] Ob der Kaskadenmechanismus zukünftig seine Funktion noch zu erfüllen vermag, bleibt fraglich. Da in der Folgenabschätzung insbesondere die Kaskaden-Abfragen kritisiert wurden, ist auch denkbar, dass diese Sicherheitsmassnahme früher oder später aus den gesetzlichen Grundlagen von Eurodac und dem EES entfernt wird.[1253]

In der – neu erst auf der zweiten Stufe stattfindenden Kontrolle – prüft die zuständige Behörde das Vorliegen der Voraussetzungen gemäss den gesetzlichen Grundlagen des betroffenen Systems. Die Zugangsbedingungen, welche vorliegen müssen, um eine Abfrage im CIR vorzunehmen, werden nicht sepa-

1252 Siehe dazu VAVOULA, IOP Privacy.

1253 Bezüglich Eurodac wurde mittlerweile eine entsprechende Anpassung der gesetzlichen Grundlage vorgenommen. Siehe dazu Kapitel III.5.7.

rat überprüft. Nicht restlos geklärt ist, ob es sich bei den Zugangsbedingungen der ersten und zweiten Zugangsstufe, abgesehen von einer allfälligen Kaskaden-Abfrage, um dieselben Kriterien handelt. Zumindest grösstenteils dürften diese deckungsgleich sein.

Der Rechtsprechung ist zu entnehmen, dass verschiedene Gerichte eine vorgängige Kontrolle des Vorliegens der Zugriffsvoraussetzungen als wichtige Sicherheitsmassnahme gegen Missbrauch werten.[1254] Wohl um die fehlende Kontrolle der Zugangsbedingungen auf der ersten Zugangsstufe auszugleichen, wurde festgelegt, dass die bei einer Abfrage des CIR erlangten Informationen nur für die Beantragung des effektiven Zugangs zu den Daten benutzt werden dürfen. Eine Nichtbeantragung ist zudem zu begründen. Dieser Regelung fehlt es jedoch an Durchsetzungskraft. Zwar ist eine Kontrolle der Verfahren und Bedingungen von Art. 22 Abs. 1-2 EU-IOP-VO vorgesehen. Es werden jedoch keine Einzelheiten dazu festgehalten (insbesondere wie sichergestellt werden kann, dass eine Nichtbeantragung begründet wird sowie die Überprüfung des Inhalts dieser Begründung). Zudem fehlen abschreckende Sanktionen bei Missbrauchsfällen. Aufgrund dessen besteht die Gefahr, dass durch die Interoperabilität der Zugang zu Datenbanken aus dem Migrationsbereich zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten insbesondere auch wegen den mangelnden Sanktionen zu routinemässigen Abfragen des CIR führen wird.[1255]

Insgesamt bewirkt die erleichterte und einheitliche Regelung der Zugangsbedingungen eine Herabsetzung der bestehenden Sicherheitsmassnahmen. Da die einer Abfrage des CIR zugrunde liegenden Daten grundsätzlich nicht in Verbindung mit kriminellen Aktivitäten stehen und auch bereits die Gewährung des Zugangs der nationalen Strafverfolgungsbehörden sowie Europol zu solchen Daten nur mangelhaft begründet und letztlich nur aufgrund von mehr oder weniger strengen Zugangsbedingungen gewährleistet wurde, erscheint dies nicht zumutbar.[1256]

Eine Erleichterung sowie Vereinheitlichung der Abfrage hätte, wenn überhaupt, eine beschränktere Datenbearbeitung resp. höhere Sicherheitsmassnahmen vorsehen sollen. Eine Beschränkung der Datenbearbeitung hätte bspw. darin bestehen können, dass sich der Zugang nicht systematisch auf alle

1254 Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 62; EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 120. Siehe dazu auch BGE 140 I 381, E. 4.5.

1255 Vgl. dazu VAVOULA, Assessment, 175.

1256 Vgl. dazu FRA, Opinion IOP, 30; VAVOULA, Assessment, 146 f.

in Eurodac, VIS, EES und ETIAS gespeicherten Daten erstreckt. Die Daten von sog. Bona-fide-Reisenden, also Drittstaatsangehörigen mit niedrigem Risikoprofil, hätten für solche Abfragen gesperrt werden können.[1257] Nur die Daten von speziell gefährlichen Personen hätten entsprechend markiert und somit für eine Abfrage durch die nationalen Strafverfolgungsbehörden resp. Europol zugelassen werden können.[1258] Auch hätte in Betracht gezogen werden können, nur die von einer roten Verknüpfung betroffenen Daten für eine solche Abfrage zur Verfügung zu stellen.[1259] Eine rote Verknüpfung wird nur bei einem Identitätsbetrug erstellt. Da dies ein Indiz für ein kriminelles Verhalten darstellt, würde zumindest mehr Bezug zwischen diesen Daten und der Abfrage zu Zwecken der Verhinderung, Aufdeckung sowie Untersuchung terroristischer sowie sonstiger schwerer Straftaten vorliegen. Ein solcher fehlt regelmässig ganz zwischen den Daten von Bona-fide-Reisenden und dieser Abfrage.[1260]

3.4.4. Zugang zum CIR zwecks Identifizierung

In Art. 20 EU-IOP-VO sind zwei unterschiedliche Abfragemöglichkeiten des CIR zwecks Identifizierung vorgesehen. Einerseits können Polizeibehörden zwecks Identifizierung einer Person bei einer Polizeikontrolle eine solche Abfrage vornehmen, sofern bestimmte Voraussetzungen erfüllt sind. Andererseits können Polizeibehörden in Fällen einer Naturkatastrophe, eines Unfalls oder eines Terroranschlags zur Identifizierung von unbekannten Personen, welche sich nicht ausweisen können, resp. nicht identifizierbarer menschlicher Überreste den CIR abfragen.[1261]

Für die folgenden Ausführungen wird die erstgenannte Variante als Abfragemöglichkeit 1 und die letztgenannte Variante als Abfragemöglichkeit 2 bezeichnet.

1257 Siehe zum Begriff der Bona-fide-Reisenden EUROPÄISCHE KOMMISSION, COM(2016) 602 final, 3.

1258 Es hätten objektive Kriterien festgelegt werden müssen, um zu bestimmen, welche Personen speziell gefährlich sind.

1259 VAVOULA, Assessment, 163 ff.

1260 Dieser fehlende Bezug bemängelte der EuGH auch bezüglich den auf Vorrat gespeicherten Verkehrsdaten für Strafverfolgungszwecke. Siehe dazu EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 58; EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 105.

1261 Siehe zu diesen beiden Abfragemöglichkeiten Kapitel IV.5.3.3.1.

3.4.4.1 *Geeignetheit*

Der CIR bezweckt die korrekte Identifizierung der im EES, VIS, ETIAS, Eurodac und ECRIS-TCN erfassten Personen gemäss Art. 20 EU-IOP-VO. Diese Bestimmung sieht zwei Abfragemöglichkeiten des CIR vor, welche die Schengen/Dublin-Staaten ihren nationalen Polizeibehörden gewähren können.[1262]

Bei der Abfragemöglichkeit 1 ist explizit festgehalten, dass die bei den Polizeikontrollen vorgenommenen Identifizierungen entweder auf die Verhinderung und Bekämpfung illegaler Einwanderung abzielen müssen oder ein hohes Mass an Sicherheit in der Union verfolgen müssen. Dies schliesst die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie den Schutz der inneren Sicherheit im Hoheitsgebiet der Schengen/Dublin-Staaten ein. Die «*genaueren Zwecke*» von solchen Abfragen sind im nationalen Recht aufzuführen.[1263]

Grundsätzlich ist es also möglich, dass bei einer solchen Polizeikontrolle Personen, welche keine gültige Aufenthaltsbewilligung (mehr) besitzen oder Personen, welche im Zusammenhang mit einer Straftat stehen, identifiziert werden können. Die Abfragemöglichkeit 1 ist demnach geeignet, das öffentliche Interesse der Wahrung der inneren Sicherheit zu unterstützen. Auch kann damit zu einer wirksamen Umsetzung der Asyl- und Visapolitik beigetragen werden.[1264] Diese Abfragemöglichkeit ist also geeignet, verschiedene öffentliche Interessen zu verfolgen.

Bei der Abfragemöglichkeit 2 ist die Identifizierung von unbekannten Personen, welche sich nicht ausweisen können, resp. von menschlichen Überresten im Zusammenhang mit Unfällen, Naturkatastrophen sowie Terroranschlägen vorgesehen. Diese Regelung im EU-Recht lässt, wie bereits vorne aufgeführt, den Zweck dieser Abfragemöglichkeit nicht klar erkennen. Die Vermutung liegt jedoch nahe, dass damit die Identifizierung von Opfern beabsichtigt ist.[1265] Es ist davon auszugehen, dass die Gesellschaft ein Interesse daran hat, dass Opfer von solchen Ereignissen identifiziert werden können.[1266] Zudem hat der Staat auch eine Untersuchungspflicht, wenn der Verdacht besteht, dass eine

1262 Siehe dazu Art. 17 Abs. 1 EU-IOP-VO.

1263 Siehe dazu Art. 20 Abs. 5 EU-IOP-VO. Auf die Problematik dieser vagen Regelung des Zwecks wurde bereits in den Ausführungen zum Kerngehalt eingegangen. Siehe dazu Kapitel V.3.3.

1264 Siehe zum öffentlichen Interesse der Interoperabilität Kapitel V.3.2.

1265 Siehe dazu Kapitel V.3.3.

1266 Siehe zu diesem Verständnis BUNDESRAT, Botschaft IOP, 8008.

Person rechtswidrig ums Leben gekommen ist.[1267] Insofern dürften mit der Abfragemöglichkeit 2 gemäss dieser Interpretation insbesondere die Gewährung von Rechten Dritter verfolgt werden.

Aufgrund der Formulierung im EU-Recht ist die Abfragemöglichkeit 2 jedoch nicht explizit auf die Identifizierung von Opfer solcher Ereignisse begrenzt. Insbesondere bei Terroranschlägen könnten grundsätzlich auch allfällige Täter identifiziert werden. Dies wäre dann insbesondere im Zusammenhang mit einem allfälligen strafrechtlichen Verfahren gewinnbringend und würde letztlich auf die Verfolgung der Wahrung der inneren Sicherheit abzielen.[1268] Zudem ist die Abfrage auch bei unbekannten Personen, welche sich nicht ausweisen können, zugelassen. In welchem Bezug diese Personen zu den genannten Ereignissen stehen müssen, ist nicht klar. Dabei könnte es sich um wichtige Zeugen solcher Ereignisse handeln. Deren Aussagen könnten entscheidend sein, um den Ablauf des entsprechenden Ereignisses zu rekonstruieren. Dadurch könnte – wie die Identifizierung von möglichen Opfern – zur Erstellung der Faktenlage eines Ereignisses beigetragen werden.

Diese Mutmassungen zeigen, dass es durchaus möglich ist, dass mit der Abfragemöglichkeit 2 ein öffentliches Interesse verfolgt wird. Aus der Regelung im EU-Recht geht jedoch nicht klar hervor, was der EU-Gesetzgeber mit dieser Abfragemöglichkeit genau bezweckt und welche öffentlichen Interessen damit verfolgt werden sollen. Die folgenden Ausführungen zeigen auf, dass dadurch die weitere Prüfung von Art. 20 EU-IOP-VO erschwert, wenn nicht sogar verunmöglicht, wird.[1269]

3.4.4.2 *Erforderlichkeit*

In der Folgenabschätzung wurde ausgeführt, dass es für die zuständigen Behörden schwierig sei, Identitätskontrollen auf dem Hoheitsgebiet der Schengen/Dublin-Staaten durchzuführen. Solche Kontrollen würden einen Hauptbestandteil der Polizeitätigkeit darstellen. Bei diesen Identitätskontrollen gehe es in einem ersten Schritt darum, die Person zu identifizieren. Ohne richtige Identifizierung der Personen sei es schwierig, Handlungen oder Entscheidungen vorzunehmen. Diese seien wiederum von grundlegender Bedeutung für

1267 Dies ergibt sich u.a. aus Art. 10 Abs. 1 BV. Siehe dazu Heri, in: Onlinekommentar BV (Version: 07.03.2025), Art. 10 BV N 36 ff. m.w.H.

1268 Siehe zum Verhältnis zur Abfrage des CIR gemäss Art. 22 EU-IOP-VO Kapitel V.3.4.4.3.e).

1269 Vgl. dazu auch BGE 146 I 11, E. 3.3.2, wonach es nicht möglich sei, ein öffentliches Interesse zu bestimmen resp. die Verhältnismässigkeit der Massnahme zu beurteilen, da die gesetzliche Grundlage «*alle denkbaren Verwendungszwecke*» einschliesse.

die innere Sicherheit, den Beitrag für die Verhütung von irregulärer Migration oder die Gewährung von Asyl. Bezüglich EU-BürgerInnen sowie in der EU wohnhaften Personen seien bereits entsprechende Register vorhanden, auf welche – sofern gesetzlich vorgesehen – für die Identifizierung zugegriffen werden dürfe. Für sich kurzzeitig in der EU aufhaltende Drittstaatsangehörige seien hingegen keine solche Register vorhanden, da diese Personen über unterschiedliche Schengen/Dublin-Staaten ein- und ausreisen könnten.[1270]

Sofern nicht mit der Aufklärung von schwerwiegender Kriminalität oder dem Migrationsmanagement verbunden, sei der Zugang der Behörden zu den Systemen für die Identifizierung von Drittstaatsangehörigen, welche sich nicht ausweisen können oder wollen, bis anhin sehr limitiert. Damit werde es den Schengen/Dublin-Staaten erschwert, Identitätsbetrug in ihrem Hoheitsgebiet zu entdecken und zu bekämpfen. Für die Identifizierung von Personen, welche sich nicht ausweisen können, seien die bereits bestehenden Zugriffsrechte nicht ausreichend, da die Identifizierungen nicht immer mit dem Migrationsmanagement im Zusammenhang stünden oder die Voraussetzungen für eine Abfrage des VIS, Eurodac, EES und ETIAS zu Strafverfolgungszwecken nicht gegeben seien. Es solle deshalb auch möglich sein, solche Identifizierungen im Rahmen der Polizeikompetenzen, welche im nationalen Recht definiert werden, durchzuführen. Damit werde das Ziel verfolgt, dass die zuständige Behörde die Person mit ihrem Namen ansprechen könne.[1271]

Es mag zwar zutreffen, dass betreffend Drittstaatsangehörige mit kurzfristigem Aufenthalt keine Möglichkeit zur Abfrage in einer Datenbank besteht. Dieser Umstand kann aber für sich allein noch keine Erforderlichkeit einer neuen Abfrage begründen. Nur weil mit dem CIR eine solche Datenbank geschaffen wird, rechtfertigt sich dadurch nicht *per se*, dass deshalb auch zwecks Identifikation von Personen auf die darin gespeicherten Daten zugegriffen werden darf. Auch nicht, wenn diese Daten für die Polizeibehörden hilfreich sein könnten.[1272]

Zur Problematik, dass Drittstaatsangehörige bei Kontrollen nicht identifiziert werden können, sind keine Statistiken resp. Belege vorgebracht worden, welche eine Erforderlichkeit der Abfragemöglichkeit 1 untermauern würden. Auch ist nicht belegt, was die Folgen sind, wenn die Polizeibehörden eine Person nicht identifizieren können resp. was sich mit dieser Abfragemöglichkeit we-

1270 European Commission, Impact assessment IOP Part 1, 39.
1271 European Commission, Impact assessment IOP Part 1, 24.
1272 Vgl. dazu WP29, Opinion proposals IOP, 11.

sentlich verbessern würde. Der Bedarf einer solchen Abfrage ist also nicht erstellt, weshalb auch dessen Erforderlichkeit kritisch zu hinterfragen ist.

Davon abgesehen bezieht sich die in der Folgenabschätzung aufgeführte Begründung lediglich auf die Abfragemöglichkeit 1. Da die Abfragemöglichkeit 2 in den Vorschlägen der EU-IOP-VO noch nicht vorgesehen war, ist dies nicht weiter erstaunlich.[1273] Es ist deshalb aber unklar, aus welchen Gründen diese Abfragemöglichkeit eingeführt wurde. Es fehlen Hinweise zur Erforderlichkeit einer solchen Abfragemöglichkeit. Insbesondere weil sich aus dem EU-Recht nicht eindeutig erschliesst, was mit dieser Abfragemöglichkeit beabsichtigt wird, kann die Erforderlichkeit der Abfragemöglichkeit 2 nicht beurteilt werden.

Die dürftige resp. nicht vorhandene Begründung der Erforderlichkeit der beiden in Art. 20 EU-IOP-VO vorgesehenen Abfragemöglichkeiten erscheint insgesamt nicht überzeugend.

3.4.4.3 *Zumutbarkeit*

a) Zugangsbedingungen

Die Abfragemöglichkeit 1 darf grundsätzlich für die Verhinderung sowie Bekämpfung illegaler Einwanderung und die Gewährleistung eines hohen Masses an Sicherheit vorgenommen werden, wobei der genaue Zweck der Abfrage im nationalen Recht näher zu definieren ist.[1274]

Abgesehen davon wird diese Abfragemöglichkeit auf bestimmte Fälle reduziert. Eine Abfrage darf nämlich nur vorgenommen werden, wenn eine Person nicht kooperieren kann (sie versteht nicht, was verlangt wird) und sich nicht ausweisen kann, wenn sie die Kooperation verweigert oder wenn berechtigte und begründete Zweifel bestehen, dass die vorgelegten Dokumente gefälscht sind oder die Person falsche Angaben zu ihrer Person macht.[1275] Eine Identitätskontrolle soll also wie bis anhin primär so ablaufen, dass die Person ihre Identität anhand eines Personalausweises oder eines anderen gültigen Dokuments beweisen kann.[1276]

1273 Siehe dazu Europäische Kommission, Vorschlag IOP-Grenze, 54; Europäische Kommission, Vorschlag IOP-Polizei, 54.

1274 Art. 20 Abs. 5 EU-IOP-VO.

1275 Art. 20 Abs. 1 EU-IOP-VO.

1276 Vgl. dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 45 f.

Bei der Abfragemöglichkeit 1 sind primär biometrische Daten zu verwenden. Diese müssen direkt vor Ort erhoben werden, «*sofern das Verfahren im Beisein der betroffenen Person eingeleitet*» wurde. Können die biometrischen Daten nicht verwendet werden oder ist eine entsprechende Abfrage nicht erfolgreich, darf die Abfrage auch mit den Identitätsdaten der Person zusammen mit den Reisedokumentdaten oder anhand der von der betroffenen Person bereitgestellten Identitätsdaten vorgenommen werden. Bei Kindern unter zwölf Jahren darf keine Abfrage vorgenommen werden, ausser wenn dies im Sinne des Kindeswohls ist.[1277]

Für die Identifizierung einer Person ist die Verwendung von biometrischen Daten grundsätzlich geeigneter, da diese Daten einzigartig sind und damit die Gefahr von falschen Treffern minimiert werden kann. Bei der Verwendung alphanumerischer Daten ist zu berücksichtigen, dass – anders als bei den biometrischen Daten – mehrere Abfrageergebnisse angezeigt werden könnten, da z.B. viele Personen denselben oder zumindest einen ähnlichen Namen verwenden. Folglich besteht eine erhöhte Gefahr von falschen Treffern.[1278] Dies dürfte insbesondere bei einer Abfrage zutreffen, welche mit den von der Person selbst bereitgestellten Identitätsdaten durchgeführt wird. In Anbetracht möglicher negativer Konsequenzen für falsch identifizierte Personen, erscheint es zur Identifizierung gerechtfertigt, die sensiblen biometrischen Daten den weniger sensiblen alphanumerischen Daten grundsätzlich vorzuziehen.

Ergibt die Abfrage einen Treffer in einem System, wird der abfragenden Behörde nicht mitgeteilt, in welchem System bereits Daten zu dieser Person erfasst sind.[1279] Aber auch ohne diese Angabe ist es möglich, dass die abfrageberechtigten Behörden darauf schliessen können. So kann aus der Angabe der Staatsangehörigkeit eines Staates, aus welchem bekanntermassen viele Personen fliehen, z.B. geschlossen werden, dass es sich um eine asylsuchende Person handeln könnte.[1280]

Des Weiteren haben die Schengen/Dublin-Staaten bei der Umsetzung im nationalen Recht zu «*berücksichtigen*», dass jede Diskriminierung von Drittstaatsangehörigen zu vermeiden ist.[1281] Der EU-Gesetzgeber scheint sich demnach dem

1277 Siehe dazu Art. 20 Abs. 1-3 EU-IOP-VO.
1278 Siehe dazu FRA, Opinion IOP, 28.
1279 Art. 18 Abs. 1 EU-IOP-VO.
1280 Siehe dazu FRA, Opinion IOP, 27.
1281 Siehe dazu Art. 20 Abs. 5 EU-IOP-VO. Die FRA hatte darauf aufmerksam gemacht, dass auch wegen des undefinierten Zwecks solcher Abfragen die Gefahr von Diskriminierungen

Risiko von diskriminierenden Praktiken bei Polizeikontrollen bewusst gewesen zu sein. Es besteht die Gefahr, dass die Kontrollen rein aufgrund des äusseren Erscheinungsbildes der betroffenen Person vorgenommen werden könnten, unabhängig von einem Verdachtsmoment. Es ist zwar zu begrüssen, dass mit der Regelung in den EU-IOP-VO versucht wurde, dieser Gefahr zu begegnen. Aufgrund der gewählten Formulierung erscheint es jedoch fraglich, ob die Schengen/Dublin-Staaten sich dieser Thematik wirklich ernsthaft annehmen werden.[1282]

Durch die aufgeführten Zugangsbedingungen wird die Abfragemöglichkeit 1 insofern begrenzt, als dass sie keine systematischen Abfragen zulässt, sondern eine Abfrage nur in bestimmten Situationen und unter bestimmten Voraussetzungen vorgenommen werden darf.

Die Abfragemöglichkeit 2 beschränkt sich auf die Abfrage von unbekannten Personen, welche sich nicht ausweisen können, resp. auf unidentifizierte sterbliche Überreste. Die Abfrage darf zudem – im Unterschied zur Abfragemöglichkeit 1 – nur mit biometrischen Daten vorgenommen werden.[1283] Diese Beschränkung ergibt sich bei der Identifizierung sterblicher Überreste bereits aus den Umständen. Die unbekannten Personen, welche sich nicht ausweisen können, könnten jedoch grundsätzlich Angaben zur Identität machen, die (auch) für die Abfrage verwendet werden könnten.

b) Weitere Sicherheitsmassnahmen

Als weitere Sicherheitsmassnahme ist bei beiden Abfragemöglichkeiten eine Protokollierungspflicht vorgeschrieben, welche sich sowohl an eu-LISA als auch an die Schengen/Dublin-Staaten richtet. Während die von eu-LISA angefertigten Protokolle bestimmte Angaben zu umfassen haben, ist dies bei den von den Schengen/Dublin-Staaten zu erstellenden Protokollen nicht näher definiert.[1284] Es wäre jedoch wichtig, dass auch die von den Schengen-Dublin/Staaten zu erstellenden Protokolle dieselben Angaben umfassen, wie diejenigen Protokolle von eu-LISA. Insbesondere weil diese Protokolle zur daten-

aufgrund der ethnischen Herkunft oder der Staatsangehörigkeit bestehe. Siehe dazu FRA, Opinion IOP, 27.

1282 Siehe dazu VAVOULA, Deathblow, 147. In der Schweiz wurden z.B. keine entsprechenden Regelungen dazu aufgenommen. Siehe dazu Kapitel V.3.4.4.3.d).

1283 Art. 20 Abs. 4 EU-IOP-VO.

1284 Siehe dazu Art. 24 Abs. 2 und Abs. 5 EU-IOP-VO. Die FRA empfahl zudem, dass auch der Ort der Abfrage sowie die Angabe, ob eine Person mehrmals kontrolliert wurde, zu erfassen sei. Je mehr Informationen protokolliert werden, desto eher kann die Kontrollbehörde darüber entscheiden, ob solche Kontrollen an bestimmten Orten oder bezüglich bestimmter Individuen missbräuchlich angewendet werden. Siehe dazu FRA, Opinion IOP, 28.

schutzrechtlichen Kontrolle verwendet werden, muss sichergestellt werden, dass zumindest gewisse Mindestangaben vorhanden sind. Ansonsten besteht die Gefahr, dass die Kontrolle nicht wirksam ausgeübt werden kann, da die notwendigen Informationen nicht erhoben wurden.[1285]

Anders als bei den Abfragen des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten müssen weder die Schengen/Dublin-Staaten noch Europol Jahresberichte über den Zugang des CIR zwecks Identifizierung verfassen. Im Hinblick auf die Vermeidung einer missbräuchlichen Verwendung durch Polizeibehörden wäre die Erhebung bestimmter Angaben zur Verwendung dieser Abfragemöglichkeiten des CIR jedoch wichtig. So müssten z.B. Informationen und Statistiken zum genauen Zweck der Abfrage, der Anzahl der Abfragen aufgeteilt nach Abfragen mit biometrischen Daten, Daten aus Reisedokumenten sowie Identitätsdaten, sowie die Anzahl und Art der Fälle, in welchen eine Person erfolgreich identifiziert werden konnte, erhoben werden.[1286]

c) (Weitere) Konkretisierungen im nationalen Recht

Beide Abfragemöglichkeiten sind fakultativer Natur, d.h. die Schengen/Dublin-Staaten sind nicht verpflichtet, eine entsprechende Zugriffsmöglichkeit im nationalen Recht vorzusehen. Wollen sie davon Gebrauch machen, sind verschiedene Aspekte dieser Verfahren im nationalen Recht zu regeln.[1287]

Für die Abfragemöglichkeit 1 müssen u.a. die «*genaueren Zwecke*», welche im Rahmen der Verhinderung und Bekämpfung der illegalen Einwanderung und der Gewährleistung eines hohen Masses an Sicherheit angesiedelt sein müssen, im nationalen Recht näher festgelegt werden. Bereits bei den Ausführungen zum Kerngehalt hat sich gezeigt, dass dadurch nicht wirklich eine Begrenzung vorgenommen wird.[1288] Zudem bedürfen auch die «*Verfahren, Be-*

1285 Siehe zur datenschutzrechtlichen Kontrolle Art. 24 Abs. 7 EU-IOP-VO. Siehe Art. 40 Abs. 4 EU-IOP-VO zum Zugang zu diesen Protokollen.

1286 Siehe dazu FRA, Opinion IOP, 57.

1287 Siehe dazu Art. 20 Abs. 4-5 EU-IOP-VO.

1288 Siehe dazu auch BGE 146 I 11, E. 3.3.2, wonach eine allgemeine Umschreibung der Aufgaben der Polizei zwar durchaus ein öffentliches Interesse darstellen kann. Diese Ziele vermögen die fragliche Massnahme jedoch nicht hinreichend zu bestimmen, da «*sie auf unterschiedlichen Ebenen liegen*» und jedes für sich betrachtet nach entsprechenden Anforderungen, Ausgestaltungen sowie Begrenzungen verlangt. Zudem ist auch zu berücksichtigen, dass eine Polizeikontrolle stets auf einen Grund zurückgeführt werden muss und somit nicht wahllos erfolgen darf (z.B. weist die kontrollierte Person Ähnlichkeiten mit einer gesuchten Person auf). Siehe dazu BGE 109 Ia 146, E. 4b.

dingungen sowie Kriterien» solcher Polizeikontrollen einer näheren Umschreibung im nationalen Recht. Ausserdem sind die abfrageberechtigten Behörden im nationalen Recht zu benennen.[1289] Den Schengen/Dublin-Staaten wird also ein umfangreicher Ermessensspielraum zur Ausgestaltung dieser Abfragemöglichkeit zugestanden. Da sich die Regelung im EU-Recht auf die Festlegung einiger weniger Bedingungen sowie Sicherheitsmassnahmen beschränkt, stellt sich die Frage, ob das EU-Recht im Sinne der Rechtsprechung zum Grundrecht auf Datenschutz genügend klare und präzise Regeln vorsieht.

Mit einer ebenfalls eher vagen Regelung im Bereich der Vorratsdatenspeicherung hatte sich der EuGH in verschiedenen Urteilen bereits auseinandergesetzt. Diese Regelung verpflichtete die Betreiber elektronischer Kommunikationsdienste spezifische Daten während eines definierten Zeitraums zu speichern, damit diese bei Bedarf von bestimmten Behörden zwecks Bekämpfung schwerer Straftaten eingesehen werden konnten. Im Urteil *Digital Rights* hat der EuGH festgehalten, dass es der EU-Gesetzgeber versäumt habe, in der fraglichen Richtlinie materiell-verfahrensrechtliche Voraussetzungen zur Zugriffsberechtigung der Behörden festzulegen. Es sei vielmehr den Mitgliedstaaten überlassen worden, die Verfahren und die Bedingungen gemäss den Anforderungen der Notwendigkeit und der Verhältnismässigkeit festzulegen. Letztlich sei kein objektives Kriterium vorgesehen, um die Datenbearbeitung *in casu* auf das absolut Notwendige zu beschränken.[1290] Auch im später ergangenen Urteil *Tele2* führte der EuGH aus, dass sich die nationale Gesetzgebung bei der Festlegung der Umstände und Voraussetzungen auf objektive Kriterien abzustützen habe, gemäss welchen die entsprechenden nationalen Behörden auf die Daten zugreifen dürften.[1291] Es müssten klare und präzise Regeln über die Tragweite und die Anwendung der Datenbearbeitung vorgesehen und Mindesterfordernisse betreffend ausreichende Garantien für den Schutz vor Missbrauch für die Betroffenen definiert werden.[1292] Auch der EGMR hatte bereits in verschiedenen Urteilen eine pauschale und undifferenzierte Regelung, welcher es zudem auch an Sicherheitsmassnahmen fehlte, kritisiert und eine Verletzung von Art. 8 EMRK bejaht.[1293]

1289 Siehe dazu Art. 20 Abs. 5 EU-IOP-VO.

1290 EuGH, Urteil v. 08.04.2014, *Digital Rights Ireland und Seitlinger u.a.*, ECLI:EU:C:2014:238, Rz. 61 f. Die fragliche Richtlinie wurde letztlich für ungültig erklärt (Rz. 73).

1291 EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 119. Siehe dazu auch FRA, biometrics, 59 f.

1292 EuGH, Urteil v. 21.12.2016, *Tele2 Sverige*, ECLI:EU:C:2016:970, Rz. 109.

1293 Siehe dazu EGMR, Urteil v. 16.02.2000, *Amann v. Switzerland*, Beschwerde Nr. 27798/95, Rz. 76 ff.; EGMR, Urteil v. 02.08.1984, *Malone v. The United Kingdom*, Beschwerde Nr. 8691/79, Rz. 67 ff. In diesen Urteilen prüfte der EGMR das Vorliegen der klaren und präzisen

Ähnlich wie bei der zitierten Rechtsprechung ist es bei der Abfragemöglichkeit 1 zumindest zu einem grossen Teil den Schengen/Dublin-Staaten überlassen, die Verfahren und Bedingungen dieser Abfrage im nationalen Recht (näher) festzulegen. Auch wenn im EU-Recht einige Beschränkungen sowie Sicherheitsmassnahmen aufgeführt werden, verbleibt den Schengen/Dublin-Staaten ein (zu) grosser Ermessensspielraum bei der Ausgestaltung dieser Abfrage. Dass die abfrageberechtigten Behörden im nationalen Recht aufzuführen sind, erscheint hingegen sachgemäss, da die Behörden je nach Schengen/Dublin-Staat anders aufgebaut sind.[1294]

Abgesehen von den Verfahren, Bedingungen und Kriterien solcher Abfragen ist zudem auch der genauere Zweck im nationalen Recht zu bestimmen. Wie bereits ausgeführt, vermögen es auch die übergeordneten Begriffe, im Rahmen welcher die Abfragen zu erfolgen haben, nicht, den Zweck klar zu begrenzen.[1295] Da es der EU-Gesetzgeber bei der Abfragemöglichkeit 1 versäumt hat, die genaueren Zwecke der Abfrage festzulegen und es grösstenteils den Schengen/Dublin-Staaten überlassen hat, die Verfahren, Kriterien sowie Bedingungen zu regeln, erscheint diese Abfragemöglichkeit nicht auf das absolut Notwendige beschränkt. Es fehlt an klaren und präzisen Regeln zur Datenbearbeitung sowie der Festlegung von ausreichenden Sicherheitsmassnahmen.

Bei der Abfragemöglichkeit 2 haben die Schengen/Dublin-Staaten ebenfalls die Verfahren, Bedingungen sowie die Kriterien festzulegen, sofern sie diese Abfragemöglichkeit nutzen wollen.[1296] Dem EU-Recht sind kaum Konkretisierungen zu dieser Abfragemöglichkeit zu entnehmen. Wie sich zudem bereits gezeigt hat, ist aus der EU-Regelung nicht eindeutig erkennbar, was mit dieser Abfragemöglichkeit bezweckt wird. Weder werden – wie bei der Abfragemöglichkeit 1 – bestimmte übergeordnete Begriffe definiert, in dessen Rahmen die Abfragen zu erfolgen haben, noch ergibt sich aus dem EU-Recht, dass der Zweck der Abfrage

Regeln beim Kriterium der gesetzlichen Grundlage. Siehe in Kapitel II.7.3, dass diese Kriterien von den Gerichten teilweise bei der gesetzlichen Grundlage und teilweise bei der Verhältnismässigkeit geprüft werden.

1294 Auch die Strafverfolgungsbehörden, welche auf die Systeme VIS, Eurodac, EES und ETIAS zugreifen dürfen, sind im nationalen Recht zu benennen. Siehe dazu Kapitel III.5.5.2; III.6.5.2; III.7.5.2 sowie III.8.5.3. Siehe zur Benennung der Behörden auch EuGH, Gutachten 1/15, 26.7.2017, ECLI:EU:C:2017:592, Rz. 183, wonach Kanada der Kommission vor dem Inkrafttreten des Abkommens die zuständigen kanadischen Behörden mitzuteilen hat. Dies wurde vom EuGH als hinreichend klar und präzise befunden. Vgl. zu einer Bewertung der Abfragemöglichkeit 1 auch WP29, Opinion proposals IOP, 12; FRA, Opinion IOP, 26 ff.; EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 40 ff.

1295 Siehe dazu Kapitel V.3.3.

1296 Art. 20 Abs. 6 EU-IOP-VO.

im nationalen Recht zu definieren ist.[1297] Insofern erscheint auch bei der Abfragemöglichkeit 2 keine Beschränkung auf das absolut Notwendige vorgenommen worden zu sein. Es fehlt auch bei dieser Abfragemöglichkeit an klaren und präzisen Regeln der Datenbearbeitung, insbesondere an der Festlegung eines Zwecks sowie ausreichenden Sicherheitsmassnahmen.[1298]

Obwohl sich bereits aus dieser Feststellung ergibt, dass die beiden Abfragemöglichkeiten des CIR zwecks Identifizierung gemäss Art. 20 EU-IOP-VO nicht verhältnismässig sind, werden im Folgenden noch einige Ausführungen zu weiteren Aspekten dieser beiden Abfragemöglichkeiten gemacht.

d) Eignung der Daten für die Abfrage

Die beiden Abfragemöglichkeiten gemäss Art. 20 EU-IOP-VO zielen auf die Identifizierung einer Person ab. Eine Identifizierung kann nur korrekt vorgenommenen werden, wenn die Daten, anhand welcher die Identifizierung erfolgen soll, ebenfalls korrekt sind. Damit das Ziel von Art. 20 EU-IOP-VO erreicht werden kann, ist es von zentraler Bedeutung, dass die Daten eine gewisse Qualität aufweisen. Wie sich bereits gezeigt hat, können diverse Faktoren die Datenqualität negativ beeinflussen. So kann sich bspw. die Art und Weise der Erhebung der Daten auf die Qualität der Daten auswirken.[1299]

Die alphanumerischen Daten, welche im CIR gespeichert werden und folglich gemäss den gesetzlichen Grundlagen des VIS, EES, ETIAS, ECRIS-TCN und Eurodac erfasst wurden, werden auf unterschiedliche Art und Weise erhoben. Bei Eurodac, dem VIS und dem EES werden die Daten von BeamtInnen erhoben.[1300] Die im ECRIS-TCN gespeicherten Daten basieren hingegen auf Daten, welche im Rahmen eines administrativen resp. gerichtlichen Verfahrens erhoben wurden.[1301] Bei ETIAS wiederum werden die Daten in der Regel von der antragstellenden Person selbst angegeben.[1302]

1297 Siehe dazu Art. 20 Abs. 6 EU-IOP-VO. Siehe zum öffentlichen Interesse Kapitel V.3.2.

1298 Siehe dazu zudem BGE 146 I 11, E. 3.3.2, wonach das *in casu* fragliche kantonale Polizeigesetz keine hinreichende gesetzliche Grundlage darstellte, weil sich bei den Verwendungszwecken verschiedene Unklarheiten ergaben. Siehe zu nicht ausreichenden Sicherheitsmassnahmen einer kantonalen Bestimmung eines Polizeigesetzes auch BGE 140 I 353, E. 8.7 ff.

1299 Siehe zur Thematik der Datenqualität Kapitel IV.5.4.2.

1300 Siehe dazu Kapitel III.5.4; III.6.4 und III.7.4.

1301 Siehe dazu Kapitel III.4.4 und III.9.4.

1302 Siehe dazu Kapitel III.8.4. Es ist jedoch auch vorgesehen, dass eine Person für eine andere einen Antrag stellen kann.

Aufgrund der Art der Erhebung dürfte es sich bei den ETIAS-Daten um die unzuverlässigsten Daten handeln. Denn diese werden in der Regel von der betroffenen Person selbst, also ohne Kontrolle durch eine Drittperson, angegeben. Dies erleichtert es, absichtlich falsche Angaben zu machen. Zudem ist die betroffene Person, anders als z.B. BeamtInnen, nicht hinsichtlich der Erhebung der Daten geschult. Es dürften deshalb vermehrt Flüchtigkeitsfehler oder sonstige (geläufige) Fehler bei der Dateneingabe auftreten.[1303]

Bei der Datenerhebung durch BeamtInnen dürften solche Fehler grundsätzlich weniger häufig auftreten. Es kann jedoch eine Rolle spielen, auf welcher Grundlage die Erhebung der Daten durch die BeamtInnen erfolgt. Werden die Daten z.B. einem offiziellen Reisedokument entnommen, dürften die Daten grundsätzlich zuverlässiger sein, als wenn die erfassten Daten auf Äusserungen der betroffenen Person beruhen. Denn auch die geschulten BeamtInnen können nicht vermeiden, dass die Person, deren Daten erhoben werden sollen, (absichtlich) falsche Angaben macht.

Am zuverlässigsten dürften diejenigen Daten sein, die im Zusammenhang mit einem administrativen resp. gerichtlichen Verfahren erhoben wurden. Bei der Erhebung der Daten in solchen Verfahren haben diverse Personen, insbesondere auch die betroffene Person, mitgewirkt. Die Wahrscheinlichkeit ist deshalb gross, dass allfällige Fehler entdeckt worden wären.

Aufgrund dieser Ausführungen ergibt sich, dass sich ETIAS-Daten für die Abfragemöglichkeiten gemäss Art. 20 EU-IOP-VO grundsätzlich nicht eignen. Einerseits weil diese Abfragen primär resp. ausschliesslich anhand biometrischer Daten vorgenommen werden müssen und in ETIAS keine solche Daten gespeichert sind. Andererseits weil die in ETIAS gespeicherten alphanumerischen Daten in der Regel von der gesuchstellenden Person selbst deklariert werden. Sie sind deshalb grundsätzlich fehleranfälliger als von BeamtInnen erhobenen Daten.

Auch die Nützlichkeit von Eurodac-Daten für die Vornahme von Identifizierungen ist in Zweifel zu ziehen. Denn bis anhin werden in diesem Informationssystem primär Fingerabdruckdaten, jedoch keine Angaben zu den Personalien erfasst.[1304] Ergibt sich also bei einer Abfrage gemäss Art. 20 EU-IOP-VO ein Treffer mit Eurodac-Daten, kann die Person dadurch nicht identifiziert werden, da deren Personalien im System nicht erfasst sind.[1305]

1303 Vgl. dazu FRA, Opinion IOP, 37 f.

1304 Siehe dazu Kapitel III.5.4.

1305 Neu sollen jedoch auch alphanumerische Daten (wie z.B. der Vor- und Nachname) in Eurodac gespeichert werden. Siehe dazu Art. 17, 19, 21 ff. VO 2024/1358.

e) Umsetzung in der Schweiz

Die beiden Abfragemöglichkeiten gemäss Art. 20 EU-IOP-VO sind fakultativer Natur. Die Schweiz möchte davon Gebrauch machen und hat deshalb entsprechendes nationales Recht geschaffen.[1306] Diese Bestimmungen sind noch nicht in Kraft gesetzt worden.[1307]

Die Abfragemöglichkeit 1 darf in der Schweiz für die Zwecke der Verhütung und Bekämpfung illegaler Einwanderung, zum Schutz der öffentlichen Sicherheit und Ordnung sowie zur Wahrung der inneren Sicherheit vorgenommen werden.[1308] Diese Begriffe sind fast identisch mit denjenigen, welche im EU-Recht verwendet werden. Diese übergeordneten Begriffe hätten jedoch im nationalen Recht genauer definiert werden sollen.[1309] Eine genauere Festlegung der mit der Abfragemöglichkeit 1 verfolgten Zwecke ist in der Schweiz – zumindest auf Gesetzesstufe – somit nicht erfolgt.[1310]

Davon abgesehen fehlen in den schweizerischen Gesetzesgrundlagen auch detaillierte Regelungen zu den Verfahren, Bedingungen und Kriterien, welche gemäss dem EU-Recht im nationalen Recht festzulegen wären. Die Regelung in der Schweiz verweist diesbezüglich lediglich auf Art. 20 Abs. 1 EU-IOP-VO und wiederholt, dass die Abfrage primär anhand von biometrischen Daten, welche der betroffenen Person vor Ort abzunehmen sind, zu erfolgen hat.[1311] Davon abgesehen fehlen auch Regelungen, welche Diskriminierungen vorbeugen sollen.[1312] Der schweizerische Gesetzgeber hat es demnach weitgehend versäumt, die gemäss dem EU-Recht notwendigen Präzisierungen vorzunehmen. Vielmehr wiederholt das nationale Recht den sich aus dem EU-Recht ergebenden Inhalt oder verweist auf diesen.

Einzig dem Erfordernis der Benennung der abfrageberechtigten Behörden ist der schweizerische Gesetzgeber nachgekommen. Verschiedene Abteilungen von fedpol, die Polizeibehörden der Kantone und Gemeinden sowie die Eidgenössische Zollverwaltung (EZV) sind im Rahmen ihrer zollrechtlichen und nicht zollrechtlichen Aufgaben zum Schutz der Bevölkerung und zur Wahrung

---

1306 Siehe dazu auch BUNDESRAT, Botschaft IOP, 8032.

1307 Der Bundesrat bestimmt den Zeitpunkt des Inkrafttretens. Siehe dazu Art. 3 Abs. 2 Bundesbeschluss IOP.

1308 Siehe dazu Art. 110b Abs. 2 E-AIG.

1309 Art. 20 Abs. 5 EU-IOP-VO.

1310 Vgl. dazu auch SFH, Vernehmlassungsantwort, 8.

1311 Art. 110b Abs. 1 Bst. a und Abs. 4 E-AIG.

1312 Gemäss Art. 20 Abs. 5 EU-IOP-VO haben die Schengen/Dublin-Staaten zu berücksichtigen, dass jede Diskriminierung von Drittstaatsangehörigen zu vermeiden ist.

der inneren Sicherheit zur Abfrage berechtigt. Dieselben Behörden dürfen in der Schweiz auch Abfragen gemäss der Abfragemöglichkeit 2 durchführen.[1313]

Bei der Abfragemöglichkeit 2 fällt auf, dass diese Abfrage gemäss dem nationalen Recht der Schweiz bei Unfällen, Naturkatastrophen sowie «*Gewalttaten*» ermöglicht werden soll.[1314] Dies entspricht insofern nicht dem EU-Recht, als dass dieses die Abfrage nur bei Terroranschlägen und nicht bei Gewalttaten vorsieht.[1315] Der Begriff des Terroranschlags ist deutlich enger gefasst als jener der Gewalttaten. Da in den Materialien der Begriff Terroranschlag und nicht Gewalttaten verwendet wird, könnte dies darauf hindeuten, dass es sich dabei um einen redaktionellen Fehler handelt.[1316] Gemäss der aktuellen Wortwahl im nationalen Recht der Schweiz ist der Anwendungsbereich der Abfragemöglichkeit 2 deutlich weiter gefasst als im EU-Recht vorgesehen.

Abgesehen davon sind in der Schweiz auch bei der Abfragemöglichkeit 2 keine Konkretisierungen des Verfahrens, der Bedingungen und der Kriterien vorgenommen worden, welchen es gemäss dem EU-Recht bedurft hätte.[1317]

Insgesamt zeigt sich, dass die Schweiz den im EU-Recht zur Abfrage des CIR zwecks Identifizierung geforderten Konkretisierungen nicht nachgekommen ist. Hinzu kommt, dass die nationale Regelung zur Abfragemöglichkeit 2 einen grösseren Anwendungsbereich vorsieht, als dies im EU-Recht vorgesehen ist. Die Umsetzung von Art. 20 EU-IOP-VO in der Schweiz erscheint vor diesem Hintergrund misslungen.

f) Abgrenzung zu Art. 22 EU-IOP-VO

Ein Vergleich der berechtigten Behörden in der Schweiz, welche Abfragen gemäss Art. 20 EU-IOP-VO und Art. 22 EU-IOP-VO vornehmen dürfen, zeigt, dass es in der Schweiz gewisse Stellen gibt, welche sowohl als Polizeibehörden i.S.v. Art. 20 EU-IOP-VO als auch als nationale Strafverfolgungsbehörden i.S.v. Art. 22 EU-IOP-VO den CIR abfragen dürfen. Dies sind bestimmte Organisationseinheiten von fedpol sowie die Polizeibehörden der Kantone.[1318] Auch

1313 Art. 110b Abs. 3 E-AIG.

1314 Art. 110b Abs. 1 Bst. b E-AIG.

1315 Siehe dazu Art. 20 Abs. 4 EU-IOP-VO.

1316 Siehe dazu BUNDESRAT, Botschaft IOP, 8032.

1317 Art. 20 Abs. 6 EU-IOP-VO.

1318 Siehe dazu Art. 120b Abs. 3 lit. a und lit. b E-AIG; Art. 120d Abs. 2 lit. a und lit. d E-AIG. Diese Stellen werden auf Verordnungsebene noch genauer bestimmt. Zur N-IOP-Verordnung existiert lediglich ein Vorentwurf (siehe dazu Vorentwurf N-IOP-Verordnung). Gemäss Art. 10 Abs. 1 lit. a und Art. 12 Abs. 1 lit. a dieses Vorentwurfs sind folgende Stellen von

wenn im EU-Recht jeweils eine unterschiedliche Bezeichnung für die abfrageberechtigten Behörden verwendet wird, schliesst das EU-Recht nicht explizit aus, dass eine Behörde sowohl gemäss Art. 20 EU-IOP-VO als auch Art. 22 EU-IOP-VO Abfragen vornehmen darf.[1319]

Aufgrund der Tatsache, dass dieselbe Organisationseinheit sowohl Abfragen gemäss Art. 20 EU-IOP-VO und Art. 22 EU-IOP-VO vornehmen darf, stellt sich die Frage nach dem Verhältnis resp. der Abgrenzung dieser beiden Abfragen. Da die Abfragen unterschiedliche Zugangsbedingungen vorsehen, muss sichergestellt werden, dass einer doppelt berechtigten Behörde keine Wahlmöglichkeit zukommt, da sonst stets die Abfrage mit den milderen Zugangsbedingungen gewählt werden dürfte.

Die Anwendungsbereiche der Abfragen gemäss Art. 20 EU-IOP-VO und Art. 22 EU-IOP-VO sind grösstenteils unterschiedlich. Eine Überschneidung der Anwendungsbereiche dieser beiden Bestimmungen könnte jedoch im Bereich der Abfragemöglichkeit 2 in Fällen von Terroranschlägen sowie der in Art. 22 EU-IOP-VO vorgesehenen Abfrage des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung von terroristischen Straftaten vorliegen. Da ein Terroranschlag zweifelsfrei eine terroristische Straftat darstellt, stellt sich die Frage nach dem Verhältnis dieser beiden Abfragen. Da der genaue Zweck der Abfragemöglichkeit 2 in Fällen von Terroranschlägen nicht eindeutig feststellbar ist, lässt sich dieses Verhältnis nicht abschliessend beurteilen. Dennoch sollen die nachfolgenden Ausführungen helfen, das Verhältnis dieser beiden Abfragen besser zu verstehen.

Die Abfragemöglichkeit 2 kann u.a. in Fällen von Terroranschlägen durch Polizeibehörden vorgenommen werden, um unbekannte Personen, welche sich nicht ausweisen können, oder nicht identifizierbare menschliche Überreste zu identifizieren. Obwohl dies nicht explizit aus dem Wortlaut hervorgeht, ist aufgrund einer grammatikalischen Auslegung dieser Bestimmung davon auszugehen, dass die zu identifizierende Person – wie auch bei der Abfragemöglichkeit 1 – vor Ort anwesend ist resp. die menschlichen Überreste am Tatort vorhanden sind. Die Abfrage erfolgt ausschliesslich anhand von biometrischen

---

fedpol sowohl bezüglich der Abfrage gemäss Art. 20 EU-IOP-VO sowie Art. 22 EU-IOP-VO abfrageberechtigt: die Bundeskriminalpolizei, die für die Bearbeitung biometrischer erkennungsdienstlicher Daten zuständigen Stellen sowie die Einsatz- und Alarmzentrale.

1319 In Art. 20 EU-IOP-VO wird der Begriff «*Polizeibehörde*» verwendet. In Art. 22 EU-IOP-VO sind die «*benannten Behörden*» abfrageberechtigt. Anstelle des letztgenannten Begriffs wird in der vorliegenden Untersuchung der Begriff «*nationale Strafverfolgungsbehörden*» verwendet.

Daten. Sie kann von der berechtigten Polizeibehörde im CIR vorgenommen werden. Es handelt sich also um ein direktes Abfragerecht. Die Angabe, aus welchem System die Daten stammen, bleibt den Polizeibehörden bei einem Treffer verwehrt.[1320]

Bei der Abfrage gemäss Art. 22 EU-IOP-VO steht nicht die Identifizierung einer Person im Fokus. Dennoch ist anzunehmen, dass diese Abfrage zumindest auch dazu dient, Verdächtige, Täter oder Opfer zu identifizieren.[1321] Eine Eingrenzung, dass solche Personen vor Ort anwesend sei müssen, ergibt sich aus dem EU-Recht nicht. Der den nationalen Strafverfolgungsbehörden sowie Europol zugestandene Zugriff auf Daten aus Eurodac, VIS, EES und ETIAS erfolgt in einem zweistufigen Verfahren, wobei verschiedene Bedingungen vorliegen müssen. Der effektive Zugriff auf die Daten muss von der abfrageberechtigten Behörde bei der unabhängigen Kontrollstelle beantragt werden. Kann das Vorliegen der benötigten Zugangsbedingungen bejaht werden, erfolgt die Einsicht in die Daten. Es handelt sich insofern um ein indirektes Abfragerecht. Die Abfrage kann mit biometrischen als auch anderen Daten erfolgen. Des Weiteren steht die Abfragemöglichkeit gemäss Art. 22 EU-IOP-VO – im Unterschied zu Art. 20 Abs. 4 EU-IOP-VO – zwingend im Zusammenhang mit Ermittlungen für ein strafrechtliches Verfahren resp. der Verhinderung von u.a. terroristischen Straftaten.

Es sind also Unterschiede in Bezug auf die Zugangsbedingungen sowie das Ergebnis der Abfrage feststellbar. Aufgrund der inhaltlichen Nähe der beiden Abfragen stellt sich jedoch die Frage, ob diese stets klar voneinander abgegrenzt werden können oder ob es Situationen gibt, in welchen sich die Anwendungsbereiche der beiden Abfragen überlappen könnten.

Angenommen es werden nicht identifizierbare menschliche Überreste an einem Tatort eines Terroranschlags gefunden. Im Zuge dieses Ereignisses werden strafrechtliche Ermittlungen aufgenommen. Unabhängig davon, ob es sich bei den menschlichen Überresten um ein Opfer oder den vermeintlichen Täter handelt, dürfte die Identifizierung von diesen Überresten für das aufgenom-

1320 Art. 20 Abs. 4 EU-IOP-VO; Art. 9 Abs. 4 UAbs. 2 EU-IOP-VO.

1321 Europäische Kommission, Vorschlag IOP-Grenze, 36; Europäische Kommission, Vorschlag IOP-Polizei, 35. Jeweils ErwG. 34 war explizit zu entnehmen, dass das zweistufige Datenabfragesystem vor allem in Fällen sinnvoll sei, «*in denen der Verdächtige, der Täter oder das mutmassliche Opfer einer terroristischen oder sonstigen schweren Straftat unbekannt*» sei. Diese Aussage findet sich zwar in den EU-IOP-VO nicht mehr. Es ist daraus aber dennoch zu schliessen, dass auch der Zugang gemäss Art. 22 EU-IOP-VO insbesondere Identifizierungszwecken dienen soll.

mene Strafverfahren von Bedeutung sein. In dieser Konstellation käme eine Abfrage gemäss Art. 22 EU-IOP-VO in Frage, da in diesem Einzelfall davon ausgegangen werden darf, dass vernünftige Gründe vorliegen, dass die Identifizierung der Überreste zur Aufdeckung resp. Untersuchung einer terroristischer Straftat beitragen kann.[1322] Gleichzeitig dürfte jedoch auch die Abfrage gemäss Art. 20 Abs. 4 EU-IOP-VO möglich sein, da menschliche Überreste im Zusammenhang mit einem Terroranschlag identifiziert werden müssen.[1323] Ist eine Behörde berechtigt, beide Abfragen durchzuführen, dürfte sie sich in dieser Konstellation für die Abfragemöglichkeit 2 entscheiden, da die Zugangsbedingungen weniger hoch sind, dieselben Systeme abgefragt werden und bei einem Treffer direkt auf die Daten zugegriffen werden darf. Dass bei dieser Abfrage bei einem Treffer nicht angegeben wird, aus welchem System die Daten stammen, dürfte dabei von untergeordneter Bedeutung sein.

Ebenfalls zu einer Wahlmöglichkeit könnte es in folgender Situation kommen: Der vermeintliche Täter eines Terroranschlags wird gefasst. Da diese Person sich nicht ausweisen kann resp. wohl auch nicht will, ist ihre Identität unbekannt. Es wird ein Strafverfahren eingeleitet, in welchem der Identifizierung der gefassten Person eine wesentliche Bedeutung beizumessen ist. Auch in dieser Konstellation dürften beide Abfragen grundsätzlich in Frage kommen.

Diese Beispiele zeigen auf, dass sich in bestimmten Situationen Überschneidungen der beiden Abfragen ergeben können. Ist eine Behörde berechtigt, beide Abfragen vorzunehmen, kommt ihr eine Wahlmöglichkeit zu. Dies ist zu vermeiden, da so die strengen Voraussetzungen von Art. 22 EU-IOP-VO umgangen werden können. Um dies zu vermeiden, hätten die beiden Abfragemöglichkeiten klar voneinander abgegrenzt werden müssen. So hätte z.B. explizit festgehalten werden können, dass eine Behörde nicht gleichzeitig hinsichtlich der Abfrage gemäss Art. 20 EU-IOP-VO sowie 22 EU-IOP-VO abfrageberechtigt sein darf. Die unterschiedliche Bezeichnung der abfrageberechtigten Behörden (also Polizeibehörden sowie benannte Behörden) scheint dies – wie das Beispiel der Umsetzung in der Schweiz anschaulich darstellt – nicht klar festzuhalten. Davon abgesehen hätte auch der Anwendungsbereich der beiden Abfragen klarer getrennt werden können. So hätte z.B. bei der Abfrage von Art. 20 Abs. 4 EU-IOP-VO klar festgehalten werden können, dass

1322 Siehe dazu die Zugangsbedingungen gemäss Art. 22 Abs. 1 EU-IOP-VO.

1323 Siehe dazu Art. 20 Abs. 4 EU-IOP-VO, wobei jedoch zu berücksichtigen ist, dass im nationalen Recht allfällige weitere Bedingungen verlangt werden. Siehe zum Erfordernis der näheren Festlegung der Verfahren, Bedingungen sowie Kriterien Art. 20 Abs. 6 EU-IOP-VO.

es dabei nicht um die Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten gehen darf. Eine klare Abgrenzung von Art. 20 EU-IOP-VO und Art. 22 EU-IOP-VO hätte auch erreicht werden können, wenn die in Art. 20 Abs. 4 EU-IOP-VO aufgeführten Ereignisse auf Naturkatastrophen und Unfälle begrenzt worden wären.[1324]

g) Bewertung

Beim Zugang zum CIR zwecks Identifizierung handelt es sich um eine Zweckerweiterung. Die mit Art. 20 EU-IOP-VO vorgesehene Datenbearbeitung geht also über den bereits in den gesetzlichen Grundlagen der einzelnen Informationssysteme bisher festgelegten Zweck hinaus.[1325] Bei der Bewertung dieser Zweckerweiterung fallen verschiedene Faktoren ins Gewicht.

So wurde die Erforderlichkeit dieser beiden Abfragemöglichkeiten nicht überzeugend begründet. Die reine Nützlichkeit der Daten reicht dazu nicht aus. Es fehlt insoweit an statistischen Daten, welche einen Bedarf untermauern würden. Zudem war die Abfragemöglichkeit 2 noch nicht von Anfang an vorgesehen. Der Folgenabschätzung ist deshalb keine Begründung der Erforderlichkeit der Abfragemöglichkeit 2 zu entnehmen.

Beide Abfragemöglichkeiten bezwecken die Identifizierung von Personen resp. von nicht identifizierten menschlichen Überresten. Eine Identifizierung darf jedoch keinen Selbstzweck darstellen. Mit einer Identifizierung muss immer auch etwas beabsichtigt werden.[1326] Nur dadurch lässt sich der Zweck erkennen. Dies wird anhand der vorliegenden Abfragemöglichkeiten deutlich. So wird insbesondere bei der Abfragemöglichkeit 2 der Zweck der Identifizierung nicht näher ausgeführt. Es können demnach nur Mutmassungen angestellt werden, um zu ergründen, zu welchem konkreten Zweck die Identifi-

1324 Wobei in gewissen Einzelfällen sich erst im Rahmen der Ermittlungen zeigen könnte, ob es sich bei einem Ereignis um einen Unfall oder einen Terroranschlag handelt.

1325 Der mit Art. 20 EU-IOP-VO verfolgte Zweck wurde den gesetzlichen Grundlagen der betroffenen Informationssysteme hinzugefügt. Ausser bei Eurodac. Aufgrund der bevorstehenden Revision der Eurodac-VO fehlen in den EU-IOP-VO konkrete Verweise auf Bestimmungen dieser Verordnung. Siehe dazu BUNDESRAT, Botschaft IOP, 8002 f. Siehe bezüglich den anderen Systemen Art. 58 Ziff. 1 IOP-Grenze-VO; Art. 60 Ziff. 1 und Ziff. 3 IOP-Grenze-VO; Art. 61 Ziff. 1 und Ziff. 3 IOP-Grenze-VO; Art. 61 Ziff. 2 und Ziff. 12 IOP-Polizei-VO.

1326 Vgl. dazu auch der Zweck des MID. Dieser beschränkt sich schliesslich auch nicht auf die Aufdeckung von Mehrfachidentitäten, sondern legt weiter fest, mit welchem Ziel dies zu erfolgen hat, also damit Identitätskontrollen vereinfacht werden können und Identitätsbetrug entdeckt werden kann. Siehe zum MID Kapitel V.3.4.7.

zierung vorgenommen werden darf. Die Abfragemöglichkeit 1 sieht gewisse übergeordnete Begriffe (Verhinderung und Bekämpfung der illegalen Einwanderung resp. der Gewährleistung eines hohen Masses an Sicherheit) als Zielrichtung vor, im Rahmen welcher die Identifizierungen zu erfolgen haben und im nationalen Recht näher auszuführen sind. Diese übergeordneten Begriffe sind jedoch derart weit gefasst, dass sich die gesamte Polizeitätigkeit darunter subsumieren lassen dürfte. Ein konkretes Ziel der Identifizierung wird durch das EU-Recht dadurch nicht vorgegeben.[1327]

Zudem wird es – abgesehen von wenigen Begrenzungen der Datenbearbeitung – mehrheitlich den Schengen/Dublin-Staaten überlassen, die Verfahren und Bedingungen dieser Abfragemöglichkeiten näher festzulegen. Durch diesen grossen Ermessensspielraum ist es den Schengen/Dublin-Staaten möglich, sehr unterschiedliche Regelungen dazu im nationalen Recht zu erlassen. Damit kann kein einheitliches Schutzniveau gewährleistet werden. Die Regelung im EU-Recht ist sehr vage und nennt keine objektiven Kriterien, anhand welcher die Datenbearbeitung zu beschränken und auf das absolut Notwendige zu reduzieren ist. Es fehlt an klaren und präzisen Regeln der Datenbearbeitung sowie an der Festlegung von ausreichenden Sicherheitsmassnahmen. Die beiden Abfragemöglichkeiten sind demnach nicht zumutbar.

Die Umsetzung von Art. 20 EU-IOP-VO in der Schweiz zeigt zudem, was auch in anderen Schengen-Staaten passieren könnte. Obwohl das EU-Recht dies vorsieht, werden keine Konkretisierungen der Verfahren, Kriterien oder Bedingungen der beiden Abfragemöglichkeiten auf nationaler Ebene vorgenommen. Abgesehen von der Benennung der zugriffsberechtigten Behörden wird im nationalen Recht der Schweiz lediglich wiederholt, was schon aus dem EU-Recht hervorgeht. Insbesondere wurde der Zweck der Abfragemöglichkeit 1 nicht genauer definiert. Somit darf diese Abfrage in der Schweiz bei der gesamten Polizeitätigkeit verwendet werden.

Ausserdem zeigt sich am Beispiel der Schweiz, dass es in bestimmten Situationen zu Überlappungen der Anwendungsbereiche der Abfrage des CIR gemäss Art. 22 EU-IOP-VO und der Abfragemöglichkeit 2 in Fällen von Terroranschlägen kommen kann. Haben bestimmte Organisationseinheiten Zugriff auf beide Abfragen, hat dies zur Folge, dass in bestimmten Situationen die strengen Zugangsbedingungen von Art. 22 EU-IOP-VO umgangen werden können.

[1327] Dies könnte allenfalls sogar eine Verletzung des Kerngehalts darstellen. Siehe dazu Kapitel V.3.3.

Um dies zu verhindern, hätte im EU-Recht eine klarere Abgrenzung dieser beiden Abfragen vorgenommen werden müssen.

Im Allgemeinen fällt zudem auf, dass Art. 22 EU-IOP-VO lediglich eine indirekte Abfragemöglichkeit für die nationalen Strafverfolgungsbehörden resp. Europol vorsieht. Bei Art. 20 EU-IOP-VO darf von den Polizeibehörden jedoch direkt auf den CIR zugegriffen werden. Es ist nicht ersichtlich, weshalb die Polizeibehörden unter weniger strengen Voraussetzungen Zugriff auf die Systeme erhalten sollten als die nationalen Strafverfolgungsbehörden.[1328] Die strengen Voraussetzungen bei der Abfrage der nationalen Strafverfolgungsbehörden sowie Europol wurden schliesslich vorgesehen, um den Zugriff auf Systeme aus dem Migrationsbereich zu rechtfertigen. Vor diesem Hintergrund erscheint es nicht nachvollziehbar, weshalb Strafverfolgungs- und Polizeibehörden unterschiedlich behandelt werden.

3.4.5. Zugang zum CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten

In Art. 21 EU-IOP-VO ist festgehalten, dass die für die manuelle Verifizierung zuständige Behörde ausschliesslich für Verifizierungszwecke auf die von einer gelben Verknüpfung betroffenen Daten zugreifen kann. Auf die von einer roten Verknüpfung betroffenen Daten dürfen diejenigen Behörden – ausschliesslich zur Bekämpfung von Identitätsbetrug – zugreifen, welche für mindestens eines der von dieser Verknüpfung betroffenen Systeme oder das SIS abfrageberechtigt sind.

Es ist zwar grundsätzlich möglich, dass eine mit einer gelben resp. roten Verknüpfung konfrontierte Behörde gemäss ihren Zugriffsrechten bereits auf alle der miteinander verknüpften Datensets zugreifen kann. Falls dem aber nicht so ist, erhalten diese Behörden Einsicht in Daten, auf welche sie gemäss den gesetzlichen Grundlagen der einzelnen Systeme nicht zugreifen dürften.

Beim Zugang zum CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten handelt es sich also um eine Erweiterung der bestehenden Zugriffsberechtigungen, da bestimmte Behörden bei Vorliegen einer gelben resp. einer roten Verknüpfung auf Daten zugreifen können, auf welche sie – gemäss ihren bisherigen Zugriffsrechten – keinen Zugriff hätten.

1328 Der Grund dafür könnte sich in den Diskussionen der HLEG ergeben haben. Die Gruppe hatte dort offenbar die Ansicht vertreten, dass Abfragen von Strafverfolgungsbehörden zu Identifikationszwecken keiner vorgängigen Genehmigung bedürfen sollten. Siehe dazu HLEG, final report, 14.

3.4.5.1 *Geeignetheit*

Mit dem Zugang zum CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten gemäss Art. 21 EU-IOP-VO ist – wohl zumindest grösstenteils – eine Erweiterung der bisherigen Zugriffsberechtigungen verbunden. Indem die Behörden zu bestimmten Zwecken auf die von einer gelben resp. roten Verknüpfung verbundenen Datensets zugreifen können, wird das Funktionieren des MID unterstützt.[1329]

Der MID bezweckt die Aufdeckung von Mehrfachidentitäten, wobei dadurch Identitätsprüfungen vereinfacht und Identitätsbetrug bekämpft werden sollen. Damit wird zu einem wirksamen Management der Aussengrenzen des Schengen-Raums sowie der Gewährleistung der inneren Sicherheit beigetragen. Die Geeignetheit dürfte insofern vorliegen, da diese Abfrage die Verfolgung verschiedener öffentlicher Interessen fördert.[1330]

3.4.5.2 *Erforderlichkeit*

In der Folgenabschätzung sind zu dieser Abfrage des CIR – anders als bei den anderen beiden Abfragen des CIR – keine Ausführungen zur Erforderlichkeit zu finden. Dies dürfte darauf zurückzuführen sein, dass sich das Bedürfnis nach einer entsprechenden Erweiterung der Zugriffsrechte erst im Verlauf der Entstehung der Interoperabilität ergeben hat. Schliesslich war auch der MID, dessen Funktionieren mit Art. 21 EU-IOP-VO unterstützt werden soll, nicht von Anfang an vorgesehen.[1331]

Die vom MID erstellten Verknüpfungen zwischen den im CIR und im SIS gespeicherten Daten können zwar mögliche Mehrfachidentitäten aufdecken. Sie vermögen aber nicht Identitätsprüfungen zu vereinfachen und Identitätsbetrug zu bekämpfen. Um dies zu erreichen, mussten neue Zugriffsrechte geschaffen werden.

So benötigen einerseits die Behörden, welche eine manuelle Verifizierung vornehmen müssen, Zugriff auf alle von einer gelben Verknüpfung betroffenen Datensets, damit sie ihre Aufgabe effektiv wahrnehmen können. Andererseits sind bei einer roten Verknüpfung entsprechende Massnahmen zwecks Bekämpfung von Identitätsbetrug vorzunehmen. Damit dem Folge geleistet werden kann, muss eine Behörde, welche auf eine solche rote Verknüpfung trifft,

1329 Siehe dazu Art. 17 Abs. 1 EU-IOP-VO.
1330 Siehe zu den öffentlichen Interessen Kapitel V.3.2.
1331 Siehe dazu Kapitel IV.4.

auf alle von dieser Verknüpfung betroffenen Datensets zugreifen können. Aus diesen Bedürfnissen ergibt sich die Erforderlichkeit der neuen Zugriffsrechte gemäss Art. 21 EU-IOP-VO.

3.4.5.3 *Zumutbarkeit*

a) Zugangsbedingungen

Die Abfrage des CIR zwecks Aufdeckung etwaiger Mehrfachidentitäten ist für gewisse Behörden und zu bestimmten Zwecken vorgesehen. So darf die für die manuelle Verifizierung zuständige Behörde, ausschliesslich für die Vornahme dieser Aufgabe, auf die von einer gelben Verknüpfung betroffenen Datensets zugreifen. Eine Behörde, die gemäss ihren Zugriffsberechtigungen auf ein Datenset zugreifen darf, welches von einer roten Verknüpfung betroffen ist, darf – ausschliesslich für die Bekämpfung von Identitätsbetrug – auch auf die anderen von der Verknüpfung betroffenen Datensets zugreifen.

b) Verweis auf das System, aus dem die Daten stammen

Die für die manuelle Verifizierung zuständige Behörde erhält gemäss Art. 21 EU-IOP-VO Zugang zu dem resp. den jeweils anderen Datenset(s) einer gelben Verknüpfung, welche sie zu verifizieren hat. Nach der Überprüfung der gelben Verknüpfung hat die zuständige Behörde der Verknüpfung die dem Ergebnis der Überprüfung entsprechende Farbe zuzuordnen (grün, rot, weiss).[1332]

Der Zugriff auf die von der gelben Verknüpfung betroffenen Datensets umfasst auch die Angabe des Informationssystems, in welchem die Daten gespeichert sind.[1333] Diese Angabe kann den Entscheid betreffend die Farbkennzeichnung nach der manuellen Verifizierung möglicherweise beeinflussen. Dies ist insbesondere bei im ECRIS-TCN gespeicherten Daten denkbar. Anhand der Angabe, dass Daten in diesem System vorhanden sind, hat die für die manuelle Verifizierung zuständige Behörde bereits Kenntnis, dass eine strafrechtliche Verurteilung vorliegt. Diese Tatsache könnte dazu führen, dass bei Personen, deren Daten im ECRIS-TCN erfasst sind, viel eher der Verdacht auf Identitätsbetrug besteht und folglich eher eine rote Verknüpfung zwischen den betroffenen Datensets erstellt wird.[1334]

1332 Siehe dazu Kapitel IV.5.3.4. m.w.H. zur Bedeutung der verschiedenen Farben.
1333 Art. 21 Abs. 1 EU-IOP-VO.
1334 FRA, Opinion IOP, 38 f.

Wieso die zuständige Behörde Kenntnis haben muss, in welchem System die Daten gespeichert sind, um die manuelle Verifizierung vorzunehmen, ist nicht ersichtlich. Diese Angabe sollte deshalb der zuständigen Behörde nicht zugänglich gemacht werden.

c) Missbräuchliche Verwendung von erlangten Daten

Die Angabe, aus welchem Informationssystem die von einer gelben Verknüpfung betroffenen Daten stammen, vermag nicht nur den Entscheid betreffend die Farbkennzeichnung nach der manuellen Verifizierung zu beeinflussen. Auch die im Rahmen von Art. 21 EU-IOP-VO erlangten Daten können über den vorgesehenen Zweck hinaus verwendet werden. Der Zugriff gemäss Art. 21 EU-IOP-VO bei gelben resp. roten Verknüpfungen ist zwar nur für einen gewissen Zweck vorgesehen (Verifizierung resp. Bekämpfung von Identitätsbetrug). Dennoch scheint es – abgesehen von den zu erstellenden Protokollen – keine Kontrolle zu geben, ob die erlangten Daten nicht auch anderweitig verwendet werden.

Problematisch ist, dass es sich bei den zugriffsberechtigten Behörden um Stellen handelt, welche bereits Datenbearbeitungen im Rahmen der einzelnen Systeme vornehmen. Es betrifft eine Vielzahl von Behörden wie z.B. Migrationsbehörden oder das SIRENE-Büro.[1335] Diese Behörden üben eine bestimmte Tätigkeit aus und treffen in diesem Zusammenhang Entscheidungen. Die manuelle Verifizierung von gelben Verknüpfungen kommt zu dieser Haupttätigkeit hinzu. Dadurch entsteht die Gefahr, dass im Rahmen von Art. 21 EU-IOP-VO erlangte Informationen auch bei der Entscheidung betreffend die Haupttätigkeit der Behörden einfliessen. Insbesondere ECRIS-TCN-Daten könnten eine behördliche Entscheidung negativ beeinflussen.[1336]

Ein Beispiel soll dies näher veranschaulichen. Eine Person, deren Daten bereits im ECRIS-TCN gespeichert sind, beantragt ein Schengen-Visum. Bei der Bearbeitung des Antrags der betroffenen Person wird eine gelbe Verknüpfung mit den im ECRIS-TCN erfassten Daten erstellt. Die für die Bearbeitung des Visumantrags zuständige Person hat nun diese Verknüpfung zu verifizieren. Anschliessend muss sie über den Visumantrag befinden. Selbst wenn sich bei der manuellen Verifizierung herausstellen sollte, dass von keinem Identitätsbetrug auszugehen ist, so ist es dennoch möglich, dass die Tatsache, dass die

[1335] Siehe zur Festlegung der für die Verifizierung zuständigen Behörde Kapitel V.3.4.7.3.c).
[1336] Vgl. in diesem Sinne auch FRA, Opinion IOP, 38 f.

antragstellende Person bereits strafrechtlich verurteilt wurde, auf die Beurteilung des Visumantrags einen (negativen) Einfluss hat.

Trotz der Beschränkung der Bearbeitung der im Rahmen von Art. 21 EU-IOP-VO erlangten Daten für bestimmte Zwecke, dürfte es in der Praxis wohl schwierig sein, dies strikt einzuhalten, da die für die manuelle Verifizierung zuständigen Behörden auch Entscheidungen in anderen Bereichen treffen.

Um diese Gefahr der missbräuchlichen Verwendung dieser Daten zu minimieren, hätte sichergestellt werden müssen, dass die für die manuelle Verifizierung zuständige Behörde die erlangten Informationen nicht anderweitig verwenden kann. So hätte z.B. eine unabhängige dritte Stelle für die manuelle Verifizierung vorgesehen werden können. Eine solche Lösung hätte zudem den Vorteil gehabt, dass die manuelle Verifizierung einheitlicher vorgenommen werden würde.[1337]

d) Weitere Sicherheitsmassnahmen

Des Weiteren haben eu-LISA sowie die Schengen/Dublin-Staaten und die Stellen der Union über die gemäss Art. 21 EU-IOP-VO erfolgenden Datenbearbeitungsvorgänge Protokoll zu führen. Diese Protokolle dürfen zur datenschutzrechtlichen Kontrolle verwendet werden.[1338] Nur bei der Protokollierungspflicht von eu-LISA wurde explizit festgehalten, welche Angaben zu erfassen sind. Im Sinne der Einheitlichkeit sowie der Effizienz wäre es hilfreich gewesen, dies bei den Protokollierungspflichten sämtlicher Behörden festzuhalten.

e) Umsetzung in der Schweiz

In der Schweiz mussten im nationalen Recht insbesondere die Zugriffsberechtigungen der Abfrage des CIR zwecks Aufdeckung von Mehrfachidentitäten festgelegt werden. So ist zur Verifizierung der gelben Verknüpfungen im MID diejenige Behörde zuständig, welche eine Abfrage auslöst, indem sie ein Dossier erfasst oder Daten im C-VIS, EES oder ETIAS aktualisiert. Bei Ausschreibungen im SIS – ausser bei Einreiseverweigerungen – ist das SIRENE-Büro zuständig. Die EZV oder die kantonale Polizei nehmen Verifizierungen im Zusammenhang mit dem EES vor. Ist das C-VIS betroffen sind das SEM und wei-

1337 Siehe dazu Kapitel V.3.4.7.3.c).

1338 Siehe dazu Art. 24 Abs. 3, 5 und 7 EU-IOP-VO. Siehe Art. 40 Abs. 4 EU-IOP-VO zum Zugang zu diesen Protokollen.

tere Visa-Behörden zuständig. Bei Verknüpfungen des ETIAS ist das SEM zuständig.[1339]

Ausserdem wird eine zentrale MID-Expertenstelle (MES) errichtet, welche die manuellen Verifizierungen von MID-Verknüpfungen unterstützen soll. Diese soll sich aus dem Personal von Bundesämtern zusammensetzen, welche für die Verifizierungen von Verknüpfungen berechtigt sind. Die MES soll bei besonders komplexen Fällen zum Einsatz kommen. Sie stellt bei Bedarf das nötige Expertenwissen zur Verfügung.[1340] Eine solche Stelle ist im EU-Recht nicht vorgesehen. Die Errichtung einer solchen Stelle scheint nicht *per se* unvereinbar mit dem EU-Recht sein. Es muss jedoch sichergestellt werden, dass dafür keine Zugriffsberechtigungen benötigt werden, welche im EU-Recht nicht vorgesehen sind.

f) Bewertung

Mit Art. 21 EU-IOP-VO wird eine Erweiterung der bisherigen Zugriffsberechtigungen vorgenommen. Diese ist notwendig, weil gelbe Verknüpfungen überprüft werden müssen, wozu ein Zugriff auf alle von der Verknüpfung betroffenen Datensets notwendig ist. Auch bei einer roten Verknüpfung ist es angezeigt, dass zur Vornahme von Massnahmen zwecks Bekämpfung von Identitätsbetrug, die zuständige Behörde auf alle von der Verknüpfung betroffenen Datensets zugreifen darf.

Da für die zugriffsberechtigten Behörden ersichtlich ist, aus welchem System die von einer Verknüpfung betroffenen Daten stammen, besteht die Gefahr, dass diese Information auch bei Entscheidungen einfliessen, welche die betroffenen Behörden bei ihrer Haupttätigkeit üblicherweise treffen. In diesen Fällen ist zu beachten, dass die damit verbundenen Konsequenzen nicht abschätzbar sind. Insbesondere wenn die abfragende Behörde gemäss Art. 21 EU-IOP-VO üblicherweise Entscheide im Rahmen von ETIAS, VIS oder Eurodac trifft, dürften daraus Ablehnungen diverser Gesuche resultieren. Immerhin stehen den betroffenen Personen gewisse Rechte zu, mit welchen sie gegen solche ggf. nicht gerechtfertigten Ablehnungen vorgehen können.[1341]

Diese Gefahr hätte vermieden werden können, wenn die manuelle Verifizierung einer dritten Stelle übertragen worden wäre oder zumindest – in orga-

---

1339 Siehe dazu auch BUNDESRAT, Botschaft IOP, 8036, 8044; Art. 110d Abs. 1 E-AIG; Art. 16d Abs. 2 E-BPI.

1340 Siehe dazu BUNDESRAT, Botschaft IOP, 8036.

1341 Siehe zu diesen Rechten der betroffenen Personen Kapitel V.3.4.8.1.b).

nisatorischer Hinsicht – sichergestellt worden wäre, dass die für die manuelle Verifizierung zuständige Behörde nicht gleichzeitig auch andere Entscheidungen im Zusammenhang mit den betroffenen Informationssystemen trifft. Alternativ hätte darauf verzichtet werden können, den Behörden diese Angabe preiszugeben.

Das Risiko einer missbräuchlichen Verwendung von im Rahmen von Art. 21 EU-IOP-VO erlangten Daten hätte also durch verschiedene Massnahmen minimiert werden können. Je nach Wahl der Massnahme wäre dies mit mehr oder weniger grossem organisatorischen resp. regulatorischen Aufwand verbunden gewesen. Da der Verzicht auf die Angabe, aus welchem System die Daten stammen, die Abfrage gemäss Art. 21 EU-IOP-VO nur marginal verändert hätte, damit aber das Risiko einer missbräuchlichen Verwendung stark hätte vermindert werden können, wäre zumindest diese Alternative zumutbar gewesen. Insofern erscheint die aktuelle Regelung nicht verhältnismässig.

3.4.6. Gemeinsamer Speicher für Identitätsdaten

3.4.6.1 *Geeignetheit*

Durch die Schaffung des CIR werden die drei Abfragen gemäss Art. 20-22 EU-IOP-VO ermöglicht.[1342] Mit diesen Abfragen werden unterschiedliche öffentliche Interessen verfolgt, wobei insbesondere die Wahrung der inneren Sicherheit im Zentrum stehen dürfte.[1343] Der CIR ist also geeignet, zur Erreichung dieser öffentlichen Interessen beizutragen.[1344]

3.4.6.2 *Erforderlichkeit*

Als mildere Massnahme für die Schaffung des CIR hatte die WP29 die Einführung eines EU-Identitätsdokuments vorgeschlagen, welches biometrische Daten enthalten hätte und die Reisenden jeweils mit sich hätten tragen müssen.[1345] Aktuell werden die Daten in den bestehenden Systemen Eurodac, VIS und SIS insofern zentral gespeichert, als jedes System über einen eigenen Speicher verfügt. Die Einführung eines Ausweises, welcher die Identitätsan-

1342 Siehe dazu Art. 17 Abs. 1 EU-IOP-VO. In der Machbarkeitsstudie des CIR wurden verschiedene Varianten in Betracht gezogen. Siehe dazu EUROPEAN COMMISSION, Feasibility Study CIR.

1343 Siehe dazu Kapitel V.3.4.3.1; V.3.4.4.1 und V.3.4.5.1.

1344 Siehe zum öffentlichen Interesse der Interoperabilität Kapitel V.3.2.

1345 WP29, Opinion proposals IOP, 5 f.

gaben samt biometrischer Daten enthalten hätte, wäre zwar als dezentrale Speicherung, eine mildere Massnahme. Fraglich ist, ob damit die mit dem CIR verfolgten Zwecke hätten erreicht werden können. Da alle drei Abfragen des CIR systemübergreifend vorgenommen werden, ist davon auszugehen, dass es (technisch) notwendig ist, dass alle dafür verwendeten Daten in einem einzigen Speicher gespeichert werden.[1346] Folglich stellt ein solches EU-Identitätsdokument keine mildere Massnahme mit gleicher Wirkungsprognose dar.

Der CIR ist also erforderlich, da die für die systemübergreifenden Abfragen gemäss Art. 20-22 EU-IOP-VO verwendeten Daten an einem Ort gespeichert werden müssen. Ansonsten sind (aus technischer Perspektive) Abgleiche von Daten, welche in mehreren Systemen gespeichert sind, nicht möglich.[1347]

3.4.6.3 *Zumutbarkeit*

a) Umfang der gespeicherten Daten

Im CIR werden bestimmte alphanumerische sowie biometrische Daten gespeichert. Unter Berücksichtigung der Datenbearbeitungen, welche im Zusammenhang mit dem CIR vorgenommen werden, stellt sich die Frage, ob alle in Art. 18 Abs. 1 EU-IOP-VO aufgeführten Daten tatsächlich zu speichern sind.

Es fällt auf, dass die im CIR zu speichernden Daten umfassender sind als die Identitätsdaten, mit welchen die Prüfung auf Mehrfachidentitäten vorgenommen wird.[1348] So sind im CIR bspw. die Vornamen der Eltern der betroffenen Person zu erfassen. Diese Angaben werden nur bei ETIAS erhoben, weshalb mit solchen Daten keine systemübergreifende Abfrage vorgenommen werden kann. Zudem handelt es sich dabei auch um selbst deklarierte Angaben. Im Vergleich mit von BeamtInnen erhobenen Daten dürften diese fehleranfälliger sein.[1349] Die Vornamen der Eltern sollten demnach nicht im CIR gespeichert werden, da sie für die mit dem CIR verfolgten Zwecke nicht benötigt werden.

1346 Siehe zu diesen drei Abfragen des CIR Kapitel V.3.4.3; V.3.4.4 und V.3.4.5.

1347 Siehe dazu Kapitel IV.5.3.3.

1348 Siehe zu den Identitätsdaten Art. 4 Ziff. 8 EU-IOP-VO. Diese Problematik hatte bereits die FRA im Rahmen ihrer Stellungnahme zu den Vorschlägen der EU-IOP-VO vorgebracht. Siehe dazu FRA, Opinion IOP, 25.

1349 Siehe dazu Kapitel IV.5.4.2.2.

b) Erhöhtes Sicherheitsrisiko

Neben dem BMS und dem MID wird insbesondere mit dem CIR eine umfassende Datenbank geschaffen. Im CIR werden sowohl alphanumerische als auch biometrische Daten von allen Drittstaatsangehörigen erfasst, welche die EU-Grenzen bereits überschritten haben oder dies beabsichtigen. Dies betrifft Millionen von Personen. Hinzu kommt, dass insbesondere biometrische Daten sehr sensibel sind, da sie untrennbar und dauerhaft mit einer Person verknüpft sind. Aufgrund der Art der im CIR gespeicherten Daten dürfte das Interesse an diesen von unberechtigten Nutzern besonders gross sein. Eine unrechtmässige Verwendung der Daten im CIR könnte aufgrund der grossen Anzahl sowie der Art der gespeicherten Daten grundsätzlich vielen Personen einen (schweren) Schaden verursachen.[1350]

Der CIR dürfte also aufgrund seiner Grösse sowie der darin gespeicherten Daten ein grösseres Sicherheitsrisiko mit sich bringen, als wenn die Daten weiterhin separat in den einzelnen Informationssystemen gespeichert würden.

c) Sicherheitsmassnahmen

Fraglich erscheint, ob dem mit dem CIR einhergehenden erhöhten Risiko für die Datensicherheit mit angemessenen Schutzvorkehrungen begegnet werden kann. In den EU-IOP-VO finden sich verschiedene allgemeine Bestimmungen zur Datensicherheit. So haben verschiedene Stellen die erforderlichen Schutzmassnahmen zu ergreifen, damit die Sicherheit des CIR – sowie auch der anderen Interoperabilitätskomponenten – gewährleistet werden kann. Des Weiteren soll eine Meldepflicht bei Sicherheitsvorfällen sicherstellen, dass die richtigen Stellen informiert werden. Davon abgesehen wird die Sicherheit der Komponenten im Rahmen einer Berichterstattung evaluiert.[1351]

In den EU-IOP-VO werden also verschiedene Massnahmen ergriffen, um die Datensicherheit im Allgemeinen zu gewährleisten. Diese Schutzmassnahmen sind sicherlich zu begrüssen. Dennoch dürfte es stark darauf ankommen, welche konkreten Massnahmen für die Gewährleistung der Datensicherheit von den verschiedenen verantwortlichen Stellen ergriffen werden. Bei den Verantwortlichkeiten der Schengen/Dublin-Staaten ist zudem davon auszugehen,

---

1350 Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 27 ff.; BUNDESRAT, Botschaft IOP, 7995 ff.; WP29, Opinion proposals IOP, 19 f. Siehe zum Thema Datensicherheit auch PRIVACY INTERNATIONAL, Ziff. 5. Siehe zum erhöhten Risiko von unrechtmässigen Nutzern Kapitel IV.5.4.1.1.

1351 Siehe zu diesen Sicherheitsmassnahmen Kapitel IV.5.4.1.2.

dass nicht überall dieselben Massnahmen ergriffen werden. Daraus könnte ein unterschiedliches Niveau der Datensicherheit resultieren. Ob sich die Sicherheitsmassnahmen als effektiv erweisen, dürfte sich deshalb erst unter genauerer Berücksichtigung der ergriffenen Massnahmen derjenigen Stellen weisen, welche für die Datensicherheit verantwortlich sind.

d) Entwicklung zu einer omnipotenten Datenbank?

Noch im Jahr 2004 hatten sich u.a. die WP29 sowie das EU-Parlament klar gegen die Schaffung einer zentralen Datenbank ausgesprochen, welche personenbezogene Daten und insbesondere auch biometrische Daten aller InhaberInnen von EU-Pässen hätte speichern sollen.[1352] Zu dieser angedachten zentralen Datenbank war damals festgestellt worden, dass diese nicht verhältnismässig sei und ein solches System ein erhöhtes Risiko für Missbrauch sowie Zweckentfremdung mit sich bringe.[1353]

Im CIR werden zwar nicht primär Daten von EU-BürgerInnen gespeichert. Vielmehr umfasst der CIR eine sehr grosse Anzahl von alphanumerischen und biometrischen Daten von fast ausschliesslich Drittstaatsangehörigen, welche einen Bezug zum Schengen-Raum aufweisen. Dabei dürften die gespeicherten Daten jedoch grundsätzlich denjenigen Angaben entsprechen, welche üblicherweise einem Pass entnommen werden können.[1354]

Die im CIR gespeicherten Daten dürfen zudem (schon jetzt) für verschiedene Zwecke verwendet werden.[1355] Hinzu kommt die Gefahr, dass die im CIR gespeicherten Daten zukünftig vermehrt auch für weitere Zwecke nutzbar gemacht werden, da diese potenziell auch für andere Zwecke nützlich sein könnten. Obwohl solche Zweckerweiterungen nicht *per se* unzulässig sind, könnte ein Speicher mit einer Vielzahl von Daten den Gesetzgeber dazu verleiten, diese auch für andere Zwecke zu nutzen. Schliesslich sind die Daten bereits vorhanden. Dies könnte dazu führen, dass solche Zweckerweiterungen weniger kritisch hinterfragt werden, weil die Daten relativ einfach verfügbar gemacht werden können. Dies ist insofern kritisch zu betrachten, als dass die

1352 Siehe zur Schaffung dieser zentralen Datenbank WP29, Pässe und Reisedokumente, 4 ff. m.w.H.

1353 WP29, Pässe und Reisedokumente, 5.

1354 Der Umstand, dass im CIR keine SIS-Daten gespeichert werden, ist insofern von untergeordneter Bedeutung, als in den anderen Informationssystemen sowieso alle Drittstaatsangehörige erfasst werden, welche einen Berührungspunkt zum Schengen-Raum aufweisen. Siehe VAVOULA, Deathblow, 143 f.

1355 Siehe dazu Kapitel IV.5.3.3.

Erforderlichkeit einer neuen Zugriffsberechtigung bereits bei der Interoperabilität kaum ausreichend begründet wurde.[1356]

Denkbar wäre zudem auch, dass weitere Systeme an den CIR angeschlossen werden. Dadurch würde je nach System der Personenkreis resp. die Datenkategorien vergrössert resp. erweitert werden.[1357] Dies könnte den CIR umso interessanter machen für weitere Zweckerweiterungen resp. für eine missbräuchliche Verwendung.

e) Bewertung

Beim CIR ist insbesondere zu berücksichtigen, dass damit eine sehr umfangreiche Datenbank geschaffen wird. Im CIR wird eine grosse Anzahl von bestimmten alphanumerischen und biometrischen Daten gespeichert, welche im Anwendungsbereich von Eurodac, VIS, EES, ETIAS und ECRIS-TCN erhoben werden. Dabei handelt es sich insbesondere um Daten von Drittstaatsangehörigen, welche sich in der EU aufhalten, in die EU kommen wollen oder die EU bereits wieder verlassen haben. Diese Daten werden in einem gemeinsamen Speicher gespeichert. Duplizierungen der Daten werden nicht vorgenommen.

Insgesamt ergibt sich, dass mit der Schaffung des CIR einerseits das Sicherheitsrisiko steigt und andererseits die Gefahr besteht, dass die darin gespeicherten Daten zukünftig vermehrt für weitere Zwecke nutzbar gemacht werden oder zusätzliche Daten darin gespeichert werden könnten. Um dem erhöhten Sicherheitsrisiko zu begegnen, wurden verschiedene Sicherheitsmassnahmen vorgesehen. Dies ist grundsätzlich zu begrüssen. Besonders kritisch ist die zukünftig potenziell ausufernde Datenbearbeitung rund um den CIR zu betrachten. Insbesondere unter Berücksichtigung, dass vor einigen Jahren ein Speicher, welcher die Daten der InhaberInnen von EU-Pässen hätte speichern sollen, als unverhältnismässig eingestuft wurde, darf nun ein Speicher, welcher ähnliche Daten von Drittstaatsangehörigen beabsichtigt zu speichern, nicht leichthin als zumutbar angesehen werden.

Das Risiko von zukünftigen (unbegründeten) Zweckerweiterungen darf nicht unterschätzt werden. Gerade weil sich im Zusammenhang mit den im Rahmen der Interoperabilität vorgenommenen Zweckerweiterungen gezeigt hat, dass die Erforderlichkeit derselben kaum begründet wurde, ist zu befürchten, dass nach der Schaffung eines Speichers von Daten, welche potenziell für viele

[1356] Siehe dazu die neu geschaffenen Abfragen gemäss Art. 20 EU-IOP-VO und Art. 21 EU-IOP-VO.

[1357] Siehe dazu auch Kapitel VI.3.

Zwecke nützlich sein könnten, ein vermeintlicher Bedarf kaum mehr hinterfragt wird. Zudem ist es auch denkbar, dass zukünftig weitere Datenbanken in die Interoperabilität integriert werden. Diese Entwicklung würde zu einer Vergrösserung des Risikos einer missbräuchlichen Verwendung der Daten führen und mehr Anreiz für weitere Zweckerweiterungen schaffen.

Bei der Beurteilung der Zumutbarkeit eines umfassenden Speichers dürfte es im Allgemeinen eine entscheidende Rolle spielen, welche Daten darin gespeichert werden und von wie vielen Datenbanken. Je umfangreicher der Speicher, desto höher ist das Risiko. Beim CIR sind besonders zukünftige Datenbearbeitungen, welche der Speicher (allzu) leicht ermöglichen könnte, kritisch zu prüfen. Insofern wäre sicherzustellen gewesen, dass mit geeigneten Massnahmen der Umfang des CIR dahingehend beschränkt wird, als möglichst wenige Angaben gespeichert werden. Zudem müssten effektive Sicherheitsmassnahmen gewährleisten, dass Zweckerweiterungen nicht vorschnell zugelassen würden und dass nur in begründeten Fällen weitere Daten im CIR gespeichert werden dürften.

3.4.7. Detektor für Mehrfachidentitäten

3.4.7.1 *Geeignetheit*

Mit dem MID wird die Aufdeckung von Mehrfachidentitäten ermöglicht, wobei dadurch einerseits Identitätsprüfungen vereinfacht und andererseits Identitätsbetrug bekämpft werden können.[1358] Es dürfte im Interesse der Allgemeinheit liegen, dass Identitätsprüfungen vereinfacht werden und dass Identitätsbetrug bekämpft wird. Damit wird zur Wahrung der inneren Sicherheit und zu einem wirksamen Management der Schengen-Aussengrenzen beigetragen.

Da der MID systematische Abgleiche von den im Rahmen der EU-Informationssysteme erhobenen Daten vornimmt, unterstützt der MID ebenso die mit diesen Systemen verfolgten öffentlichen Interessen.[1359] Diese bestehen insbesondere im wirksamen Management der Schengen-Aussengrenzen, der Wahrung der inneren Sicherheit sowie der wirksamen Umsetzung der Asyl- und Visapolitik.[1360] Insgesamt trägt der MID insbesondere zu einem hohen Mass an Sicherheit bei.[1361]

1358 Art. 25 Abs. 1 EU-IOP-VO.

1359 Art. 25 Abs. 1 EU-IOP-VO.

1360 ErwG. 40 EU-IOP-VO.

1361 Vgl. zum Ganzen auch EUROPEAN COMMISSION, Impact assessment IOP Part 1, 41.

3.4.7.2 *Erforderlichkeit*

In der Folgenabschätzung wurde ausgeführt, dass die Aufdeckung von Mehrfachidentitäten eine Grundvoraussetzung darstelle, damit die einzelnen Informationssysteme ihre Ziele erreichen könnten. Aufgrund der eigenständigen Struktur der Informationssysteme sei bis anhin keine systemübergreifende Identitätsprüfung möglich.[1362] Dies führe zu Informationslücken, welche den Behörden ein komplettes Bild verwehrten. Es sei deshalb gegenwärtig schwierig, Mehrfachidentitäten aufzudecken. Mit dem MID könnten jedoch Verbindungen zwischen den verschiedenen Daten hergestellt werden. Dadurch könne nicht nur Identitätsbetrug entdeckt werden, sondern auch Fälle von Verwechslungen bei Bona-fide-Reisenden.[1363]

Der Rat der EU verwies in seinen Schlussfolgerungen zum weiteren Vorgehen bezüglich der Interoperabilität zudem darauf, dass die Täter von Terroranschlägen sowie anderen strafbaren Handlungen betrügerische Identitätsangaben verwendet hätten und dies bei deren Vorgehensweise von entscheidender Bedeutung gewesen sei.[1364]

Der Folgenabschätzung können jedoch keine konkreten Angaben oder Einschätzungen zum Ausmass des Identitätsbetrugs entnommen werden.[1365] Das Ausmass der Problematik mit den Mehrfachidentitäten resp. dem Identitätsbetrug wurde somit nicht durch objektive Beweise belegt. Ohne Einzelheiten zum Ausmass des Identitätsbetrugs, ist die Erforderlichkeit und die Verhältnismässigkeit der vorgeschlagenen Massnahme kaum überprüfbar.[1366]

1362 Ausgenommen davon sind gewisse Aspekte vom EES, VIS und ETIAS, welche teilweise miteinander verbunden sind.

1363 Siehe zum Ganzen EUROPEAN COMMISSION, Impact assessment IOP Part 1, 41.

1364 RAT DER EUROPÄISCHEN UNION, Schlussfolgerungen, 2.

1365 Aus der Folgenabschätzung geht lediglich hervor, dass geschätzt werde, dass mindestens 500'000 Drittstaatsangehörige Mehrfachidentitäten verwenden, aus verschiedenen Gründen. Siehe dazu EUROPEAN COMMISSION, Impact assessment IOP Part 2, 16 f. Dies sagt jedoch noch nichts über das Ausmass des Identitätsbetrugs aus.

1366 EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 35 f. Siehe dazu auch SFH, Vernehmlassungsantwort, 12; EISELE, impact assessment. Vgl. dazu auch JONES, 30.

3.4.7.3 *Zumutbarkeit*

a) Zweckerweiterung?

In der Folgenabschätzung wurde festgehalten, dass – anders als beim CIR zur Abfrage zwecks Identifizierung[1367] – der mit dem MID verfolgte Zweck nicht als sekundäres Ziel in die gesetzlichen Grundlagen der betroffenen Informationssysteme aufgenommen werden müsse. Denn bereits für die Erreichung der primären Zwecke der Informationssysteme sei eine korrekte Identifizierung von Drittstaatsangehörigen notwendig.[1368] Insofern ergibt sich daraus, dass die Datenbearbeitung durch den MID von den Zwecken der betroffenen Informationssysteme als bereits abgedeckt betrachtet wurde.

Es mag zwar zutreffen, dass die Erfüllung der Zwecke der Informationssysteme massgeblich davon abhängt, dass die betroffenen Personen korrekt identifiziert werden können. Vereinzelt werden in den gesetzlichen Grundlagen der Informationssysteme tatsächlich Elemente der Zielsetzung des MID aufgegriffen. So wird der Begriff «*Mehrfachidentität*» in den Erwägungsgründen der gesetzlichen Grundlagen des SIS verwendet.[1369] Des Weiteren findet sich in den Erwägungsgründen der EES-VO ein indirekter Bezug zur Aufdeckung von Mehrfachidentitäten, welche zu vermeiden sind.[1370] Das VIS und das EES verfolgen gar ausdrücklich das Ziel der Bekämpfung von Identitätsbetrug.[1371] Dass Identitäten missbräuchlich verwendet werden können, wird zudem aus den gesetzlichen

---

1367 Der mit Art. 20 EU-IOP-VO verfolgte Zweck wurde in die gesetzlichen Grundlagen der betroffenen Systeme integriert. Ausgenommen ist jedoch Eurodac. Wegen der Revision der Eurodac-VO finden sich in den EU-IOP-VO (noch) keine konkreten Verweise auf Bestimmungen dieser Verordnung. Siehe dazu BUNDESRAT, Botschaft IOP, 8002 f. Siehe zu den anderen Systemen Art. 58 Ziff. 1 IOP-Grenze-VO; Art. 60 Ziff. 1 und 3 IOP-Grenze-VO; Art. 61 Ziff. 1 und 3 IOP-Grenze-VO; Art. 61 Ziff. 2 und 12 IOP-Polizei-VO.

1368 EUROPEAN COMMISSION, Impact assessment IOP Part 1, 41.

1369 Demnach sollte eine Ausschreibung Bezug nehmen auf das persönliche Identifizierungsdokument resp. dessen Nummer sowie eine Kopie, sofern dies vorhanden ist, um die Identifizierung zu erleichtern und Mehrfachidentitäten aufzudecken. Siehe dazu ErwG. 10 SIS-Rückkehr-VO; ErwG. 16 SIS-Grenze-VO; ErwG. 16 SIS-Polizei-VO.

1370 So soll aufgrund der Fingerabdruckabnahme vermieden werden, dass ein Drittstaatsangehöriger nicht schon unter einer anderen Identität resp. mit einem anderen Reisedokument erfasst ist. Siehe ErwG. 21 EES-VO. Ausserdem soll der Zugang zum EES für die Zwecke der Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten den verantwortlichen Behörden ermöglichen, Fälle aufzuklären, in denen Verdächtige mehrere Identitäten verwenden. Siehe ErwG. 22 EES-VO.

1371 Siehe zum EES Art. 6 Abs. 1 Bst. i EES-VO sowie auch Art. 27 Abs. 1 EES-VO. Siehe zum VIS Art. 2 Bst. c und Bst. e VIS-VO. Vgl. dazu ausserdem ErwG. 10 VO 2021/1134; ErwG. 12 VO 2021/1134; ErwG. 17 VO 2021/1134.

Grundlagen des SIS ersichtlich, wobei es sich dabei um eine Regelung von Fällen handelt, in welchen Identitäten missbraucht werden.[1372] In den gesetzlichen Grundlagen des ETIAS sowie des ECRIS-TCN sind die Begriffe «*Mehrfachidentität*» sowie «*Identitätsbetrug*» hingegen nicht auffindbar. Auch der Eurodac-VO sind diese beiden Begriffe nicht zu entnehmen.

Bestimmte Informationssysteme enthalten also (vereinzelte) Elemente der Zielsetzung des MID. Die Zielsetzung des MID geht also zumindest teilweise mehr oder weniger über den Zweck der betroffenen Systeme hinaus. Deswegen hätte die Zielsetzung des MID in die gesetzlichen Grundlagen der einzelnen Systeme aufgenommen werden sollen.[1373]

b) Datenqualität

Der Datenqualität kommt beim MID insbesondere deshalb eine wichtige Bedeutung zu, weil diese Komponente gelbe Verknüpfungen zwischen verschiedenen Datensets erstellt, welche ähnliche Daten enthalten. Sind viele der vom MID geprüften Daten falsch, werden folglich viele gelbe Verknüpfungen erstellt, welche im Anschluss manuell zu verifizieren sind. Eine tiefe Qualität der Daten könnte also zu einem (unverhältnismässig) grossen Aufwand bei der manuellen Verifizierung führen. Es ist deshalb von zentraler Bedeutung, dass die vom MID geprüften Daten möglichst korrekt sind.

In diesem Sinne ist es zu begrüssen, dass in den EU-IOP-VO verschiedene Massnahmen enthalten sind, welche eine hohe Qualität der Daten herbeiführen sollen. So müssen insbesondere die in die Systeme eingegebenen Daten sowie auch die Templates eine gewisse Mindestqualität aufweisen, bevor sie am jeweils vorgesehenen Ort gespeichert werden. Ausserdem soll eu-LISA Mechanismen und Verfahren für die automatische Datenqualitätskontrolle einführen. Des Weiteren wird die Datenqualität regelmässig durch die Kommission evaluiert, wobei bei Bedarf Empfehlungen abgegeben werden können.[1374]

c) Manuelle Verifizierung

Die vom MID erstellten gelben Verknüpfungen sind manuell zu überprüfen.[1375] In den EU-IOP-VO ist festgelegt, welche Behörde dafür zuständig ist. Grund-

1372 Art. 47 SIS-Grenze-VO; Art. 62 SIS-Polizei-VO.

1373 Vgl. dazu auch EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 33 f.; VAVOULA, Deathblow, 144 f.; VAVOULA, Interoperability, 178 f.; GUTHEIL, et al., 14, 69.

1374 Siehe dazu Kapitel IV.5.4.2.4.

1375 Art. 30 Abs. 2 EU-IOP-VO.

sätzlich ist dies diejenige Behörde, welche die Daten in ein System eingegeben hat und aufgrund welcher in der Folge durch die automatisierte Abfrage des MID die gelbe Verknüpfung mit bereits erfassten Daten erstellt wurde. Davon ausgenommen sind Verknüpfungen, welche eine SIS-Ausschreibung betreffen. In diesen Fällen ist immer das SIRENE-Büro zuständig, welches die Ausschreibung vorgenommen hat.[1376]

Somit werden die manuellen Verifizierungen von vielen verschiedenen Behörden – und folglich auch von einer Vielzahl von verschiedenen BeamtInnen – vorgenommen. Diese werden nicht alle dasselbe Niveau an Erfahrung und Ausbildung für diese Tätigkeit mitbringen. Selbst mit einer detaillierten Anweisung dürfte es nicht möglich sein, europaweit einheitliche Vorgehensweisen zur Einteilung in die Farbkategorien nach erfolgter Verifizierung zu etablieren. Im Ergebnis werden die BeamtInnen zumindest in bestimmten Konstellationen über viel Ermessen verfügen.[1377]

d) Eignung von ETIAS-Daten für die Abfrage

ETIAS-Daten werden, wie auch die Daten der anderen Systeme, vom MID einer Prüfung auf Mehrfachidentitäten unterzogen. Wie bereits ausgeführt, werden diese Daten von den betroffenen Personen selbst deklariert. Sie sind deshalb grundsätzlich anfälliger für Fehler als Daten, welche von BeamtInnen erhoben werden. Im ETIAS werden zudem keine biometrischen Daten gespeichert. Verknüpfungen, welche vom MID erstellt werden, können demnach nur alphanumerische Daten betreffen. ETIAS-Daten eigenen sich demnach nur begrenzt für die Vornahme von Abgleichen durch den MID.[1378] Denn es besteht die Gefahr, dass der MID eine Vielzahl von Verknüpfungen zwischen ETIAS-Daten und Daten aus anderen Systemen erstellt, welche in der Folge zu verifizieren sind. Damit könnte ein grosser Aufwand verbunden sein. Fraglich erscheint, ob dieser in Anbetracht der Zielsetzung des MID verhältnismässig erscheint.

1376 Siehe dazu Art. 29 EU-IOP-VO. Bei der Zuständigkeit des SIRENE-Büros stellt sich die Frage, wie dieses darüber informiert wird, dass eine manuelle Verifizierung vorzunehmen ist. Dies geht nicht aus den EU-IOP-VO hervor. Vgl. dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 91.

1377 FRA, Opinion IOP, 40.

1378 Allenfalls könnten ETIAS-Daten speziell gekennzeichnet werden, was heisst, dass die Daten weniger zuverlässig sind. Siehe dazu FRA, Opinion IOP, 38.

e) Vereinfachung von Identitätsprüfungen

Mit dem Ziel der Aufdeckung von Mehrfachidentitäten sollen nicht nur Personen aufgespürt werden können, welche über ihre Identität täuschen. Auch die Identitätsprüfung von Personen mit berechtigten Mehrfachidentitäten soll erleichtert werden.[1379]

Es gibt verschiedene Gründe, wieso eine Person über eine legale Mehrfachidentität verfügen kann. So können Personen mit verschiedenen Staatsangehörigkeiten z.B. mit unterschiedlichen Reisepässen reisen. Auch eine im Zuge einer Heirat vorgenommene Namensänderung kann dazu führen, dass eine Person in verschiedenen Informationssystemen berechtigterweise mit unterschiedlichen Identitäten erfasst wird. Zudem existieren auch sog. Tarnidentitäten, die eine berechtigte Mehrfachidentität mit sich bringen.[1380]

Bei Personen, welche mit verschiedenen Identitäten erfasst werden, wird eine gelbe Verknüpfung zwischen den verschiedenen Datensets erstellt, da (berechtigterweise) unterschiedliche Angaben zu den Identitätsdaten vorliegen.[1381] Diese gelben Verknüpfungen sind einer manuellen Verifizierung zu unterziehen.[1382]

Die manuelle Verifizierung dürfte häufig bei der Einreise in den Schengen-Raum stattfinden, da in diesem Zeitpunkt die Angaben zur Einreise im EES erfasst werden und die Daten von visumpflichtigen Drittstaatsangehörigen bereits im VIS und diejenigen von visumbefreiten Drittstaatsangehörigen im ETIAS gespeichert sind. Es besteht insofern die Gefahr, dass Personen mit rechtmässigen Mehrfachidentitäten überdurchschnittlich oft an der Grenze angehalten werden. Um allfällige Nachteile für die betroffenen Personen zu vermeiden, ist sicherzustellen, dass die manuelle Verifizierung nicht zu viel Zeit in Anspruch nimmt.[1383]

Abgesehen von Personen mit berechtigten Mehrfachidentitäten können auch Personen mit geläufigen Namen von einer Vereinfachung bei der Identitätsprüfung profitieren. Insbesondere wenn keine biometrischen Daten erfasst wurden, besteht bei Letzteren eine Verwechslungsgefahr. Auch in solchen Konstellationen werden ebenfalls gelbe Verknüpfungen erstellt, welche manu-

1379 Art. 25 Abs. 1 EU-IOP-VO.
1380 Siehe zu den Tarnidentitäten in der Schweiz Art. 18 NDG.
1381 Vgl. dazu Art. 30 Abs. 1 Bst. a-b EU-IOP-VO.
1382 Art. 30 Abs. 2 EU-IOP-VO.
1383 Vgl. zum Ganzen FRA, Opinion IOP, 36 f.; SFH, Vernehmlassungsantwort, 12. Vgl. dazu auch Carrera.

ell zu verifizieren sind. Somit dürften auch Personen mit geläufigen Namen vermehrt bei der Einreise aufgehalten werden. Erst wenn nach der manuellen Verifizierung die grüne resp. weisse Verknüpfung erstellt ist, wirkt sich die Datenbearbeitung im Zusammenhang mit dem MID positiv auf diese Personen aus, da sie danach nicht mehr fälschlicherweise verwechselt werden resp. festgestellt wurde, dass berechtigte Mehrfachidentitäten vorliegen.[1384]

Die Qualität der manuellen Verifizierung ist also äusserst wichtig. Nur wenn richtigerweise erkannt wird, dass es sich um berechtigte Mehrfachidentitäten handelt resp. sich die Daten auf zwei unterschiedliche Personen beziehen, kann das Ziel des MID, Identitätsprüfungen zu vereinfachen, erreicht werden. Wird hingegen bei der manuellen Verifizierung eine berechtigte Mehrfachidentität resp. eine Verwechslung mit einer anderen Person nicht erkannt, wird eine rote Verknüpfung erstellt und die betroffene Person erleidet möglicherweise allfällige Nachteile aufgrund der gegen den vermeintlichen Identitätsbetrug ergriffenen Massnahmen. In Einzelfällen mag dies nicht vermeidbar sein. Eine durchgehend tiefe Qualität der manuellen Verifizierung würde die Situation für Personen mit berechtigten Mehrfachidentitäten resp. mit geläufigen Namen durch die Interoperabilität nicht verbessern. Vielmehr würde sich deren Situation dahingehend verschlechtern, als dass ihnen regelmässig unberechtigterweise Identitätsbetrug angelastet werden könnte.

f) Vorgehensweise bei Identitätsbetrug

Auf die von einer roten Verknüpfung betroffenen Daten darf «*ausschliesslich zur Bekämpfung von Identitätsbetrug*» zugegriffen werden.[1385] Eine konkrete Vorgehensweise dazu wurde im EU-Recht jedoch nicht näher definiert. Es ist deshalb einerseits unklar, ob die betroffene Behörde zwingend aktiv werden muss oder lediglich kann. Andererseits ist auch nicht festgelegt, welche Massnahmen zu ergreifen sind. Gerade weil es sich bei der Bekämpfung von Identitätsbetrug um ein erklärtes Ziel der Interoperabilität handelt, wäre es von zentraler Bedeutung gewesen, festzulegen, in welcher Form diese Bekämpfung vorgenommen werden sollte. Ohne eine solche Regelung ist davon auszugehen, dass sich in der Praxis unterschiedliche Vorgehensweisen etablieren werden, welche mehr oder weniger effektiv sind. Insgesamt besteht die Gefahr, dass mit der Interoperabilität ein Identitätsbetrug zwar aufgedeckt werden

---

1384 Vgl. dazu FRA, Opinion IOP, 36 f.; SFH, Vernehmlassungsantwort, 12. Vgl. dazu auch Carrera.

1385 Art. 21 Abs. 2 EU-IOP-VO.

kann, dieser jedoch mangels eingehender Regelung letztlich nicht bekämpft wird.[1386]

g) Weitere Sicherheitsmassnahmen

Über die Datenbearbeitungsvorgänge im MID sind von eu-LISA, den Schengen/Dublin-Staaten als auch von den Stellen der Union Protokolle zu erstellen, welche – wie auch die Protokolle betreffend das ESP, den BMS und den CIR – zur datenschutzrechtlichen Kontrolle verwendet werden. Während die zu protokollierenden Angaben für eu-LISA klar vorgegeben sind, fehlt eine solche Regelung für die Schengen/Dublin-Staaten sowie die Stellen der Union. Damit die durch die Protokollierungspflicht beabsichtigte Kontrolle gewährleistet werden kann, muss sichergestellt werden, dass auch diese Akteure zumindest die für eu-LISA vorgegebenen Angaben protokollieren.[1387]

h) Speicherfrist

Die im MID gespeicherten Identitätsbestätigungsdateien inklusive der Verknüpfungen werden grundsätzlich nur so lange gespeichert, wie die verknüpften Daten in mindestens zwei Systemen gespeichert werden. Die Löschung erfolgt automatisch.[1388]

Von diesem Grundsatz gibt es eine Ausnahme. Wird eine weisse oder rote Verknüpfung von im CIR gespeicherten Daten erstellt, wird für die neuen Daten keine neue individuelle Datei angelegt. Vielmehr werden die neuen Daten der individuellen Datei der verknüpften Daten hinzugefügt.[1389] Obwohl vorgesehen ist, dass die Erstellung einer Verknüpfung auf die Aufbewahrungsdauer keinen Einfluss hat, scheint die genannte Bestimmung der EU-IOP-VO eine Verlängerung der Speicherdauer zu ermöglichen.[1390]

Die Speicherdauer sollte sowieso nach dem Zweck der Verknüpfungen bemessen werden. Wird eine rote Verknüpfung erstellt, sind grundsätzlich entsprechende Massnahmen zu ergreifen. Danach hat die rote Verknüpfung ihren Zweck erfüllt und erscheint nicht mehr notwendig. Sie könnte also gelöscht

1386 In der Folgenabschätzung war noch festgehalten worden, dass jede Verknüpfung je nach Farbe ein Follow-up Verfahren vorsehen sollte. Dies wurde bei den roten Verknüpfungen versäumt. Siehe dazu EUROPEAN COMMISSION, Impact assessment IOP Part 1, 42.

1387 Siehe dazu Art. 36 EU-IOP-VO. Siehe betreffend den Zugang zu den Protokollen auch Art. 40 Abs. 4 EU-IOP-VO.

1388 Art. 35 EU-IOP-VO.

1389 Art. 19 Abs. 2 EU-IOP-VO.

1390 WP29, Opinion proposals IOP, 19.

werden. Bei den grünen Verknüpfungen scheint hingegen die festgelegte Speicherdauer angemessen. Mit dieser Verknüpfung soll schliesslich sichergestellt werden, dass zwei unterschiedliche Personen nicht miteinander verwechselt werden.[1391]

i) Bewertung

Die obigen Ausführungen haben gezeigt, dass verschiedene Aspekte der Regelung des MID aus datenschutzrechtlicher Perspektive kritisch zu bewerten sind.

Besonders hervorzuheben ist an dieser Stelle, dass die gesetzlichen Grundlagen der einzelnen Informationssysteme zwar teilweise die Bekämpfung von Identitätsbetrug als Zielsetzung vorsehen. Dennoch erscheint der Zweck des MID nicht vollständig in den gesetzlichen Grundlagen der betroffenen Informationssysteme abgebildet zu sein. Auch unter Berücksichtigung, dass sich die mit dem MID vorgenommene Datenbearbeitung nicht aus den gesetzlichen Grundlagen der involvierten Systeme erschliesst, hätte diese in diese Rechtsgrundlagen aufgenommen werden sollen.

Davon abgesehen wurde festgestellt, dass der Qualität der manuellen Verifizierung eine entscheidende Bedeutung zukommt. Da verschiedene Stellen diese manuelle Verifizierung vornehmen werden, liegt die Gefahr einer uneinheitlichen Praxis auf der Hand. Mit entsprechenden Schulungen sowie Anweisungen des Personals ist dies unbedingt zu vermeiden. Denn nur wenn im Anschluss an die Verifizierung die korrekte Farbe der Verknüpfung gesetzt werden kann, können die Ziele des MID erreicht werden. Personen mit berechtigten Mehrfachidentitäten werden also als solche erkannt und müssen zukünftig nicht mehr unnötig bei Identitätskontrollen aufgehalten werden. Aber auch Personen, welche über ihre Identitäten täuschen, werden entdeckt. Alternativ hätte auch eine dritte Stelle mit der manuellen Verifizierung betraut werden können. So hätte eine einheitliche Praxis der Prüfung der Mehrfachidentitäten eher sichergestellt werden können.[1392]

Die Regelung des MID büsst zudem bei der Effektivität insofern ein, als keine konkreten Massnahmen im EU-Recht festgehalten wurden, welche zu ergreifen sind, wenn eine rote Verknüpfung erstellt wird. Dadurch besteht das Ri-

1391 WP29, Opinion proposals IOP, 10 f. Siehe zur Speicherdauer auch FRA, borders and security, 23 f.

1392 Siehe dazu Kapitel V.3.4.5.3.c).

siko, dass keine oder nicht die richtige Massnahme ergriffen wird, womit letztlich dem Ziel des MID nicht entsprochen werden kann.

Des Weiteren hätte bei der Regelung der Speicherfrist sichergestellt werden müssen, dass keine Verlängerung derselben erfolgt und sich diese zudem am Zweck der Datenbearbeitung orientiert. Auch stellt sich die Frage, ob der Einbezug von ETIAS-Daten in die Prüfung der Mehrfachidentitäten tatsächlich einen Mehrwert bringt oder ob damit vielleicht sogar die Effizienz des MID eingebüsst wird. Insofern erscheint die Ausgestaltung des MID aufgrund der oben genannten Aspekte unverhältnismässig.

3.4.8. Ausgewählte Sicherheitsmassnahmen

3.4.8.1 *Rechte der betroffenen Personen*

a) Recht auf Information

Das Recht auf Information ist in den EU-IOP-VO explizit verankert. Es steht denjenigen Personen zu, deren Daten im BMS, CIR oder im MID gespeichert werden. Der Inhalt des Rechts auf Information ergibt sich mittels Verweises auf die einschlägigen datenschutzrechtlichen Bestimmungen des EU-Sekundärrechts.[1393]

Ein Vergleich mit den Vorschlägen der EU-IOP-VO zeigt, dass – neben diesen Verweisen – ursprünglich explizit auch gewisse Angaben zum Inhalt des Rechts auf Information enthalten waren.[1394] Bezogen auf diese Regelung forderten der EDSB und die FRA die explizite Aufführung weiterer Aspekte des Rechts auf Information, so z.B. die Speicherfrist, die Angabe zu den verschiedenen Zwecken der Datenbearbeitung – insbesondere, dass die personenbezogenen Daten u.U. von Strafverfolgungsbehörden abgerufen werden können – oder die Empfänger der Daten. Diese weiteren Aspekte sind zwar in den datenschutzrechtlichen Bestimmungen des Sekundärrechts aufgeführt. Dennoch stellte die FRA klar, eine Wiederholung dieser Aspekte in den EU-IOP-VO sei angezeigt, um Klarheit für die Betroffenen zu schaffen. Mit der Interoperabilität sei es zunehmend schwieriger der Informationspflicht nachzukom-

1393 Siehe dazu Art. 47 EU-IOP-VO.

1394 Siehe dazu EUROPÄISCHE KOMMISSION, Vorschlag IOP-Grenze, 69 f.; EUROPÄISCHE KOMMISSION, Vorschlag IOP-Polizei, 69 (jeweils Art. 46). Es handelte sich dabei um folgende Angaben: Identität und Kontaktangaben des jeweiligen Verantwortlichen, Kontaktangaben des EDSB und der nationalen Aufsichtsbehörde und Informationen über das Verfahren für die Geltendmachung der Rechte auf Einsicht, Berichtigung und Löschung.

men, weshalb zumindest die wichtigsten Aspekte dieses Rechts der betroffenen Personen explizit im EU-Recht festzuhalten seien.[1395]

Ein Blick auf Art. 47 EU-IOP-VO lässt erkennen, dass dieser Empfehlung nicht Folge geleistet wurde. Erstaunlicherweise sind nicht einmal mehr diejenigen Aspekte der Informationspflicht in der Bestimmung enthalten, welche in den Vorschlägen der EU-IOP-VO noch explizit vorgesehen waren. Eine explizite Nennung der Angaben, über welche zu informieren ist, würde für die Betroffenen in der Tat mehr Klarheit verschaffen. So müssen nun mehrere gesetzliche Grundlagen konsultiert werden, damit sich der Inhalt der Informationspflicht erschliesst. Dies ist weder im Sinne der Betroffenen noch derjenigen Personen, an welche sich die Informationspflicht richtet. Diese verstreute Regelung der Informationspflicht erhöht die Gefahr, dass dem Recht auf Information in der Praxis nur ungenügend Rechnung getragen wird.[1396] Dies ist möglichst zu verhindern, zumal das Recht auf Information eine wichtige Sicherheitsmassnahme darstellt. Ohne genügende Information über die Art und Weise der Datenbearbeitung können die Rechte auf Auskunft, Berichtigung und Löschung nicht wahrgenommen werden.[1397]

b) Recht auf Auskunft, Berichtigung und Löschung

Das in den EU-IOP-VO geregelte Recht auf Auskunft, Berichtigung und Löschung bezieht sich ausschliesslich auf die in der Identitätsbestätigungsdatei gespeicherten Angaben des MID.[1398]

Fehler des MID sind typischerweise auf ungenaue oder unrechtmässig gespeicherte Daten im CIR zurückzuführen. Diese Fehler können nicht auf Grund der Rechte gemäss den EU-IOP-VO behoben werden. Denn für die Verarbeitung der Daten im CIR sind diejenigen Behörden zuständig, welche bei den einzelnen Systemen dafür verantwortlich sind. Dies führt zu einer Fragmentierung der Rechte der betroffenen Personen, da Fehler im CIR nicht gemäss Art. 48 EU-IOP-VO behoben werden können. Eine Überprüfung der Verknüpfung müsste demnach auch eine Korrektur der Daten im CIR beinhalten, da

1395 Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 118; FRA, Opinion IOP, 45 ff.

1396 Die FRA hat zum Recht auf Information bei Eurodac einen Leitfaden erstellt, welcher sich an die Behörden richtet. Siehe dazu FRA, Practical Guide Eurodac. Ein solcher Leitfaden wäre auch für die Informationspflicht bei der Interoperabilität hilfreich.

1397 FRA, Opinion IOP, 45. Vgl. dazu auch Nygård.

1398 Siehe zu den Einzelheiten Art. 48 EU-IOP-VO.

sonst das Recht auf Berichtigung und Löschung nicht effektiv ausgeübt werden kann.[1399]

Des Weiteren trägt die Person, welche ihre Daten berichtigen möchte, die Beweislast. Während offensichtliche Fehler von alphanumerischen Daten, wie ein falsch geschriebener Name, z.B. durch das Vorlegen von Dokumenten mit personenbezogenen Daten, widerlegt werden können, ist dies bei biometrischen Daten nicht möglich.[1400] Eine Möglichkeit, einen biometrischen Test zu machen, um zu beweisen, dass ein falscher Treffer vorliegt, ist nicht vorgesehen. Es besteht die Gefahr, dass die betroffene Person in solchen Fällen automatisch eines Identitätsbetrugs bezichtigt wird. Mehrfachidentitäten können auch auf eine schlechte Datenqualität biometrischer Daten zurückzuführen sein.[1401] Die betroffenen Personen haben in einer solchen Konstellation jedoch eine schwache Position, dies zu beweisen. Dies umso mehr, als dass biometrische Daten grundsätzlich als besonders verlässlich angesehen werden. Gegen eine Entscheidung aufgrund biometrischer Daten können die betroffenen Personen somit kaum einen Gegenbeweis vorbringen. Dies beeinträchtigt die Ausübung der Rechte der Betroffenen.[1402]

Die Interoperabilität basiert zu einem grossen Teil auf biometrischen Abgleichen. Von falschen Treffern betroffene Personen haben kaum die Möglichkeit, sich mittels Gegenbeweisen dagegen zu wehren. Daher kommt der Datenqualität eine erhöhte Bedeutung zu. Je besser diese ist, desto weniger falsche Treffer sind zu erwarten.

c) Web-Portal

Eine der grössten Hürden für die betroffenen Personen betreffend die Ausübung ihrer Rechte im Zusammenhang mit ihren Daten stellt die Ausübung des Rechts auf Zugang und Auskunft dar. Dies zeigt sich bspw. dadurch, dass bei den Informationssystemen Eurodac, VIS und SIS das Recht auf Zugang zu den Daten nur sehr selten geltend gemacht wird.[1403] Die FRA vermutet, dass es den betroffenen Personen häufig am Bewusstsein und dem Verständnis, wie das

1399 Siehe dazu FRA, Opinion IOP, 50.

1400 Eine Berichtigung muss nicht unbedingt sehr kompliziert sein. Durch Vorweisen eines Dokuments, wie einer verlässlichen Geburtsurkunde oder eines Passes kann eine Berichtigung vorgenommen werden. Insbesondere Asylsuchende sind aber oftmals nicht im Besitz von solchen Dokumenten. Siehe dazu FRA, biometrics, 101.

1401 Siehe zur Thematik der Datenqualität Kapitel IV.5.4.2.

1402 Vgl. zum Ganzen FRA, borders and security, 33 f.

1403 Im Jahr 2023 wurden 377 Auskunftsgesuche bezüglich Eurodac-Daten gestellt. Siehe dazu EU-LISA, Eurodac report 2023, 18.

Recht auf Zugang, Berichtigung und Löschung ausgeübt werden kann, fehlt.[1404] Administrative Hürden, Sprachbarrieren, mangelndes Verständnis der Verfahren sowie die Tatsache, dass lediglich wenige AnwältInnen darauf spezialisiert sind, stellen die Hauptgründe dar, wieso viele Personen ihr Recht auf Auskunft, Berichtigung oder Löschung von fehlerhaften Angaben, welche in den Informationssystemen gespeichert sind, nicht wahrnehmen.[1405]

Diese Schwierigkeiten können sich durch die Interoperabilität noch vergrössern. Denn durch die Interoperabilität wird es für die betroffenen Personen zunehmend schwieriger vorherzusehen, inwiefern ihre Daten bearbeitet werden. Zudem muss die betroffene Person zuerst in Erfahrung bringen, an welche Behörde sie sich zur Ausübung ihrer Rechte wenden muss. Auch wenn die Behörden gehalten sind, die Anfragen an die zuständige Behörde weiterzuleiten, entstehen dadurch Verzögerungen.[1406] Diese durch die Interoperabilität verursachten zusätzlichen Hindernisse erschweren auch die Ausübung des Rechts auf Auskunft. Dieses Recht stellt wiederum den Ausgangspunkt für die Ausübung von weiteren Rechten dar.[1407]

Es ist deshalb zu begrüssen, dass mit dem Web-Portal die Geltendmachung dieser Rechte erleichtert werden soll. Das Portal soll dabei u.a. Informationen zu den Rechten und Verfahren enthalten.[1408] Die genaue Ausgestaltung desselben wird sich auf die Effizienz der Geltendmachung der Rechte auswirken.[1409]

Nichtsdestotrotz können mit dem Web-Portal die Schwierigkeiten beim Beweis von falschen Treffern nicht behoben werden. Ausserdem wird dadurch auch keine Berichtigung der Daten des CIR ermöglicht, welche bei der Geltendmachung der Rechte beim MID notwendig wäre. Wurde eine Person bei der Erhebung der Daten nicht ausreichend informiert, vermag auch das Web-Portal diese Unterlassung nicht mehr zu beheben.[1410]

3.4.8.2 *Datenübermittlung an Dritte*

Die EU-IOP-VO statuieren ein grundsätzliches Verbot der Übermittlung von im Rahmen der Interoperabilität verarbeiteten Daten an Drittstaaten, internationale

1404 Siehe dazu FRA, biometrics, 100.
1405 FRA, biometrics, 17.
1406 Siehe dazu FRA, Opinion IOP, 50 ff.
1407 VAVOULA, Interoperability, 190.
1408 Siehe zu den Einzelheiten Art. 49 EU-IOP-VO.
1409 Es muss Informationen zur Substanz der Rechte haben und nicht nur, ob diese Rechte existieren und welche Verfahren einzuhalten sind. Siehe dazu VAVOULA, Interoperability, 190.
1410 VAVOULA, Interoperability, 190.

Organisationen sowie private Stellen. Vorbehalten sind jedoch die in den gesetzlichen Grundlagen der einzelnen Systeme vorgesehenen Ausnahmen.[1411]

Trotz dieses grundsätzlichen Verbots stellt sich die Frage, ob mit der Interoperabilität das Risiko einer unrechtmässigen Weiterleitung an Drittstatten, internationale Organisationen oder private Stellen vergrössert wird. Dies könnte sich insofern ergeben, weil Zugriffserweiterungen vorgenommen und neuen Akteuren Abfragerechte gewährt werden.[1412] Diese von der FRA geäusserte Befürchtung ist nicht unbegründet. Schliesslich dürfte die Erhöhung der Anzahl der abfrageberechtigten Stellen sowie der Erweiterung der Zugriffsberechtigungen mit einem grösseren Risiko einer unrechtmässigen Weitergabe der Daten an Dritte einhergehen.[1413]

3.4.8.3 *Aufsicht*

Die Aufsicht über die Datenbearbeitung im Zusammenhang mit der Interoperabilität wird durch die koordinierte Aufsicht von den nationalen Aufsichtsbehörden sowie dem EDSB sichergestellt.[1414]

Die nationalen Aufsichtsbehörden erhalten durch die EU-IOP-VO neue Aufsichtspflichten. Damit diese effektiv wahrgenommen werden können, muss sichergestellt werden, dass auch die benötigten Ressourcen bereitgestellt werden.[1415] In den EU-IOP-VO wird lediglich ausgeführt, dass die Schengen/Dublin-Staaten ausreichende Ressourcen und Fachkenntnisse zur Verfügung stellen müssen.[1416] Damit wurde eine kostengünstige Lösung für die EU geschaffen.[1417] Bereits jetzt sind die nationalen Aufsichtsbehörden teilweise überlastet und unterbesetzt.[1418] Abgesehen von ausreichenden Ressourcen ist auch die Unabhängigkeit der Aufsichtsbehörden von zentraler Bedeutung. Diese haben die Schengen/Dublin-Staaten sicherzustellen.[1419]

1411 Siehe dazu Art. 50 EU-IOP-VO.

1412 Siehe Art. 21 EU-IOP-VO; Art. 20 EU-IOP-VO.

1413 Siehe dazu FRA, Opinion IOP, 15, wobei insbesondere die unrechtmässige Weitergabe von Eurodac-Daten für die Betroffenen resp. deren Familien mit schwerwiegenden Nachteilen verbunden sein kann.

1414 Siehe dazu Kapitel IV.5.4.3. Dieses Modell entspricht auch dem für die einzelnen Systeme gewählten Modell der Aufsicht. Siehe Kapitel III.4.2; III.5.2; III.6.2; III.7.2; III.8.2 und III.9.2.

1415 FRA, Opinion IOP, 11. Siehe dazu auch SFH, Vernehmlassungsantwort, 4.

1416 Art. 51 Abs. 4 EU-IOP-VO.

1417 Vgl. zum Ganzen Groenendijk.

1418 Siehe dazu Carrera.

1419 Siehe dazu Art. 51 Abs. 1 EU-IOP-VO. In diesem Kontext erscheint es nicht unproblematisch, wenn die nationalen Kontrollbehörden im Zusammenhang mit der Abfrage zwecks

Auch die Komplexität der gesetzlichen Regelung kann eine effektive Aufsicht der Datenschutzbehörden auf EU-Ebene sowie nationaler Ebene beeinträchtigen. So sind für die Datenbearbeitung viele gesetzliche Grundlagen relevant und verschiedene Akteure involviert. Dies birgt die Gefahr, dass es in der Praxis schwierig werden könnte, eine Organisation für die unrechtmässige Datenbearbeitung verantwortlich zu machen.[1420]

Schliesslich wurde auch eine Eigenkontrolle in den EU-IOP-VO verankert. Gemäss dieser müssen die Schengen/Dublin-Staaten sowie die zuständigen EU-Stellen sicherstellen, dass die auf die Interoperabilitätskomponenten zugriffsberechtigten Behörden die erforderlichen Massnahmen zur Überwachung der Einhaltung der Bestimmungen der EU-IOP-VO ergreifen sowie ggf. mit der Aufsichtsbehörde zusammenarbeiten. Die ordnungsgemässe Datenverarbeitung wird insbesondere durch das häufige Überprüfen der Protokolle, welche über die Datenbearbeitungen im ESP, BMS, CIR und MID zu erstellen sind, sichergestellt.[1421]

Insgesamt zeigt sich also, dass verschiedene Aufsichtsmechanismen vorhanden sind. Deren Effektivität dürfte jedoch stark von der jeweiligen Umsetzung abhängen.

3.4.8.4 *Haftung und Sanktionen*

Die EU-IOP-VO enthalten Bestimmungen zur Haftung resp. zu den Sanktionen.[1422] Mit Schadenersatzvorschriften sollen Nachteile ausgeglichen werden können, welche mit den Datenschutzregeln hätten verhindert werden sollen. Die Akteure, welche Daten bearbeiten, sollen für ihr Fehlverhalten haften. Mit den Schadenersatzvorschriften wird Druck auf sie ausgeübt, die Datenschutz-

Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten teilweise derselben organisatorischen Struktur zugehörig sind, wie die um Einsicht ersuchende Behörde. Dies ist grundsätzlich der Unabhängigkeit abträglich. Siehe dazu FRA, Opinion IOP, 31. Siehe zur Umsetzung von Art. 22 EU-IOP-VO in der Schweiz Kapitel V.3.4.3.3.e).

1420 Vgl. dazu BROUWER, A point of no return. Siehe dazu auch EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 23, wonach sich die Komplexität auch auf die Verwaltung und Kontrolle der Systeme auswirkt. Da IT-Grosssysteme sich in einschneidender Weise auf die Grundrechte von natürlichen Personen auswirken, ist eine effiziente und starke unabhängige Aufsicht vorzusehen.

1421 Siehe dazu Art. 44 EU-IOP-VO. Siehe zur Protokollierungspflicht bei den Interoperabilitätskomponenten Art. 10 EU-IOP-VO; Art. 16 EU-IOP-VO; Art. 24 EU-IOP-VO; Art. 36 EU-IOP-VO.

1422 Siehe zur Haftung Art. 46 EU-IOP-VO und zu den Sanktionen Art. 45 EU-IOP-VO.

vorschriften einzuhalten. Die vorgesehene Haftung ist verschuldensabhängig. Kann sich ein Akteur exkulpieren, entsteht eine Haftungslücke und die geschädigte Person bleibt auf ihrem Schaden sitzen. Des Weiteren ergibt sich der Umfang der Schadenersatzpflicht aus dem nationalen Recht. Die effektive Ausgestaltung des Schadenersatzanspruchs kann deshalb in jedem Schengen/Dublin-Staat anders geregelt sein. Dies kann zu Ungleichheiten führen.[1423]

Ähnlich wie die Schadenersatzvorschriften tragen auch die Sanktionen dazu bei, dass die Datenbearbeitungsgrundsätze eingehalten werden und Missbrauch verhindert wird.[1424] Die Ausgestaltung dieser Sanktionen ist im nationalen Recht zu regeln. Obwohl diese gemäss dem EU-Recht wirksam, verhältnismässig und abschreckend sein müssen, lässt dies den Schengen/Dublin-Staaten viel Ermessen betreffend deren Ausgestaltung. Somit ist nicht nur bei den Haftungsbestimmungen, sondern auch bei den Sanktionsbestimmungen mit unterschiedlichen Regelungsarten zu rechnen.

3.4.9. Bewertung

Die durch die Interoperabilität ermöglichten Datenbearbeitungen wirken sich verschiedentlich auf den Schutz der betroffenen Daten aus. So werden durch die Schaffung von grossen Datenspeichern, insbesondere dem CIR, neue (Sicherheits-)Risiken für die dort gespeicherten Daten geschaffen. Auch verändert die Interoperabilität die Zugangsbedingungen der Abfrage der Systeme VIS, Eurodac, EES und ETIAS zum Zwecke der Verhinderung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten. Wie aus der vorliegenden Analyse hervorgeht, ist damit eine Herabsetzung der bereits bestehenden Sicherheitsmassnahmen verbunden. Davon abgesehen dürfen die im CIR gespeicherten Daten auch für neue Abfragen verwendet werden. Damit sind zusätzliche Datenbearbeitungen verbunden, welche jeweils neue Risiken mit sich bringen können. Es ist zu begrüssen, dass in den EU-IOP-VO verschiedene Sicherheitsmassnahmen vorgesehen sind, damit solche Risiken geringgehalten werden können. Die Effektivität dieser Sicherheitsmassnahmen dürfte jedoch – zumindest teilweise – stark von deren konkreten Umsetzung abhängen.

So kommt z.B. der festzulegenden Mindestqualität, welche die Daten aufweisen müssen, ehe sie im CIR resp. BMS gespeichert werden dürfen, eine zentrale Rolle zu. Denn diese trägt dazu bei, dass die Daten korrekt sind. Dies

1423 Vgl. dazu MATZ, 242 ff.
1424 Vgl. dazu Art. 45 EU-IOP-VO.

wirkt sich wiederum positiv auf die im Rahmen der Interoperabilität vorgesehenen Identifizierungen von Personen aus, da nur mit korrekten Daten auch eine korrekte Identifizierung resp. Nicht-Identifizierung vorgenommen werden kann. Des Weiteren kommt auch den Rechten der betroffenen Personen eine wichtige Rolle zu, da aufgrund verschiedener Fehlerquellen damit zu rechnen ist, dass auch falsche Daten bearbeitet werden. Dies kann mit verschiedenen negativen Folgen für die betroffene Person verbunden sein. In solchen Situationen ist es entscheidend, dass die Personen über das Recht verfügen, falsche Daten berichtigen resp. löschen zu lassen. Da bereits aktuell die Vermutung besteht, dass die Geltendmachung dieser Rechte für die Betroffenen zu unübersichtlich ist, ist die Einführung eines Web-Portals sicherlich zu begrüssen. Wichtig erscheint, dass dieses den betroffenen Personen die für die Geltendmachung ihrer Rechte notwendigen Informationen tatsächlich zur Verfügung stellt. Zudem dürfte die Qualität der Aufsicht stark davon abhängen, ob die Aufsichtsbehörden über ausreichende Ressourcen verfügen.

Aus den obigen Ausführungen geht hervor, dass verschiedene durch die Interoperabilität ermöglichte Datenbearbeitungen nicht verhältnismässig erscheinen. Die damit verfolgten öffentlichen Interessen sind zwar jeweils erheblich und legitim, sie vermögen jedoch den Schutz der personenbezogenen Daten teilweise nicht zu überwiegen. Insofern liegt in Bezug auf diese Datenbearbeitungen ein Ungleichgewicht zwischen den sich *in casu* gegenüberstehenden Interessen vor.

Wie bereits oben aufgezeigt, wäre eine datenschutzfreundliche(re) Ausgestaltung von verschiedenen Datenbearbeitungen der Interoperabilität durchaus möglich. So hätten bspw. griffigere Massnahmen für die Bekämpfung des Identitätsbetrugs vorgesehen werden müssen. Des Weiteren hätte bei der Abfrage gemäss Art. 22 EU-IOP-VO die Erforderlichkeit der anvisierten Erleichterung sowie Vereinheitlichung einer bereits bestehenden Abfrage eingehender begründet werden müssen. Wäre dies gelungen, hätten verschiedene Sicherheitsmassnahmen dazu führen können, dass dem Schutz der personenbezogenen Daten besser hätte entsprochen werden können.

4. Fazit

Indem die Interoperabilität diverse Bearbeitungen von personenbezogenen Daten vorsieht, welche von verschiedenen Stellen der EU sowie den Schengen/Dublin-Staaten vorgenommen werden dürfen, stellt sie einen Eingriff in das Grundrecht auf Datenschutz dar.

Bei der Prüfung der Rechtfertigung dieses Eingriffs wurde festgestellt, dass mit den EU-IOP-VO grundsätzlich eine gesetzliche Grundlage vorliegt (wobei auf eine abschliessende Beurteilung bezüglich Art. 20 EU-IOP-VO verzichtet wurde). Nicht ausser Acht gelassen werden darf jedoch, dass deren Umfang sowie auch die zahlreichen Verweise auf andere EU-Rechtsakte es den betroffenen Personen erschweren, das Ausmass der Interoperabilität zu erfassen und ihr Verhalten danach zu richten.

Des Weiteren wurden verschiedene öffentliche Interessen identifiziert, welche mit der Interoperabilität verfolgt werden. Die Wahrung der inneren Sicherheit steht dabei im Fokus. Da mit der Interoperabilität auch die EU-Informationssysteme effizienter genutzt werden sollen, wird damit auch zur Wahrung der von diesen Systemen verfolgten öffentlichen Interessen beigetragen. Dabei handelt es sich abgesehen von der Wahrung der inneren Sicherheit um das Interesse an einem wirksamen Management der Schengen-Aussengrenzen sowie einer wirksamen Umsetzung der Asyl- und der Visapolitik.

Bezüglich dem Kerngehalt hat sich gezeigt, dass in den EU-IOP-VO zahlreiche Sicherheitsmassnahmen vorgesehen wurden, welche das Risiko einer missbräuchlichen Verwendung der Daten möglichst minimieren sollen. Des Weiteren stehen die bearbeiteten Daten zumindest grösstenteils im Zusammenhang mit Aufenthalten von Drittstaatsangehörigen im Schengen-Raum. Die Datenbearbeitung beschränkt sich also auf einen bestimmten Teil des Privatlebens der Betroffenen und lässt diese dadurch nicht gläsern erscheinen. Da die beiden Abfragemöglichkeiten gemäss Art. 20 EU-IOP-VO sehr vage gehalten sind und insbesondere kein konkreter Zweck dieser Datenbearbeitungen auf EU-Ebene festgelegt wurde, könnte sich die Frage stellen, ob damit in den Kerngehalt eingegriffen wird. Da sich die Regelung gemäss Art. 20 EU-IOP-VO als unverhältnismässig erweisen wird, wurde diese Frage bewusst offengelassen.

Bei der Prüfung der Verhältnismässigkeit wurden die vier Interoperabilitätskomponenten sowie die drei Abfragen des CIR einzeln analysiert. Aus dieser Analyse ging hervor, dass die Komponenten ESP und BMS aus datenschutzrechtlicher Perspektive verhältnismässig erscheinen. Der CIR als Datenbank, die drei Abfragen des CIR sowie der MID sind diesbezüglich differenzierter zu betrachten.

Aktuell wird der Zugriff auf die von der Interoperabilität umfassten Systeme zwecks Verhinderung, Aufdeckung sowie Untersuchung terroristischer oder sonstiger schwerer Straftaten nur unter strengen Voraussetzungen gewährt. Die bestehenden Sicherheitsmassnahmen werden durch Art. 22 EU-IOP-VO geschwächt. Dies erscheint insbesondere mangels eines nachgewiesenen, ein-

deutigen Bedürfnisses der abfrageberechtigten Behörden unverhältnismässig, zumal diese Abfrage ursprünglich nur unter der Bedingung der aktuell geltenden strengen Voraussetzungen gewährt wurde.

Der Zugang des CIR zwecks Identifizierung gemäss Art. 20 EU-IOP-VO, welcher zwei Abfragemöglichkeiten vorsieht, vermag den Anforderungen des Grundrechts auf Datenschutz (ebenfalls) nicht standzuhalten. Diese Bestimmung ist derart vage formuliert, dass der Zweck dieser Abfragemöglichkeiten nicht bzw. nicht eindeutig erkennbar ist. Auch unter Berücksichtigung, dass es grösstenteils den Schengen/Dublin-Staaten überlassen ist, die Verfahren und Bedingungen dieser Abfragemöglichkeiten im nationalen Recht zu regeln, fehlt es im EU-Recht an klaren und präzisen Regeln zur Datenbearbeitung. Die Regelung gemäss Art. 20 EU-IOP-VO ist demnach nicht verhältnismässig.

Weiter erscheint die Regelung der Abfrage des CIR zwecks Aufdeckung von Mehrfachidentitäten gemäss Art. 21 EU-IOP-VO und die damit zusammenhängende Datenbearbeitung beim MID unbefriedigend. Bei Art. 21 EU-IOP-VO besteht die Gefahr, dass im Rahmen dieser Abfrage erlangte Daten missbräuchlich verwendet werden. Die Regelung des MID versäumt es zudem, konkrete Massnahmen, welche bei der Aufdeckung eines Identitätsbetrugs zu ergreifen sind, vorzusehen. Dadurch kann nicht sichergestellt werden, dass ein im Rahmen der Interoperabilität entdeckter Identitätsbetrug auch wirklich bekämpft wird. Die aktuelle Regelung erscheint deshalb nicht verhältnismässig.

Mit der Schaffung des CIR werden die darin gespeicherten Daten einem grösseren Sicherheitsrisiko ausgesetzt. Aufgrund der Anzahl sowie des Informationswertes der Daten ist zudem zu befürchten, dass diese zukünftig aufgrund eines vermeintlichen Bedarfs für weitere Datenbearbeitungen beansprucht werden (oder weitere Datenbanken an den CIR angeschlossen werden). Noch vor ein paar Jahren wurde eine Datenbank, welche bestimmte (Identitäts-)Angaben eines umfangreichen Personenkreises hätte speichern sollen, als nicht verhältnismässig beurteilt. Diese Ansicht erscheint mittlerweile offenbar überholt. Das Risiko von missbräuchlichen Datenbearbeitungen sowie Zweckerweiterungen ist jedoch nicht unbeachtlich. In diesem Sinne wäre sicherzustellen gewesen, dass nur möglichst wenige Daten gespeichert werden und dass eine allfällige Vergrösserung des CIR (einerseits in Bezug auf die darin gespeicherten Daten als auch andererseits hinsichtlich der Datenbanken, deren Daten im CIR gespeichert werden) resp. eine allfällige Zweckerweiterung auf das absolut Notwendige beschränkt werden.

Zusammenfassend ergibt sich aus den obigen Ausführungen, dass sich verschiedene Datenbearbeitungen der Interoperabilität als nicht verhältnismäs-

sig erwiesen haben. Insofern kommt die vorliegende Untersuchung zum Schluss, dass die aktuelle Ausgestaltung der Interoperabilität nicht in allen Teilen mit dem grundrechtlich geschützten Datenschutz vereinbar ist.

VI. Schlussbemerkungen

Im Rahmen einer Schlussbetrachtung wird im Folgenden die bisherige Entwicklung der Interoperabilität in den Kontext vergangener und aktueller sicherheitspolitischer Erwägungen gesetzt. Es zeigt sich, welche Umstände zur Entstehung der Interoperabilität beigetragen haben, welche wohl noch vor ein paar Jahren undenkbar gewesen wäre. Mit Blick auf die Zukunft wird im Anschluss versucht, mögliche Einflüsse der Interoperabilität auf künftige Datenbearbeitungen von Informationssystemen zu antizipieren resp. mögliche Weiterentwicklungen der Interoperabilität zu prognostizieren.

1. Kontext der Entstehungsgeschichte der Interoperabilität

Der Fortschritt der Technologie ermöglicht es, dass immer grössere Mengen an Daten verarbeitet werden können. Diese Datenbearbeitungen werden für die betroffenen Individuen zunehmend undurchsichtiger. Mittlerweile sind enorm grosse Datenbestände vorhanden. Diese werden zunehmend miteinander abgeglichen resp. analysiert, um daraus Erkenntnisse zum Privatleben der betroffenen Personen zu ziehen. Der Einsatz von neuen Technologien kann grundsätzlich sehr wertvoll sein. Damit geht aber oftmals auch ein grosses Missbrauchspotential miteinher. So zeigten z.B. die Enthüllungen von Edward Snowden im Jahr 2013, welche grossangelegte Überwachungen des Internets und der Telekommunikation durch Nachrichtendienste einiger Staaten offenlegten, Gefahren von Überwachungstechnologien auf.[1425] Die Snowden-Enthüllungen haben auf eindrückliche Weise offenbart, dass Massenüberwachungen begrenzt und kontrolliert, wenn nicht sogar verboten werden sollten. Dem Datenschutz wurde danach wieder mehr Beachtung geschenkt.[1426]

Eine Reihe von Terroranschlägen in verschiedenen europäischen Städten hat diese Entwicklung jedoch wieder stark gebremst und für eine Verschiebung der Prioritäten weg vom Datenschutz hin zur (Massen)Überwachung gesorgt. Diese wurde als notwendig und hilfreich zur Aufarbeitung resp. Verhinderung von Terroranschlägen und somit zur Erhöhung der inneren Sicherheit er-

---

1425 Vgl. zum Ganzen FRA/Europarat/EDSB, Handbuch, 411 ff. Siehe zu den Enthüllungen und den anschliessenden Entwicklungen Edgar.

1426 Rusinova, 17.

achtet. Verschiedene europäische Staaten haben entsprechendes nationales Recht erlassen.[1427] Im Kontext dieser terroristischen Anschläge sowie auch der Migrationskrise, also in einer Phase, in welcher dem Bedürfnis nach Sicherheit wieder vermehrt Rechnung getragen wurde, entstand schliesslich die Interoperabilität.[1428] Die Priorisierung dieses Interesses und die damit verbundene Herabsetzung des Interesses des Datenschutzes zeigt sich in der Ausgestaltung der Interoperabilität. Die Begründungen für die Einführung einer neuen Datenbearbeitung sind aus juristischer Sicht oft dürftig. Die Hauptmotivation zu solchen Neuerungen dürfte darin liegen, die ohnehin im Rahmen der einzelnen Systeme erhobenen Daten möglichst vielseitig zu nutzen, um die innere Sicherheit zu gewährleisten.

Die Einbettung der Entstehung der Interoperabilität in den Kontext der Terroranschläge und der Migrationskrise macht deutlich, dass diese vor allem durch den technischen Fortschritt sowie aufgrund der damaligen sicherheitspolitischen Lage ermöglicht werden konnte.[1429] Insofern ist davon auszugehen, dass die Interoperabilität noch vor einigen Jahren weder aus technischer noch aus politischer oder juristischer Sicht möglich gewesen wäre.[1430] Im Jahr 2010 hatte die Kommission nämlich noch festgehalten, dass «*ein einziges, übergreifendes und vielseitig einsetzbares EU-Informationssystem*» zwar ein «*Höchstmass an Informationsaustausch*» ermöglichen könnte. Das Recht auf Privatsphäre und Datenschutz der Einzelnen würde dadurch jedoch in grober und rechtswidriger Weise eingeschränkt. Ausserdem sei ein solches System «*äusserst schwer zu entwickeln und zu betreiben*». Im Bereich Freiheit, Sicherheit und Recht hätten sich verschiedene Informationssysteme unterschiedlicher Art entwickelt. Diese unterteilte Struktur des Informationsmanagements könne die Rechte der Bürger auf Privatsphäre besser wahren «*als dies jede zentralisierte Alternative leisten könnte*».[1431] Mit der Interoperabilität werden nun aber genau solche zentralisierten Lösungen anvisiert. Insbesondere mit dem CIR, aber auch mit dem BMS, werden zentrale Speicher geschaffen, welche

1427 Siehe dazu RUSINOVA, 17 ff. m.w.H.

1428 Siehe zur Entstehungsgeschichte der Interoperabilität ausführlich Kapitel IV.3 und IV.4.

1429 Die EU-IOP-VO wurden zudem auch relativ zügig verabschiedet. Siehe dazu QUINTEL, Privacy.

1430 Vgl. dazu JONES, 38. Auch am Beispiel von ETIAS zeigt sich, dass die Idee für ein solches System bereits im Jahr 2008 vorhanden war. Aufgrund von Zweifeln der Kommission an der Notwendigkeit eines solchen Systems wurde dieses jedoch nicht umgesetzt. Im Zuge der terroristischen Attentate lebte die Idee schliesslich wieder auf und es wurden entsprechende gesetzliche Grundlagen in Kraft gesetzt. Siehe dazu ALEGRE/JEANDESBOZ/VAVOULA, 14; VAVOULA, Right to Private Life, 246.

1431 Siehe dazu EUROPÄISCHE KOMMISSION, KOM(2010)385 endg., 4.

bestimmte Daten von verschiedenen Informationssystemen speichern. Damit sollen systemübergreifende Abfragen ermöglicht werden. Diese verfolgen jeweils einen eigenen Zweck. Damit dürfte der CIR nicht mehr weit von einem einzigen, übergreifenden und vielseitig einsetzbarem EU-Informationssystem entfernt sein.[1432] Dass ein solches System noch vor ein paar Jahren – aufgrund datenschutzrechtlicher Bedenken – undenkbar gewesen war, zeigt, dass sich die Haltung – aufgrund des gestiegenen Bedürfnisses nach Sicherheit – in Bezug auf die Struktur und die Ausgestaltung von Informationssystemen stark geändert hat.

2. Paradigmenwechsel im Datenmanagement von Informationssystemen

Zwischen den bereits in Betrieb genommenen Informationssystemen gab es bis anhin nur vereinzelt Berührungspunkte. Bei den Systemen, deren Inbetriebnahme noch bevorsteht, ist eine Zunahme solcher Berührungspunkte zu verzeichnen. Teilweise wurden sogar bereits gemeinsame technische Komponenten vorgesehen.[1433] Die Interoperabilität fügt dieser Entwicklung insofern eine neue Dimension hinzu, als für sechs Informationssysteme verschiedene gemeinsame technische Komponenten geschaffen werden, welche die Systeme miteinander verknüpfen sollen. Der Ansatz der eigenständigen, isolierten Ausgestaltung der Systeme wurde bei der Entstehung der Interoperabilität nämlich als Schwäche angesehen, da die vorhandenen Daten dadurch nicht vollumfänglich genutzt werden könnten.[1434] Die Interoperabilität bricht deshalb die eigenständige Struktur der EU-Informationssysteme auf und schafft durch die Einführung der vier Komponenten eine enge Vernetzung dieser Informationssysteme. In diesem Sinne stellt die Interoperabilität einen Paradigmenwechsel im Datenmanagement von Informationssystemen dar.[1435]

1432 Vgl. dazu VAVOULA, Deathblow, 143 f.

1433 Siehe dazu Kapitel III.10.

1434 VAVOULA, Assessment, 173 f. Vgl. dazu auch VAVOULA, IOP Privacy.

1435 In seiner Stellungnahme zu den Vorschlägen der EU-IOP-VO hat der EDSB festgehalten, dass «*the decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a ‹point of no return›*». Siehe dazu EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 25.

3. Ausblick

In der Annahme, dass in der nächsten Zeit das Bedürfnis nach Sicherheit nicht sinken wird, wird im Folgenden anhand der in der vorliegenden Untersuchung gewonnenen Erkenntnisse versucht, mögliche – durch die Interoperabilität angestossene – Entwicklungen zu antizipieren.

Am Beispiel der sukzessiven Gewährung der Abfrage der Systeme VIS, Eurodac, EES und ETIAS zu Zwecken der Verhinderung, Aufdeckung sowie Untersuchung von terroristischen und sonstigen schweren Straftaten hat sich bereits gezeigt, dass eine Datenbearbeitung zunehmend weniger in Frage gestellt wird, wenn sie bereits bei anderen Informationssystemen vorgenommen wird. Vor allem als die Hürde zum Zugang zu Eurodac-Daten überwunden war, wurden die Erforderlichkeit sowie die Effektivität dieses Zugangs immer weniger kritisch hinterfragt. Mit Verweis darauf, dass eine solche Abfrage bereits bei anderen Systemen vorhanden ist, wurde zunehmend weniger begründet, weshalb eine entsprechende Abfrage auch bei anderen Systemen vorzusehen ist.[1436] Im Sinne dieses Beispiels besteht die Gefahr, dass gewissermassen am Vorbild der Interoperabilität, mit dieser in Verbindung stehende Entwicklungen in anderen Bereichen zunehmend weniger begründet werden. Diese im Datenschutz zu beobachtende Tendenz ist bedenklich. So verlangt doch der grundrechtlich geschützte Datenschutz, dass eine Datenbearbeitung hinsichtlich ihrer Notwendigkeit begründet und stets auf das absolut Notwendige begrenzt wird.

Wie bereits aufgezeigt wird mit der Interoperabilität die bisher eigenständige Struktur der Systeme aufgebrochen und es werden gemeinsame Komponenten geschaffen. Damit ist ein Paradigmenwechsel im Datenmanagement von Informationssystemen verbunden. Obwohl auch bereits die noch in Betrieb zu nehmenden Systeme, welche von der Interoperabilität betroffen sind, vermehrt Berührungspunkte zueinander aufweisen, dürfte insbesondere die Interoperabilität dazu beitragen, dass auch bei anderen Systemen vermehrt verknüpfende Elemente geschaffen werden könnten.

Zudem zeigt sich am Beispiel des Zugangs des CIR zwecks Identifizierungen gemäss Art. 20 EU-IOP-VO, dass die in den Systemen erhobenen Daten für zusätzliche Zwecke verwendet werden dürfen. Solche Zweckerweiterungen sind bei einigen Informationssystemen nicht neu. So wurde bereits die Abfrage der nationalen Strafverfolgungsbehörden sowie von Europol auf Daten des VIS,

[1436] Siehe dazu Kapitel V.3.4.3.2.

Eurodac, EES und ETIAS zu Zwecken der Verhinderung, Aufdeckung sowie Untersuchung terroristischer oder sonstiger schwerer Straftaten als sog. sekundäres Ziel in die gesetzlichen Grundlagen der genannten Systeme aufgenommen.[1437] Mit der Abfrage gemäss Art. 20 EU-IOP-VO kommt nun ein weiterer Zweck hinzu. Insofern dürfte es nicht überraschen, wenn zukünftig bereits erhobene Daten auch für zusätzliche Zwecke bearbeitet werden dürfen. Insbesondere könnte auch die Schaffung des CIR, also eines Speichers mit einer umfassenden Sammlung an alphanumerischen sowie biometrischen Daten von einem grossen Personenkreis, diese Tendenz insofern noch verstärken, als die im CIR gespeicherten Daten potenziell für weitere Zwecke nützlich sein könnten. Davon abgesehen könnte die Errichtung des CIR dazu führen, dass zukünftig keine Systeme mehr für einen bestimmten Zweck errichtet werden, sondern primär grosse Speicher geschaffen werden, um die darin vorhandenen Daten für mannigfaltige Zwecke verwenden zu können.

Die Verschiedenartigkeit der Zwecke verdeutlicht zudem, dass Informationssysteme für jegliche Zwecke nutzbar gemacht werden können, sofern diese nicht unvereinbar mit dem ursprünglichen Zweck der Systeme erscheinen. Die bisherigen Zweckerweiterungen der Systeme deuten darauf hin, dass die Hürde einer solchen Unvereinbarkeit der Zwecke sehr hoch angesetzt sein dürfte. Dadurch könnten die Anwendungsbereiche von Informationssystemen weiter ausgedehnt werden.[1438] Bereits durch die mit der Interoperabilität eingeführten Zweckerweiterungen werden die Ziele der inneren Sicherheit mit denjenigen der Migrationskontrolle zunehmend vermischt.[1439] Die Gefahr dieser Entwicklung besteht darin, dass die Grenzen zwischen den Bereichen Migration und Strafbekämpfung zusehends verblassen und letztlich das Risiko besteht, dass Terroristen, Kriminelle sowie Drittstaatsangehörige einander gleichgesetzt werden könnten. Aus den Massnahmen und Zielen in den Bereichen Migration und polizeiliche Zusammenarbeit gehen zwar gewisse Synergien hervor. Dennoch handelt es sich dabei um zwei verschiedene Politikbereiche und öffentliche Interessen.[1440]

1437 Siehe dazu Kapitel III.10.

1438 Siehe dazu VAVOULA, IOP Privacy.

1439 MICHÉA, 51 ff. m.w.H.

1440 Vgl. dazu EDSB, Reflexionspapier IOP, N 21 f.; EDSB, Stellungnahme Vorschläge EU-IOP-VO, N 20. So hat die Kommission zwar argumentiert, dass die Bereiche Grenzmanagement, Migrationssteuerung sowie Strafbekämpfung miteinander verknüpft seien, weil bspw. die Routen der irregulären MigrantInnen auch von Personen mit terroristischen Absichten benutzt würden, um in den Schengen-Raum zu gelangen. Siehe dazu EUROPÄISCHE KOMMISSION, COM(2016) 205 final, 2. Europol hat vor ein paar Jahren zwar bestätigt, dass es Fälle gibt, in welchen Terroristen die Migrationsströme genutzt haben. Es gebe hinge-

Des Weiteren hat sich am Beispiel der Abfrage des CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten gemäss Art. 22 EU-IOP-VO gezeigt, dass bestehende Sicherheitsmassnahmen – ohne dies eingehend zu diskutieren – herabgesetzt werden. Dies ist insofern stossend, als dass diese Abfrage ursprünglich nur unter der Bedingung von strengen Zugangsvoraussetzungen gewährt wurde. Es ist zwar möglich, dass sich eine Beurteilung der Sicherheitsmassnahmen und damit der Verhältnismässigkeit im Laufe der Zeit verändert. Da der Zugang der nationalen Strafverfolgungsbehörden sowie Europol zu Daten aus dem VIS, Eurodac, EES und ETIAS jedoch zum Zeitpunkt der Gewährung dieser Abfrage (teilweise) höchst umstritten war, wäre es zumindest angezeigt gewesen, klar darzulegen, weshalb sich eine Herabsetzung der Sicherheitsmassnahmen aufdrängt. So jedoch besteht die Gefahr, dass auch bei anderen Datenbearbeitungen – gewissermassen am Vorbild der Interoperabilität – die Sicherheitsmassnahmen ohne eingehende Begründung herabgesetzt werden.

Abgesehen davon ist auch anzunehmen, dass sich der Anwendungsbereich der Interoperabilität – nach deren Inbetriebnahme – zunehmend vergrössern wird. Der Entstehungsprozess der Interoperabilität zeigt nämlich auf, dass abgesehen von den erwähnten EU-Informationssystemen auch geprüft wurde, ob noch andere Systeme resp. Daten in die Interoperabilität integriert werden könnten. Es ist deshalb zu erwarten, dass künftig weitere Systeme resp. Daten in der einen oder anderen Form in die Interoperabilität eingebunden werden. Ein solcher Einbezug könnte bspw. aus einer Verknüpfung der Systeme der Prüm-Zusammenarbeit, den PNR-Daten oder anderen Fluggastdaten (den sog. API-Daten) mit einer oder mehreren Interoperabilitätskomponenten bestehen.[1441] Eine solche Vergrösserung des Anwendungsbereichs der Interoperabilität könnte dazu führen, dass vermehrt auch Daten von Staatsangehörigen der Schengen/Dublin-Staaten, und nicht mehr fast ausschliesslich von Drittstaatsangehörigen, bearbeitet würden.[1442]

Obwohl die Interoperabilität grundsätzlich ein eigenständiges Projekt darstellt, ist insgesamt davon auszugehen, dass der mit der Interoperabilität vor-

gen keine konkreten Anhaltspunkte, dass Terroristen systematisch die Flüchtlingsströme nutzten, um nach Europa zu reisen. Somit liege kein direkter Zusammenhang zwischen (irregulärer) Migration und Terrorismus vor. Siehe dazu EUROPOL, Terrorism Situation 2016, 7.

1441 Siehe dazu VAVOULA, Deathblow, 154. Vgl. zum Anschluss weiterer Systeme an die Interoperabilität auch QUINTEL, Privacy. Siehe zu den API-Daten VAVOULA, Police Information Exchange, 44 ff.

1442 Vgl. dazu JONES, 38.

genommene Paradigmenwechsel sowie die anderen vorgenannten Entwicklungen der Interoperabilität auch auf andere Systeme übergreifen werden. So dürfte die Interoperabilität der EU-Informationssysteme als Vorbild dienen, um auch andere Systeme miteinander zu verknüpfen und (weitere) Zweckerweiterungen resp. Herabsetzungen von bestehenden Sicherheitsmassnahmen einzuführen. Da die Interoperabilität den Weg zu solchen Entwicklungen gewissermassen geebnet hat, ist zu befürchten, dass diese künftig nicht mehr kritisch hinterfragt werden. Ob sich diese Prognosen bewahrheiten, wird sich erst in der Zukunft zeigen. Zuerst sind jedoch erste Praxiserfahrungen nach der Inbetriebnahme der Interoperabilität mit Spannung zu verfolgen.

Curriculum Vitae

Livia Matter erlangte den Bachelor of Law an der Universität Basel. Nach einem mehrmonatigen (Sprach-)Aufenthalt in Argentinien absolvierte sie den bilingualen Master of Law an den Universitäten Basel und Genf.

Nach verschiedenen Volontariaten (u.a. an einem erstinstanzlichen Zivilgericht und in einem multinationalen Pharmaunternehmen) war sie während rund zwei Jahren als Fachspezialistin Asyl beim Staatssekretariat für Migration (SEM) tätig. Im Anschluss begann sie als Diplomassistentin am Lehrstuhl für Völkerrecht, Europarecht und öffentliches Recht an der Universität Freiburg i.Ue. Es folgte eine befristete Anstellung als Assistentin bei der FernUni Schweiz sowie ein dreimonatiger Forschungsaufenthalt am European University Institute (EUI) in Florenz. Seit 2021 arbeitet sie als Juristin im Fachbereich Europarecht und Koordination Schengen/Dublin beim Bundesamt für Justiz (BJ).

Die EU betreibt in den Bereichen Migration, Sicherheit und Grenzmanagement bereits verschiedene Datenbanken. Weitere sind geplant und werden in den kommen Jahren den Betrieb aufnehmen. Mit der Interoperabilität der EU-Informationssysteme sollen diese Datenbanken – anhand von vier technischen Komponenten – miteinander verknüpft werden. Damit sind verschiedene neue Datenbearbeitungen verbunden. Da die Mehrheit dieser Datenbanken sowie auch die Interoperabilität selbst sogenannte Schengen/Dublin-Weiterentwicklungen darstellen, beteiligt sich auch die Schweiz an diesen Projekten. Die vorliegende Dissertation untersucht, inwiefern diese neuen Datenbearbeitungen mit dem grundrechtlichen Anspruch auf Datenschutz vereinbar sind. Dabei steht die Perspektive der Schweiz im Fokus.