Rat der
Europäischen Union

Brüssel, den 25. Juli 2022
(OR. en)

11583/22

DATAPROTECT 229
JAI 1070
DIGIT 149
MI 595
FREMP 164

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	25. Juli 2022
Empfänger:	Generalsekretariat des Rates
Nr. Komm.dok.:	COM(2022) 364 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Erster Bericht über die Anwendung und Wirkungsweise der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung)

Die Delegationen erhalten in der Anlage das Dokument COM(2022) 364 final.

Anl.: COM(2022) 364 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 25.7.2022
COM(2022) 364 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Erster Bericht über die Anwendung und Wirkungsweise der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung)

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Erster Bericht über die Anwendung und Wirkungsweise der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung)

Inhaltsverzeichnis

1 DIE RICHTLINIE ZUM DATENSCHUTZ BEI DER STRAFVERFOLGUNG ALS WICHTIGSTES INSTRUMENT ZUR SICHERSTELLUNG DES DATENSCHUTZES IN DER SICHERHEITSPOLITIK DER EUROPÄISCHEN UNION

In dieser Mitteilung wird der erste Bericht der Kommission über die Bewertung und Überprüfung der Richtlinie (EU) 2016/680[1] (im Folgenden „Richtlinie zum Datenschutz bei der Strafverfolgung“ oder „Richtlinie“) gemäß Artikel 62 Absatz 1 jener Richtlinie dargelegt.

Im Rahmen des Berichts werden insbesondere die Anwendung und Wirkungsweise der Vorschriften der Richtlinie zum Datenschutz bei der Strafverfolgung über die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen geprüft, wie dies in jener Richtlinie verlangt wird, jedoch verfolgt der Bericht auch einen breiteren Ansatz. Er verortet die Richtlinie im Rahmen des EU-Rechts über den Schutz personenbezogener Daten und des EU-Rechts zur Regelung der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (im Folgenden „Strafverfolgung“)[2]. Der Bericht bietet einen Überblick über die Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung in das nationale Recht der Mitgliedstaaten, stellt die ersten Erkenntnisse über die Anwendung und Wirkungsweise der Richtlinie dar und zeigt das weitere Vorgehen auf.

1.1 Ein wichtiges Element eines einheitlichen Datenschutzrahmens der Europäischen Union

Die Richtlinie zum Datenschutz bei der Strafverfolgung ist einer der drei Pfeiler des EU-Rahmens zur Gewährleistung des Grundrechts auf Schutz personenbezogener Daten. Die anderen beiden sind die Datenschutz-Grundverordnung (im Folgenden „DSGVO“)[3] und die EU-Datenschutzverordnung für die Organe, Einrichtungen und sonstigen Stellen der Union (im Folgenden „EU-DSVO“)[4]. Das Grundrecht auf Datenschutz ist in Artikel 8 der Charta der

---

[1] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates 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).
[2] Artikel 1 Absatz 1 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[3] 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 (ABl. L 119 vom 4.5.2016, S. 1).
[4] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

Grundrechte der Europäischen Union (im Folgenden „Charta“)[5] und in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (im Folgenden „AEUV“)[6] verankert.

Die Richtlinie zum Datenschutz bei der Strafverfolgung trat am 6. Mai 2016 in Kraft und musste von den Mitgliedstaaten bis zum 6. Mai 2018 umgesetzt werden[7].

Die Richtlinie zum Datenschutz bei der Strafverfolgung ist der erste Rechtsakt der EU, der auf einem umfassenden Ansatz für den Schutz personenbezogener Daten bei deren Verarbeitung durch die zuständigen Behörden (d. h. Justizbehörden, die Polizei und andere Strafverfolgungsbehörden gemäß Artikel 3 Nummer 7 der Richtlinie) zum Zwecke der Strafverfolgung beruht. Die Richtlinie stellt im Vergleich zum Rahmenbeschluss 2008/977/JI des Rates[8], der durch sie aufgehoben und ersetzt wurde, einen wichtigen Fortschritt mit Blick auf die Sicherstellung der einheitlichen Anwendung der Datenschutzvorschriften in der gesamten EU dar. Erstens bietet die Richtlinie ein vollständiges Regelwerk für sowohl die grenzüberschreitende als auch die innerstaatliche Verarbeitung personenbezogener Daten zum Zwecke der Strafverfolgung, während der Rahmenbeschluss des Rates lediglich die grenzüberschreitende Verarbeitung behandelte. Zweitens bietet die Richtlinie ein umfassendes und horizontales Regelwerk, wohingegen es beim vorherigen Ansatz so war, dass jeder sektorspezifische Rechtsakt der EU, der die Verarbeitung personenbezogener Daten im Kontext der Strafverfolgung vorsah, seinen eigenen Datenschutzvorschriften unterlag[9].

Die DSGVO, die EU-DSVO und die Richtlinie zum Datenschutz bei der Strafverfolgung beruhen auf ähnlichen Konzepten und Grundsätzen[10], was die einheitliche Auslegung und Anwendung der EU-Datenschutzvorschriften zur Folge hat. Sie teilen gemeinsame Definitionen und enthalten ähnliche Pflichten für Verantwortliche und Auftragsverarbeiter. In der Richtlinie zum Datenschutz bei der Strafverfolgung wird jedoch auch speziell auf Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten im Kontext der Strafverfolgung eingegangen. Die entsprechenden Bestimmungen umfassen Verpflichtungen i) zur Unterscheidung verschiedener Kategorien betroffener Personen, ii) zur Unterscheidung zwischen faktenbasierten personenbezogenen Daten und auf persönlichen Einschätzungen beruhenden Daten sowie iii) zur Protokollierung der Verwendung personenbezogener Daten und zur Einhaltung spezifischer Sicherheitsanforderungen[11].

---

[5] Charta der Grundrechte der Europäischen Union (ABl. C 202 vom 7.6.2016, S. 389).
[6] Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung) (ABl. C 202 vom 7.6.2016, S. 47).
[7] Artikel 63 Absatz 1 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[8] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).
[9] Die Rechtsakte über das Schengener Informationssystem und andere Instrumente des Schengen-Besitzstands enthielten beispielsweise spezifische Bestimmungen, um Fragen wie die Rechte betroffener Personen zu regeln.
[10] Hierzu gehören Rechtmäßigkeit und Verarbeitung nach Treu und Glauben, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht (Artikel 4 der Richtlinie zum Datenschutz bei der Strafverfolgung).
[11] Artikel 6, 7, 25 und 29 der Richtlinie zum Datenschutz bei der Strafverfolgung.

Aufgrund des spezifischen Charakters der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit wurde es als erforderlich erachtet, spezifische Vorschriften über den Schutz personenbezogener Daten und den freien Verkehr personenbezogener Daten in diesen Bereichen zu erlassen.[12] Die Sensibilität des Bereichs der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit sowie die Komplexität der nationalen Rechtsrahmen zur Regelung der Strafverfolgung führten dazu, dass eine Richtlinie als am besten geeignet angesehen wurde, um in diesem Bereich ein hohes Maß an Datenschutz zu erreichen. Eine Richtlinie gibt den Mitgliedstaaten bei der Umsetzung der Grundsätze, der Durchführung der Vorschriften und der Anwendung der Ausnahmebestimmungen auf nationaler Ebene zudem den notwendigen Spielraum.[13]

Die Kommission veröffentlichte ihren ersten Bericht über die Umsetzung der DSGVO am 24. Juni 2020.[14] Darin gelangte sie zu dem Schluss, dass die DSGVO ihre Ziele nach allgemeiner Auffassung erreicht hat, insbesondere dadurch, dass den Bürgerinnen und Bürgern damit ein starkes Bündel durchsetzbarer Rechte verliehen wird und ein neues System der EU für Verwaltung und Durchsetzung geschaffen wurde. Im Bericht wurden zu ergreifende Maßnahmen dargelegt, um die Anwendung der DSGVO durch alle Interessenträger zu erleichtern und eine Datenschutzkultur in der EU zu fördern und weiterzuentwickeln, zusammen mit einer konsequenten Durchsetzung.

Der vorliegende Bericht knüpft an die Überprüfung der von der EU erlassenen Rechtsakte über die Datenverarbeitung durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung an. Der Zweck dieser Überprüfung bestand darin, festzustellen, inwieweit eine Anpassung der betreffenden Rechtsakte an die Richtlinie zum Datenschutz bei der Strafverfolgung notwendig ist.[15] Mit ihrer Mitteilung vom 24. Juni 2020 „Weiteres Vorgehen hinsichtlich der Angleichung

---

[12] Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang zur Schlussakte der Regierungskonferenz, die den Vertrag von Lissabon annahm (ABl. C 115 vom 9.5.2008, S. 345).

[13] Begründung des Vorschlags für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (KOM(2012) 10 endgültig vom 25.1.2012).

[14] Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung“ (COM(2020) 264 final vom 24.6.2020).

[15] Artikel 62 Absatz 6 der Richtlinie zum Datenschutz bei der Strafverfolgung sah vor, dass die Kommission bis zum 6. Mai 2019 andere Rechtsakte der EU über die Verarbeitung personenbezogener Daten für Strafverfolgungszwecke überprüfen musste, um festzustellen, inwieweit eine Anpassung an diese Richtlinie notwendig ist, und um gegebenenfalls die erforderlichen Vorschläge zur Änderung dieser anderen Rechtsakte der EU zu unterbreiten, damit ein einheitliches Vorgehen beim Schutz personenbezogener Daten innerhalb des Anwendungsbereichs dieser Richtlinie gewährleistet ist.

des früheren Besitzstands des dritten Pfeilers an die Datenschutzvorschriften“[16] ist die Kommission dieser Verpflichtung nachgekommen. In der Mitteilung wurden zehn Rechtsakte genannt, die an die Richtlinie zum Datenschutz bei der Strafverfolgung angepasst werden sollten, und es wurde ein Zeitplan für diese Arbeit aufgestellt.

Schließlich wurde der vorliegende Bericht parallel zum Bericht der Kommission über die Anwendung der EU-DSVO erstellt. Ein wichtiges Element des letzteren Berichts ist die Überprüfung der Vorschriften in Kapitel IX der EU-DSVO über die Verarbeitung operativer personenbezogener Daten durch Einrichtungen und sonstige Stellen der Union bei der Ausübung von Tätigkeiten, die in den Anwendungsbereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen[17] (im Folgenden „JI-Agenturen“) fallen. Die betreffenden Vorschriften beruhen größtenteils auf der Richtlinie zum Datenschutz bei der Strafverfolgung. Artikel 98 der EU-DSVO sieht vor, dass die Kommission Rechtsakte überprüft, die die Verarbeitung operativer personenbezogener Daten durch JI-Agenturen regeln, und geeignete Gesetzgebungsvorschläge insbesondere im Hinblick auf die Anwendung der Bestimmungen des Kapitels IX auf Europol[18] und die Europäische Staatsanwaltschaft vorlegen sowie notwendige Änderungen dieses Kapitels vorschlagen kann.

1.2 Ein wesentlicher Beitrag zur Sicherstellung einer starken Sicherheitspolitik in der Europäischen Union

Die Kommission hat stets betont, dass eine effektive und wirklich sichere EU auf einer uneingeschränkten Wahrung der Grundrechte aufbauen muss, die in der Charta und im sekundären EU-Recht verankert sind. Die Richtlinie zum Datenschutz bei der Strafverfolgung leistet einen wichtigen Beitrag zur Sicherheitspolitik der EU, indem sie sicherstellt, dass die personenbezogenen Daten von Opfern, Zeugen und Tatverdächtigen ordnungsgemäß geschützt werden. Ferner trägt die Richtlinie durch die Harmonisierung der Vorschriften über den Schutz personenbezogener Daten, die von zuständigen Behörden in EU- und Schengen-Ländern verarbeitet werden, zu einem stärkeren Vertrauen und zur Sicherheit der Daten bei, die zum Zwecke der Strafverfolgung zwischen Behörden ausgetauscht werden, und erleichtert so die grenzüberschreitende Zusammenarbeit bei der Bekämpfung von Kriminalität und Terrorismus.[19] Die Richtlinie spielt auch eine wichtige Rolle dabei, eine Kultur der Einhaltung des Datenschutzes unter den zuständigen Behörden zu fördern.

---

[16] Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Weiteres Vorgehen hinsichtlich der Angleichung des früheren Besitzstands des dritten Pfeilers an die Datenschutzvorschriften“ (COM(2020) 262 final vom 24.6.2020).
[17] Dritter Teil Titel V Kapitel 4 und 5 AEUV.
[18] Dies wurde bereits durch den Vorschlag der Kommission aus dem Jahr 2020 zur Änderung der Europol-Verordnung angegangen.
[19] Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Erster Fortschrittsbericht zur EU-Strategie für die Sicherheitsunion“ (COM(2020) 797 final vom 9.12.2020).

In der Strategie für eine Sicherheitsunion[20] wird ferner betont, dass neue Technologien wie künstliche Intelligenz als wirksame Instrumente zur Verbrechensbekämpfung genutzt werden könnten. Um dieses Potenzial auszuschöpfen, gilt es, dabei höchste Standards für die Achtung der Grundrechte zu gewährleisten. Die Datenschutzgesetzgebung, einschließlich der Richtlinie zum Datenschutz bei der Strafverfolgung, bildet die Grundlage, auf der die sektorspezifische Gesetzgebung aufbauen kann. Das vorgeschlagene KI-Gesetz[21] würde beispielsweise den Rahmen für die Verwendung personenbezogener Daten zur biometrischen Fernidentifizierung in öffentlichen Räumen zum Zwecke der Strafverfolgung weiter abstecken.

Schließlich weist Kriminalität (insbesondere Cyberkriminalität und sonstige durch den Cyberraum ermöglichte Kriminalität) in einer vernetzten Welt zunehmend einen grenzübergreifenden Charakter auf. Selbst bei der Untersuchung innerstaatlicher Fälle stoßen die zuständigen Behörden immer öfter auf grenzüberschreitende Situationen, da Informationen elektronisch in einem Drittland gespeichert sind. Dadurch wächst die Notwendigkeit der internationalen Zusammenarbeit bei strafrechtlichen Ermittlungen, sowohl aufseiten der Behörden der Mitgliedstaaten als auch aufseiten der EU-Einrichtungen wie Europol und Eurojust. Bei einer solchen Zusammenarbeit, insbesondere bei der Erhebung und dem Austausch elektronischer Beweismittel[22], werden häufig personenbezogene Daten übermittelt. Starke Datenschutzgarantien sind daher von wesentlicher Bedeutung. Diese Garantien helfen auch dabei, Vertrauen zwischen den Strafverfolgungsbehörden aufzubauen, um so für einen schnelleren und effektiveren Informationsaustausch zu sorgen und die Rechtssicherheit zu stärken, wenn Informationen anschließend bei Strafverfahren verwendet werden. In diesem Zusammenhang bietet die Richtlinie zum Datenschutz bei der Strafverfolgung ein aktualisiertes Instrumentarium zur Erleichterung solcher Übermittlungen personenbezogener Daten aus der EU an ein Drittland oder eine internationale Organisation (z. B. Interpol[23]), wobei gleichzeitig weiterhin ein hohes Schutzniveau für die personenbezogenen Daten sichergestellt wird. Die

---

[20] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen mit dem Titel „EU-Strategie für eine Sicherheitsunion“ (COM(2020) 605 final vom 24.7.2020).

[21] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021) 206 final vom 21.4.2021).

[22] Bei rund 85 % der Ermittlungen zu schweren Straftaten werden elektronische Informationen und Beweismittel benötigt, und 65 % aller Anfragen sind an Anbieter gerichtet, die in einem Land ansässig sind, das einer anderen Gerichtsbarkeit unterliegt. Siehe die Arbeitsunterlage der Kommissionsdienststellen mit dem Titel „Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings“ (Folgenabschätzung zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren) (SWD(2018) 118 final).

[23] Siehe auch Erwägungsgrund 25 der Richtlinie zum Datenschutz bei der Strafverfolgung.

Kommission und die Mitgliedstaaten haben seit dem Inkrafttreten der Richtlinie die gesamte Palette ihrer Instrumente genutzt, was somit bestätigt, dass sie breit und flexibel genug ist, um eine wirksame internationale polizeiliche und justizielle Zusammenarbeit zu ermöglichen.

1.3 Wichtige Aspekte hinsichtlich der Erstellung des Berichts

Bei der Vorbereitung des vorliegenden Berichts hat die Kommission aus einer Vielzahl von Quellen und im Wege gezielter Konsultationen Informationen und Rückmeldungen gesammelt. Im Zusammenhang mit Artikel 62 der Richtlinie zum Datenschutz bei der Strafverfolgung berücksichtigte die Kommission die Beiträge und Standpunkte des Europäischen Parlaments[24], des Rates[25], des Europäischen Datenschutzausschusses (im Folgenden „EDSA“)[26] und der nationalen Datenschutzaufsichtsbehörden. Zusätzliche Rückmeldungen wurden durch einen Fragebogen an Organisationen der Zivilgesellschaft (die von der Agentur der Europäischen Union für Grundrechte kontaktiert wurden)[27] und durch Antworten im Rahmen einer öffentlichen Sondierung[28] gesammelt. Die Kommission berücksichtigte ferner Ausführungen der Expertengruppe mit Vertretern der Mitgliedstaaten für die DSGVO und die Richtlinie zum Datenschutz bei der Strafverfolgung[29] sowie Ausführungen des deutschen Ratsvorsitzes[30].

---

[24] Beitrag des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments zum kommenden Bericht der Europäischen Kommission über die Bewertung und Überprüfung der Richtlinie zum Datenschutz bei der Strafverfolgung, 7. Februar 2022.

[25] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates 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 (im Folgenden „Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung“) (Dokument 13943/21 des Rates vom 18.11.2021, https://data.consilium.europa.eu/doc/document/ST-13943-2021-INIT/de/pdf).

[26] Contribution of the EDPB to the European Commission’s evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62 (Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung durch die Europäische Kommission nach Artikel 62, im Folgenden „Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung“), angenommen am 14. Dezember 2021. https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[27] Von den 804 Organisationen der Zivilgesellschaft, an die sich die Agentur der Europäischen Union für Grundrechte (FRA) gewandt hat, antworteten insgesamt 88. Allerdings konnten nur 17 Beiträge berücksichtigt werden, da 61 Beiträge nicht im Zusammenhang mit der Richtlinie zum Datenschutz bei der Strafverfolgung standen oder da die betreffenden Organisationen angegeben hatten, dass sie nicht in Bezug auf den Schutz der Grundrechte im Bereich der Strafverfolgung tätig bzw. überhaupt nicht mit der Richtlinie vertraut sind.

[28] Sondierung, Datenschutz bei der Strafverfolgung – Bericht über die Richtlinie zum Datenschutz bei der Strafverfolgung, 24. Januar 2022. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13288-Datenschutz-bei-der-Strafverfolgung-Bericht-uber-die-Richtlinie-zum-Datenschutz-bei-der-Strafverfolgung_de

[29] Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (Expertengruppe der Kommission für die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680) (E03461). https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3461&lang=de

[30] Presidency Report on the exchange of police data with third countries – Experiences in the application of Article 37 of the Law Enforcement Directive (Bericht des Vorsitzes über den Austausch von Polizeidaten mit Drittländern – Erfahrungen bei der Anwendung von Artikel 37 der Richtlinie zum Datenschutz bei der Strafverfolgung), Dezember 2020.

Zudem trug sie der Analyse der nationalen Umsetzungsmaßnahmen und einer geringen Zahl von Beschwerden, die sie diesbezüglich erhalten hatte, Rechnung.

Die Richtlinie zum Datenschutz bei der Strafverfolgung gilt für alle Mitgliedstaaten und alle Schengen-Länder (da sie eine Weiterentwicklung des Schengen-Besitzstands darstellt[31]), jedoch werden im vorliegenden Bericht nur die EU-Mitgliedstaaten behandelt.

Drei Faktoren hatten Auswirkungen auf die Erstellung dieses Berichts. Erstens konnten zwei Drittel der Mitgliedstaaten die Frist zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung in nationales Recht bis Mai 2018 nicht einhalten. Dennoch setzten die meisten Mitgliedstaaten die Richtlinie bis 2019 um, nachdem die Kommission Vertragsverletzungsverfahren eingeleitet hatte. Die Erfahrung zur Anwendung der Richtlinie ist daher eher begrenzt, was auch vom EDSA[32] und dem Rat[33] betont wird. Zweitens erwies es sich im Vergleich zur DSGVO schwieriger, Statistiken zur Anwendung der Richtlinie zusammenzustellen. Einige Datenschutzaufsichtsbehörden erheben bei ihren Aufsichtstätigkeiten keine gesonderten statistischen Daten zur Richtlinie und zur DSGVO. Dies ist beispielsweise in Bezug auf Meldungen von Datenschutzverletzungen[34] sowie Beschwerden im Rahmen der Richtlinie[35] der Fall, was es teilweise schwierig macht, einen genauen Überblick über diese Aspekte der Richtlinie zu erhalten[36].

Drittens ist es wichtig, zu beachten, dass sich die Rechtsprechung in Bezug auf die Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung gerade erst entwickelt. Beim Gerichtshof der Europäischen Union (im Folgenden „EuGH“) sind derzeit mehrere Rechtssachen hinsichtlich der Auslegung wichtiger Bestimmungen der Richtlinie, darunter das Auskunftsrecht und das Recht auf einen wirksamen gerichtlichen Rechtsbehelf betroffener Personen, anhängig. Die entsprechenden Urteile werden für mehr Klarheit sorgen und zu einem stärker harmonisierten Ansatz unter den Mitgliedstaaten beitragen.

2 EINE ZUFRIEDENSTELLENDE UMSETZUNG, DOCH EINIGE PROBLEME BLEIBEN OFFEN

Die Kommission hat eine Expertengruppe mit Vertretern der Mitgliedstaaten[37] eingerichtet, um die Mitgliedstaaten dabei zu unterstützen, die Richtlinie zum Datenschutz bei der

[31] Siehe die Erwägungsgründe 101–103 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[32] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 4.
[33] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 7.
[34] Die Behörden in Dänemark, Litauen, Norwegen und Österreich sowie mehrere Behörden in Deutschland führen beispielsweise keine gesonderten Statistiken über Datenschutzverletzungen gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung. Sechs Behörden haben zudem berichtet, dass bei ihnen keine Meldungen zu Verstößen gegen die Richtlinie eingegangen sind.
[35] Die Behörden in Dänemark und Österreich sowie mehrere Behörden in Deutschland führen beispielsweise keine gesonderten Statistiken über Beschwerden im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung.
[36] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 43.
[37] Siehe Fußnote 29.

Strafverfolgung in nationales Recht umzusetzen. Die Gruppe erleichtert die Gespräche und den Erfahrungsaustausch zwischen den Mitgliedstaaten und der Kommission über Datenschutzvorschriften. Sie hielt vom Erlass der Richtlinie im Jahr 2016 bis zur Umsetzungsfrist im Mai 2018 regelmäßig Treffen ab und nahm ihre Arbeit 2021 wieder auf.

Im unten dargelegten Überblick über die Umsetzung liegt der Fokus auf den zentralen Problemen, die bisher ermittelt wurden. Er beruht hauptsächlich auf der von der Kommission vorgenommenen Analyse der Informationen, die die Mitgliedstaaten übermittelten, als sie die Kommission über die von ihnen ergriffenen nationalen Maßnahmen zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung in nationales Recht unterrichteten. Diese Analyse wurde durch eine externe Studie eines externen Auftragnehmers unterstützt. Die Kommission stand zudem im bilateralen Austausch mit mehreren Mitgliedstaaten.

2.1 Eine insgesamt vollständige Umsetzung, aber mit einigen Problemen bei spezifischen Bestimmungen

Die Kommission leitete im Juli 2018 Vertragsverletzungsverfahren gegen 19 Mitgliedstaaten ein, da diese es versäumt hatten, fristgerecht bis Mai 2018 Gesetze zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung zu erlassen und die Kommission ordnungsgemäß über die Umsetzung zu unterrichten. Ein weiteres Verfahren aufgrund einer teilweisen Nichtumsetzung wurde im Juli 2019 gegen einen anderen Mitgliedstaat eingeleitet. Infolgedessen teilten die meisten Mitgliedstaaten der Kommission anschließend ihre nationalen Umsetzungsvorschriften mit, woraufhin diese die Vertragsverletzungsverfahren gegen sie 2019 (bzw. 2020 im Falle eines Mitgliedstaats) schrittweise einstellte. Im Jahr 2021 verwies die Kommission ihre Vertragsverletzungsklage gegen Spanien an den EuGH, da Spanien es noch immer nicht geschafft hatte, die Richtlinie zum Datenschutz bei der Strafverfolgung umzusetzen und die Kommission über seine Umsetzungsmaßnahmen zu unterrichten. Angesichts der Schwere und Dauer des Verstoßes verhängte der EuGH erstmals sowohl einen Pauschalbetrag als auch ein Zwangsgeld gegen Spanien.[38]

Im April 2022 leitete die Kommission ferner ein Vertragsverletzungsverfahren gegen Deutschland ein, nachdem sie eine Lücke bei der Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung in Bezug auf die Tätigkeiten der deutschen Bundespolizei festgestellt hatte.

Die Kommission wird die Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung in den Mitgliedstaaten weiterhin bewerten und die erforderlichen Maßnahmen ergreifen, um etwaige Lücken zu beseitigen.

2.2 Prioritäten für die Prüfung auf Übereinstimmung

[38] Urteil vom 25. Februar 2021, Europäische Kommission/Königreich Spanien, C-658/19, ECLI:EU:C:2017:548.

Die Kommission prüft des Weiteren, ob die Anforderungen der Richtlinie zum Datenschutz bei der Strafverfolgung von den Mitgliedstaaten in ihren nationalen Bestimmungen ordnungsgemäß umgesetzt wurden (Prüfung auf Übereinstimmung).

Im Rahmen der Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung wurden die vorherigen Rechtsvorschriften zum Datenschutz von den Mitgliedstaaten entweder geändert oder aufgehoben und durch ein oder mehrere neue horizontale Datenschutzgesetze ersetzt. In vielen Fällen wurde die Richtlinie in nationales Recht umgesetzt, indem jeweils auf die gleiche oder eine gleichwertige Bestimmung der DSGVO zurückgegriffen wurde (z. B. in Bezug auf Begriffsbestimmungen, Meldungen von Datenschutzverletzungen, die Benennung eines Datenschutzbeauftragten sowie die Organisation, den Status, die Zuständigkeiten, die Aufgaben und die Befugnisse der nationalen Datenschutzaufsichtsbehörden). Einige Bestimmungen der Richtlinie wurden zudem durch neue Bestimmungen beispielsweise im allgemeinen Verwaltungsrecht, im Verwaltungsverfahrensrecht oder im Strafverfahrensrecht umgesetzt. Mehrere Mitgliedstaaten setzten auch einige Bestimmungen der Richtlinie in sektorspezifischen Rechtsvorschriften um, mit denen die Tätigkeit und die Befugnisse spezifischer zuständiger Behörden geregelt werden. Bei der Feststellung, ob die Richtlinie in einem bestimmten Mitgliedstaat ordnungsgemäß umgesetzt wurde, muss daher möglicherweise eine Vielzahl nationaler Rechtsakte berücksichtigt werden. Insgesamt spiegeln die einzelstaatlichen Rechtsvorschriften die Grundsätze und zentralen Bestimmungen der Richtlinie größtenteils wider. Es wurde jedoch eine Reihe von Problemen festgestellt, wobei die wichtigsten in den folgenden Abschnitten dargelegt werden. Die Kommission hat bereits mehrere Vertragsverletzungsverfahren gegen Mitgliedstaaten eingeleitet.[39] Der Überprüfungsprozess ist noch nicht abgeschlossen und die Kommission wird weiterhin alle zur Verfügung stehenden Instrumente, einschließlich Vertragsverletzungsverfahren, nutzen, sollte eine nationale Umsetzungsmaßnahme nicht mit der Richtlinie zum Datenschutz bei der Strafverfolgung im Einklang stehen.

Die Rechtsprechung zur Richtlinie zum Datenschutz bei der Strafverfolgung steckt noch in den Anfängen. Der EuGH hat erste Urteile zur Auslegung der Richtlinie erlassen, darunter in den

[39] Im April 2022 leitete die Kommission gegen Griechenland, Finnland und Schweden Vertragsverletzungsverfahren aufgrund einer fehlenden Konformität ihrer nationalen Umsetzungsgesetze mit der Richtlinie zum Datenschutz bei der Strafverfolgung ein. Beim Verfahren gegen Griechenland geht es um mehrere Punkte, unter anderem die Nichtanwendung des nationalen Gesetzes zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung auf die Verarbeitung personenbezogener Daten durch Justiz- und Strafverfolgungsbehörden sowie Behörden unter ihrer Aufsicht für die meisten Straftaten, die Umsetzung der Bestimmungen zur Datenspeicherung und Überprüfung (Artikel 5), die Rechtsgrundlage der Datenverarbeitung (Artikel 8) und Garantien im Zusammenhang mit automatisierter Entscheidungsfindung (Artikel 11). Die Vertragsverletzungsverfahren gegen Finnland und Schweden wurden eingeleitet, da ihre Rechtsvorschriften keinen Zugang zu einem wirksamen Rechtsbehelf vor einem Gericht für betroffene Personen vorsehen. Die Kommission eröffnete im Mai 2022 ein Vertragsverletzungsverfahren gegen Deutschland, da mehrere nationale Gesetze zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung keine wirksamen Abhilfebefugnisse auf Bundes- und Länderebene vorsehen.

Rechtssachen WS/Bundesrepublik Deutschland[40] und B/Latvijas Republikas Saeima[41]. Zum Zeitpunkt der Erstellung dieses Berichts waren mehrere Vorabentscheidungsverfahren beim EuGH anhängig (wie in den folgenden Abschnitten angegeben).

2.2.1 Anwendungsbereich der Richtlinie zum Datenschutz bei der Strafverfolgung

Die Schwierigkeit, die Anwendungsbereiche der Richtlinie zum Datenschutz bei der Strafverfolgung und der DSGVO voneinander abzugrenzen, wurde sowohl von der Expertengruppe mit Vertretern der Mitgliedstaaten für die DSGVO und die Richtlinie zum Datenschutz bei der Strafverfolgung[42] als auch vom EDSA[43] als Problem angesprochen. Einige Datenschutzaufsichtsbehörden haben zudem angemerkt, dass dies für zuständige Behörden schwierig sein kann.[44]

Der Anwendungsbereich der Richtlinie zum Datenschutz bei der Strafverfolgung wird durch zwei wichtige Elemente definiert[45]: den Begriff der „zuständigen Behörde“ (persönlicher Anwendungsbereich) und den Begriff der „Straftat“ (sachlicher Anwendungsbereich).

Im Hinblick auf den persönlichen Anwendungsbereich fällt Datenverarbeitung erstens unter die Richtlinie zum Datenschutz bei der Strafverfolgung, wenn sie durch eine zuständige Behörde erfolgt, und zweitens, wenn die personenbezogenen Daten für die Zwecke der Richtlinie[46] (d. h. zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit) verarbeitet werden. Nach Ansicht der Kommission sind „zuständige Behörden“ im Sinne der Richtlinie[47] entweder staatliche Organe oder private Einrichtungen, die nach dem Gesetz mit besonderen Rechten ausgestattet sind, die über das hinausgehen, was für die Beziehungen zwischen Privatpersonen gilt, und/oder die die Möglichkeit der Ausübung von Zwangsbefugnissen umfassen. Diese Behörden sind zuständige Behörden gemäß der Richtlinie,

---

[40] Urteil vom 12. Mai 2021, WS/Bundesrepublik Deutschland, C-505/19, ECLI:EU:C:2021:376. Die Rechtssache betraf unter anderem die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten (Artikel 4 Absatz 1 Buchstabe a und Artikel 8 der Richtlinie zum Datenschutz bei der Strafverfolgung) im spezifischen Kontext einer von Interpol herausgegebenen Red Notice. Der Gerichtshof urteilte, dass die Verarbeitung der in einer von Interpol herausgegebenen Red Notice enthaltenen personenbezogenen Daten nicht unrechtmäßig sei, solange nicht mit einer rechtskräftigen gerichtlichen Entscheidung festgestellt worden sei, dass das Verbot der Doppelbestrafung bei den Taten, auf die sich die betreffende Red Notice bezieht, greift.

[41] Urteil vom 22. Juni 2021, B/Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504. Der EuGH legte die Definition der „zuständigen Behörde“ im Sinne von Artikel 3 Nummer 7 und den Begriff „Straftat“ aus. Siehe auch den Abschnitt unten.

[42] Siehe das Protokoll der Sitzung der Expertengruppe der Kommission für die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 vom 5. Mai 2021. https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=25283&fromExpertGroups=true

[43] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 7.

[44] Die Datenschutzaufsichtsbehörden von Irland, Frankreich und Ungarn haben diesbezüglich Bedenken geäußert.

[45] Artikel 2 Absatz 1 und Erwägungsgründe 12–14 der Richtlinie zum Datenschutz bei der Strafverfolgung.

[46] Artikel 1 der Richtlinie zum Datenschutz bei der Strafverfolgung.

[47] Artikel 3 Nummer 7 der Richtlinie zum Datenschutz bei der Strafverfolgung.

wenn sie zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit) Daten verarbeiten (auch dann, wenn sie dies nur sporadisch und/oder in Einzelfällen tun). Dies bedeutet beispielsweise, dass die Verarbeitung personenbezogener Daten durch solche Einrichtungen für andere Zwecke als die der Richtlinie (z. B. personalwirtschaftliche oder andere administrative Zwecke, etwa die Verarbeitung personenbezogener Daten durch die zentralen Meldestellen nach dem Besitzstand im Bereich der Bekämpfung von Geldwäsche[48]) in den Anwendungsbereich der DSGVO und nicht der Richtlinie fällt.

Der Begriff der „Straftat" ist von zentraler Bedeutung für die Feststellung, ob Datenverarbeitung in den Anwendungsbereich der Richtlinie zum Datenschutz bei der Strafverfolgung fällt. Dem EuGH zufolge sind für die Beurteilung des strafrechtlichen Charakters einer Zuwiderhandlung drei Kriterien maßgebend: erstens die rechtliche Einordnung der Zuwiderhandlung im innerstaatlichen Recht, zweitens die Art der Zuwiderhandlung und drittens der Schweregrad der dem Betroffenen drohenden Sanktion.[49] Der eigenständige Charakter des Begriffs der „Straftat" gemäß dem Erwägungsgrund 13 der Richtlinie zum Datenschutz bei der Strafverfolgung impliziert unter anderem, dass eine Zuwiderhandlung im Recht der Mitgliedstaaten nicht einzig und allein zum Zwecke der Anwendung der Richtlinie als Straftat festgelegt werden kann.

Die Frage der Abgrenzung zwischen den Anwendungsbereichen der DSGVO und der Richtlinie zum Datenschutz bei der Strafverfolgung stellt sich in einigen Mitgliedstaaten hinsichtlich der Abgrenzung zwischen Straftaten und Ordnungswidrigkeiten. Insbesondere beziehen sich mehrere nationale Umsetzungsgesetze auf Zwecke für die Verarbeitung personenbezogener Daten, die nicht in Artikel 1 der Richtlinie aufgeführt sind (z. B. Gefahren für die öffentliche Ordnung oder öffentliche Sicherheit). Die Frage stellt sich auch deshalb, weil mehrere Mitgliedstaaten der Ansicht sind, dass einige Verwaltungsstellen (z. B. zentrale Meldestellen, wie oben erwähnt) Aufgaben erfüllen, die unter die Richtlinie fallen.

Zumeist wird in den Rechtsvorschriften der Mitgliedstaaten jegliche Verarbeitung von Daten durch zuständige Behörden für die Zwecke der Richtlinie zum Datenschutz bei der Strafverfolgung umfassend berücksichtigt. Einige Mitgliedstaaten haben sich hingegen dafür entschieden, die zuständigen Behörden gemäß der Richtlinie in ihren nationalen Rechtsvorschriften ausführlich aufzuzählen. Manche Mitgliedstaaten sehen ferner eine Ausnahmeregelung für die Verarbeitung durch bestimmte Arten von zuständigen Behörden oder die Verarbeitung bestimmter Arten von Daten vor.

---

[48] In Artikel 41 der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, mit dem die Tätigkeit der zentralen Meldestellen geregelt wird, heißt es ausdrücklich, dass für die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie die Verordnung (EU) 2016/679 gilt.

[49] Urteil vom 22. Juni 2021, B/Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504, Rn. 87.

Die Frage des Anwendungsbereichs der Richtlinie zum Datenschutz bei der Strafverfolgung ist Gegenstand eines Vorabentscheidungsersuchens an den EuGH. Das Landesverwaltungsgericht Tirol (Österreich) befasste sich mit dieser Problematik, nachdem eine zuständige Behörde erfolglos versucht hatte, sich Zugang zu Daten auf einem beschlagnahmten Mobiltelefon zu verschaffen (Auslegung des Artikels 2 der Richtlinie). Die Rechtssache betrifft ferner die Bedingungen eines solchen Zugangs.[50]

2.2.2 Governance und Befugnisse der Datenschutzaufsichtsbehörden

Alle bis auf zwei Mitgliedstaaten (Belgien und Schweden) haben die Aufsichtsbehörde, die auch für die Durchsetzung der DSGVO zuständig ist, mit der Durchsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung betraut. Belgien hat eine andere Aufsichtsbehörde mit der Aufsicht über die Polizei für die Zwecke der Richtlinie beauftragt. In Schweden obliegt die Aufsicht über bestimmte zuständige Behörden, einschließlich der Polizei, sowohl der für die DSGVO zuständigen Aufsichtsbehörde als auch einer anderen Aufsichtsbehörde. Ferner sind die Datenschutzaufsichtsbehörden gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung nicht für die Aufsicht über die Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig.

Hinsichtlich der Bestimmungen der Richtlinie zum Datenschutz bei der Strafverfolgung über die Unabhängigkeit der Datenschutzaufsichtsbehörden[51] haben alle Mitgliedstaaten in ihren Umsetzungsgesetzen festgelegt, dass die Datenschutzaufsichtsbehörden bei der Erfüllung ihrer Aufgaben unabhängig handeln. Außerdem sehen die Mitgliedstaaten vor, dass die Mitglieder ihrer Datenschutzaufsichtsbehörden keiner Beeinflussung von außen unterliegen und dass sie weder um Weisung ersuchen noch Weisungen entgegennehmen.

Die Überwachung der Einhaltung der Vorschriften durch die Datenschutzaufsichtsbehörden ist von wesentlicher Bedeutung und in Artikel 8 Absatz 3 der Charta verankert. In der Richtlinie zum Datenschutz bei der Strafverfolgung wird von den Mitgliedstaaten verlangt, dass die Datenschutzaufsichtsbehörden Untersuchungsbefugnisse, Abhilfebefugnisse und beratende Befugnisse haben, die wirksam sein müssen. Dies ist eine Voraussetzung, um die Datenschutzvorschriften ordnungsgemäß durchzusetzen und so das Ziel der Richtlinie eines hohen Schutzniveaus für die Grundrechte zu erreichen, insbesondere in Bezug auf das Recht auf Schutz personenbezogener Daten, und um den freien Datenverkehr in der EU sicherzustellen. Die Datenschutzaufsichtsbehörden müssen in der gesamten EU gleichwertige Befugnisse haben, damit sie ihre Aufgaben wie in der Richtlinie verlangt erfüllen.[52]

Alle Mitgliedstaaten haben ihre Behörden mit den in der Richtlinie zum Datenschutz bei der Strafverfolgung beschriebenen Untersuchungsbefugnissen ausgestattet und die meisten Mitgliedstaaten haben ihnen außerdem weitere Befugnisse eingeräumt (z. B. zur Durchführung

---

[50] Vorabentscheidungsersuchen in der Rechtssache C. G./Bezirkshauptmannschaft Landeck, C-548/21.
[51] Kapitel VI Abschnitt 1 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[52] Erwägungsgründe 7 und 82 der Richtlinie zum Datenschutz bei der Strafverfolgung.

von Prüfungen, zum Betreten von Räumlichkeiten, zum Kopieren von Daten und zur Beschlagnahme von Objekten[53]). Daher waren fast alle Datenschutzaufsichtsbehörden der Ansicht, dass sie wirksame Untersuchungsbefugnisse haben.

Fast alle Mitgliedstaaten haben die in der Richtlinie zum Datenschutz bei der Strafverfolgung beschriebenen Abhilfebefugnisse[54] eingeräumt. Viele haben sich dabei stark an dem Wortlaut der Richtlinie orientiert, während einige sehr weit gefasste Formulierungen verwendet haben, die vernünftigerweise so ausgelegt werden könnten, dass sie alle in der Richtlinie dargelegten Befugnisse umfassen.

Darüber hinaus sehen die meisten Rechtsvorschriften der Mitgliedstaaten für die Datenschutzaufsichtsbehörden die Befugnis vor, Bußgelder zu verhängen.[55]

Nicht alle Mitgliedstaaten haben ihre Datenschutzaufsichtsbehörden mit der Befugnis ausgestattet, Verstöße gegen die innerstaatlichen Rechtsvorschriften, die zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung erlassen wurden, den Justizbehörden zur Kenntnis zu bringen und die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen. Diese Befugnis ist wichtig und ergänzt die anderen Mittel, die den Datenschutzaufsichtsbehörden zur Verfügung stehen, um ein hohes Schutzniveau für die Grundrechte natürlicher Personen und insbesondere ihr Recht auf Schutz personenbezogener Daten wirksam sicherzustellen.

2.2.3 Rechtsbehelfe

Alle Mitgliedstaaten sehen das Recht auf Beschwerde bei ihrer entsprechenden Aufsichtsbehörde vor.[56] In den meisten nationalen Gesetzen ist eine Frist für das Einlegen einer solchen Beschwerde festgelegt. Es ist wichtig, dass diese Frist das Recht betroffener Personen in diesem Zusammenhang nicht behindert.

Im Einklang mit der Richtlinie zum Datenschutz bei der Strafverfolgung[57] sehen alle Mitgliedstaaten unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen

---

[53] Siehe auch Randnummer 23 des Beitrags des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung: 24 Mitgliedstaaten räumten die Befugnis ein, Zugang zu jeglichen Räumlichkeiten des Verantwortlichen und des Auftragsverarbeiters sowie zu jeglichen Anlagen und Mitteln der Datenverarbeitung zu erhalten, 21 Mitgliedstaaten sahen einen Prüfungsprozess vor und neun Mitgliedstaaten räumten andere Befugnisse ein (z. B. zur Beschlagnahme von Objekten, zur Aufforderung zur Anhörung vor der Datenschutzaufsichtsbehörde und zum Ersuchen operativer Hilfe der Polizei).

[54] Artikel 47 Absatz 2 Buchstaben a bis c der Richtlinie zum Datenschutz bei der Strafverfolgung.

[55] Diese Möglichkeit wurde in 18 Mitgliedstaaten eingeräumt: Bulgarien, Estland, Griechenland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Portugal, Rumänien, Schweden, Slowakei, Tschechien, Ungarn und Zypern. Die Datenschutzaufsichtsbehörden in drei Mitgliedstaaten (Estland, Lettland und Österreich) können Bußgelder gegen natürliche Personen (z. B. Beschäftigte) oder private Einrichtungen (d. h. solche, die Auftragsverarbeiter sind) verhängen.

[56] Artikel 52 der Richtlinie zum Datenschutz bei der Strafverfolgung.

[57] Artikel 53 der Richtlinie zum Datenschutz bei der Strafverfolgung.

Rechtsbehelfs, der in ihrem Rechtssystem zur Verfügung steht, einen gerichtlichen Rechtsbehelf gegen die Beschlüsse der Aufsichtsbehörde vor. Ein gerichtlicher Rechtsbehelf wird in allen bis auf zwei Mitgliedstaaten[58] zur Verfügung gestellt, wenn eine Aufsichtsbehörde sich nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat[59].

Die meisten Mitgliedstaaten sehen bei mutmaßlichen Verstößen gegen die Richtlinie zum Datenschutz bei der Strafverfolgung auch einen gerichtlichen Rechtsbehelf gegen Verantwortliche und Auftragsverarbeiter vor.[60] Mehrere nationale Umsetzungsgesetze sehen jedoch für die betroffene Person nicht das Recht vor, gemeinnützige Einrichtungen, Organisationen und Vereine zu beauftragen, in ihrem Namen eine Beschwerde bei der Aufsichtsbehörde einzureichen oder einen gerichtlichen Rechtsbehelf einzulegen.[61]

2.2.4 Fristen für die Speicherung und Überprüfung

Die Ansätze der Mitgliedstaaten bezüglich der Umsetzung der Fristen für die Speicherung und Überprüfung personenbezogener Daten im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung[62] unterscheiden sich stark voneinander. Die meisten nationalen Datenschutzgesetze zur Umsetzung der Richtlinie erfüllen lediglich die allgemeine Anforderung des Artikels 5 der Richtlinie. Das bedeutet, dass im sektorspezifischen Recht tatsächliche Fristen für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung festgelegt werden müssen. Manche Mitgliedstaaten setzen die Bestimmung um, indem sie die Fristen in sektorspezifischen Rechtsvorschriften festsetzen.

In einigen Mitgliedstaaten sehen die Rechtsvorschriften jedoch vor, dass die zuständige Behörde die Fristen festlegt. In manchen Fällen sind in den Rechtsvorschriften keine Kriterien für die regelmäßige Überprüfung festgelegt und es wird nicht verlangt, dass solche Kriterien in anderen Rechtsvorschriften aufzuführen sind, und/oder es ist nicht vorgesehen, dass Verfahren zur Sicherstellung der Einhaltung der Fristen ebenfalls im innerstaatlichen Recht festzulegen sind.

Es ist anzumerken, dass das Oberste Verwaltungsgericht Bulgariens den EuGH kürzlich um Vorabentscheidung zur Auslegung des Artikels 5 der Richtlinie zum Datenschutz bei der Strafverfolgung in Bezug auf die Fristen für die Speicherung von Daten ersucht hat.[63]

---

[58] Finnland und Schweden.
[59] Artikel 53 Absatz 2 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[60] Artikel 54 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[61] Artikel 55 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[62] Artikel 5 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[63] Vorabentscheidungsersuchen in der Rechtssache NG/Direktor na Glavna direktsia „Natsionalna politsia“ pri MVR – Sofia, C-118/22.

2.2.5 Rechtsgrundlage für die Verarbeitung, einschließlich besonderer Kategorien personenbezogener Daten

Die Mehrheit der Mitgliedstaaten sieht – unter Verwendung von Formulierungen, die häufig weitgehend Artikel 8 der Richtlinie zum Datenschutz bei der Strafverfolgung entsprechen – vor, dass die Rechtsgrundlage für die Verarbeitung im Recht der EU oder der Mitgliedstaaten festgelegt sein muss. Einige nationale Datenschutzgesetze zur Umsetzung der Richtlinie erfüllen jedoch nicht die Anforderung, dass die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung im Recht anzugeben sind[64]. Andere nationale Datenschutzgesetze zur Umsetzung der Richtlinie enthalten nicht alle Bestimmungen gemäß Artikel 8. Die Rechtsgrundlage für die Verarbeitung muss im nationalen Recht angegeben sein und dieses muss den Anforderungen nach Artikel 8 entsprechen. Darüber hinaus kann die bloße erneute Wiedergabe der allgemeinen Anforderungen des Artikels 8 der Richtlinie zum Datenschutz bei der Strafverfolgung im nationalen Recht nicht als ausreichende Rechtsgrundlage für einen spezifischen Verarbeitungsvorgang angesehen werden: In den nationalen Rechtsvorschriften müssen die für die Verarbeitung der personenbezogenen Daten zuständige Behörde, die von ihr erfüllten öffentlichen Aufgaben zur Rechtfertigung einer solchen Verarbeitung sowie der Zweck der Verarbeitung angegeben werden.

Für die Verarbeitung besonderer Kategorien personenbezogener Daten[65] setzen die meisten Mitgliedstaaten voraus, dass diese unbedingt erforderlich ist. Die meisten Mitgliedstaaten geben zudem die gleichen rechtlichen Gründe für die Verarbeitung sensibler Daten wie in Artikel 10 der Richtlinie zum Datenschutz bei der Strafverfolgung an (die Verarbeitung muss nach dem Recht zulässig sein, der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dienen oder sich auf Daten beziehen, die die betroffene Person offensichtlich öffentlich gemacht hat). In manchen Mitgliedstaaten beinhalten die Umsetzungsgesetze einige zusätzliche Gründe für die Datenverarbeitung (z. B. kann die Verarbeitung solcher Daten notwendig sein, um eine Gefahr abzuwenden oder zu vermeiden, die das Leben, die körperliche Unversehrtheit oder das Vermögen von Personen unmittelbar gefährdet, oder um die Gesundheit oder Interessen der betroffenen oder einer anderen Person zu schützen). Wenn das nationale Datenschutzgesetz zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung nicht die notwendigen Garantien für die Rechte und Freiheiten der betroffenen Personen bietet (wie es in einigen Mitgliedstaaten der Fall ist), müssen solche Garantien in den sektorspezifischen Rechtsvorschriften vorgesehen sein.

Manche nationalen Umsetzungsgesetze beziehen sich auf eine Einwilligung im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Verarbeitung besonderer Kategorien personenbezogener Daten. Es sei darauf hingewiesen, dass es den Mitgliedstaaten zwar nicht verwehrt ist, in ihrem nationalen Recht vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke der Richtlinie zum Datenschutz bei

[64] Artikel 8 Absatz 2 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[65] Artikel 10 der Richtlinie zum Datenschutz bei der Strafverfolgung.

der Strafverfolgung zustimmen kann, diese Einwilligung jedoch nur als Garantie dienen und nicht die Rechtsgrundlage für eine solche Verarbeitung darstellen kann. Die Gespräche zu diesem Thema zeigen, dass es zweckmäßig wäre, mehr Leitlinien zur Rolle der Einwilligung im Kontext der Verarbeitung personenbezogener Daten zum Zwecke der Strafverfolgung bereitzustellen.

2.2.6 Automatisierte Entscheidungsfindung

Die Umsetzungsgesetze sämtlicher Mitgliedstaaten enthalten Bestimmungen, mit denen eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung verboten wird, es sei denn, sie ist im Recht vorgesehen[66]. In den meisten Umsetzungsgesetzen der Mitgliedstaaten ist vorgeschrieben, dass solche Entscheidungen nicht auf besonderen Kategorien personenbezogener Daten beruhen dürfen, sofern nicht geeignete Garantien vorhanden sind[67]. Ebenfalls verboten wird darin das Profiling, das Diskriminierung zur Folge hat[68]. Einige innerstaatliche Rechtsvorschriften beziehen sich jedoch nicht auf geeignete Garantien für die Rechte und Freiheiten der betroffenen Person in Fällen, in denen automatisierte Entscheidungsfindung nach dem Recht erlaubt ist. Insbesondere ist es so, dass nicht alle Mitgliedstaaten das Recht auf persönliches Eingreifen seitens des Verantwortlichen vorsehen oder geeignete Maßnahmen zum Schutz der Rechte und/oder Freiheiten sowie der berechtigten Interessen der betroffenen Person vorschreiben.

2.2.7 Rechte betroffener Personen

Alle Mitgliedstaaten haben sich dafür entschieden, die durch die Richtlinie zum Datenschutz bei der Strafverfolgung gebotene Möglichkeit zu nutzen, das Recht betroffener Personen auf Auskunft über ihre personenbezogenen Daten einzuschränken[69]. Die meisten Mitgliedstaaten sehen auch Einschränkungen anderer Rechte betroffener Personen vor[70]. Die nationalen Datenschutzgesetze, mit denen die Richtlinie zum Datenschutz bei der Strafverfolgung umgesetzt wird, folgen häufig nur der allgemeinen Formulierung der Richtlinie, ohne die Umstände oder Bedingungen, unter denen die Einschränkungen anzuwenden sind, näher zu bestimmen. In solchen Fällen müssen diese Umstände und Bedingungen in den sektorspezifischen Rechtsvorschriften näher ausgeführt werden, da es sonst dem Ermessen der Verantwortlichen überlassen ist, wann sie diese Einschränkungen anwenden.

Die meisten Mitgliedstaaten sind der Anforderung der Richtlinie zum Datenschutz bei der Strafverfolgung nachgekommen, es betroffenen Personen zu ermöglichen, ihre Rechte über die Datenschutzaufsichtsbehörde auszuüben[71]. Ebenso haben die meisten Mitgliedstaaten von der

---

[66] Artikel 11 Absatz 1 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[67] Artikel 11 Absatz 2 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[68] Artikel 11 Absatz 3 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[69] Artikel 15 Absatz 1 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[70] Artikel 13 Absatz 3 und Artikel 16 Absatz 4 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[71] Artikel 17 der Richtlinie zum Datenschutz bei der Strafverfolgung.

Möglichkeit Gebrauch gemacht, zu bestimmen, dass die Rechte betroffener Personen im Kontext einzelstaatlicher strafrechtlicher Ermittlungen und Strafverfahren im Einklang mit dem nationalen Recht ausgeübt werden[72].

In den Umsetzungsgesetzen mehrerer Mitgliedstaaten spiegeln sich nicht alle spezifischen Anforderungen der Richtlinie zum Datenschutz bei der Strafverfolgung in Bezug auf die Art und Weise wider, wie die Rechte betroffener Personen auszuüben sind (z. B. Format und Kommunikationsmittel der Antworten, Unentgeltlichkeit).

Ein deutsches Gericht hat ein Vorabentscheidungsersuchen[73] vorgelegt, das die Auslegung der Einschränkungen des Rechts betroffener Personen auf Auskunft über ihre Daten (Artikel 15 der Richtlinie zum Datenschutz bei der Strafverfolgung im Lichte von Artikel 54 jener Richtlinie) sowie das Recht auf einen wirksamen gerichtlichen Rechtsbehelf nach Artikel 47 der Charta und die Berufsfreiheit nach Artikel 15 der Charta betrifft.

2.2.8 Einige wichtige Bestimmungen, die spezifisch für die Richtlinie zum Datenschutz bei der Strafverfolgung sind

Einige Bestimmungen der Richtlinie zum Datenschutz bei der Strafverfolgung sind spezifisch für den Kontext der Strafverfolgung und haben keine Entsprechung in der DSGVO.

Kategorien betroffener Personen

Die Mitgliedstaaten sind gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung verpflichtet, von einem Verantwortlichen zu verlangen, gegebenenfalls und so weit wie möglich zwischen den Daten verschiedener Kategorien betroffener Personen zu unterscheiden, und Beispiele für diese Kategorien anzugeben (z. B. „Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden“, kurz „Verdächtige“).[74] Die in der Richtlinie aufgeführten Kategorien finden sich in den Rechtsvorschriften einiger Mitgliedstaaten nur zum Teil bzw. überhaupt nicht wieder. Im Rahmen der Präzisierung der Kategorie „Verdächtige“ wird in einigen nationalen Gesetzen nicht vorausgesetzt, dass „ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden“. Die anstehende Entscheidung des EuGH in der anhängigen Rechtssache Ministerstvo na vatreshnite raboti/B. C.[75] wird für eine klarere Auslegung der Richtlinie zum Datenschutz bei der Strafverfolgung in Bezug auf die Kategorien betroffener Personen sorgen, einschließlich der Anforderung, dass die Kategorisierung betroffener Personen als Verdächtige davon abhängig sein sollte, dass „ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden“.

Unterscheidung zwischen Klassen personenbezogener Daten und Überprüfung der Datenqualität

---

[72] Artikel 18 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[73] Vorabentscheidungsersuchen in der Rechtssache TX/Bundesrepublik Deutschland, C-481/21.
[74] Artikel 6 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[75] Vorabentscheidungsersuchen in der Rechtssache Ministerstvo na vatreshnite raboti/B. C., C-205/21.

Die Mitgliedstaaten müssen vorsehen, dass bei personenbezogenen Daten so weit wie möglich zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten unterschieden wird.[76] Sie müssen ferner Maßnahmen ergreifen, um dafür zu sorgen, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Wenn unrichtige Daten übermittelt worden sind, sollte dies den Empfängern unverzüglich mitgeteilt werden; in diesen Fällen ist eine Berichtigung oder Löschung oder die Einschränkung der Verarbeitung der personenbezogenen Daten vorzunehmen. Die meisten Mitgliedstaaten haben diese Anforderung umgesetzt, jedoch sind einige der erforderlichen spezifischen Maßnahmen in mehreren nationalen Umsetzungsgesetzen nicht ausdrücklich vorgesehen.

Protokollierung

Insgesamt zwölf Mitgliedstaaten[77] haben die Möglichkeit genutzt, ihre automatisierten Verarbeitungssysteme erst bis zum Mai 2023 mit den Protokollierungspflichten in Einklang bringen zu müssen[78].

Die meisten Mitgliedstaaten sehen vor, dass in automatisierten Verarbeitungssystemen Verarbeitungsvorgänge protokolliert werden[79]. Die Protokollierung wird in einigen nationalen Gesetzen nicht für alle Arten von Vorgängen verlangt. In der Richtlinie zum Datenschutz bei der Strafverfolgung ist festgelegt, welche Arten von Informationen Protokolle mindestens enthalten müssen. In einigen einzelstaatlichen Rechtsvorschriften wurden nicht alle erforderlichen Arten von Informationen berücksichtigt (z. B. der Grund für die Abfrage oder Offenlegung personenbezogener Daten).

3 ERSTE ERKENNTNISSE ÜBER DIE ANWENDUNG UND WIRKUNGSWEISE DER RICHTLINIE ZUM DATENSCHUTZ BEI DER STRAFVERFOLGUNG

3.1 Beschwerden und positive Auswirkungen auf die Rechte betroffener Personen

Mit der Richtlinie zum Datenschutz bei der Strafverfolgung wird der Schutz der Grundrechte und -freiheiten natürlicher Personen und insbesondere des Rechts auf Datenschutz sichergestellt. Sie bietet einen umfassenden Rahmen für die Rechte der betroffenen Person und die Ausübung dieser Rechte, einschließlich des Rechts auf Unterrichtung, Auskunft, Berichtigung oder Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung. Die Richtlinie hat dafür gesorgt, dass betroffene Personen besser nachvollziehen, welche Rechte sie haben und wie sie diese ausüben können, was sich in der gestiegenen Zahl der Anträge widerspiegelt, die den zuständigen Behörden zugeleitet wurden. Die Praxis hat gezeigt, dass die Rechte auf Auskunft

[76] Artikel 7 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[77] Deutschland hat für bestimmte Gesetze auf Bundes- und Länderebene, mit denen die Richtlinie zum Datenschutz bei der Strafverfolgung umgesetzt wird, von der Möglichkeit Gebrauch gemacht.
[78] Artikel 63 Absatz 2 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[79] Artikel 25 der Richtlinie zum Datenschutz bei der Strafverfolgung.

und Löschung im Vergleich zu den anderen Rechten, die betroffenen Personen im Rahmen der Richtlinie übertragen wurden, am häufigsten bei den zuständigen Behörden geltend gemacht werden.[80]

Die Richtlinie zum Datenschutz bei der Strafverfolgung ermöglicht es, dass für bestimmte Rechte (das Auskunftsrecht[81] und das Recht auf Berichtigung oder Löschung[82]) sowie die Informationen, die ein Verantwortlicher der betroffenen Person in Bezug auf die verarbeiteten personenbezogenen Daten zur Verfügung stellen muss[83], Einschränkungen festgelegt werden. Die betroffenen Personen können bei den Datenschutzaufsichtsbehörden beantragen, dass sie eine Einschränkung des betreffenden Rechts durch eine zuständige Behörde überprüfen, oder sie auffordern, zu prüfen, ob die Einschränkung im Einklang mit der Richtlinie erfolgt ist (indirekte Ausübung des Rechts).[84] Ungefähr die Hälfte der Datenschutzaufsichtsbehörden berichtet, dass ein solcher Antrag eingegangen ist.[85] Die Praxis zeigt, dass es beträchtliche Unterschiede bei der Anzahl an eingegangenen Anträgen geben kann (z. B. ging in Kroatien ein solcher Antrag ein, während es in Frankreich jedoch mehr als 1500 waren).[86] Die Datenschutzaufsichtsbehörden entschieden nach einer Prüfung oder Überprüfung dieser Beschwerden, dass die meisten Anträge unzulässig waren, allerdings wurde in mehreren Fällen der Verantwortliche angewiesen, die personenbezogenen Daten zu berichtigen oder zu löschen oder ihre Verarbeitung einzuschränken, wodurch die ordnungsgemäße Anwendung der Einschränkungen sichergestellt wurde.[87]

Die Richtlinie zum Datenschutz bei der Strafverfolgung sieht vor, dass eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht eine Beschwerde im Namen einer betroffenen Person einreichen kann. Allem Anschein nach wird auf diese Möglichkeit jedoch nicht ausreichend zurückgegriffen (nur vier Datenschutzaufsichtsbehörden berichteten, dass bei ihnen eine solche Beschwerde eines repräsentativen Gremiums eingegangen war[88]). Ebenso meldeten die Organisationen der Zivilgesellschaft nur wenige Aufforderungen, eine solche Beschwerde einzureichen.[89]

---

[80] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 15.
[81] Artikel 15 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[82] Artikel 16 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[83] Artikel 13 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[84] Artikel 17 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[85] Vier Datenschutzaufsichtsbehörden erheben keine statistischen Daten zu den nach Artikel 17 der Richtlinie zum Datenschutz bei der Strafverfolgung eingegangenen Anträgen.
[86] Hierbei geht es um Anträge, die seit der Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung bis Dezember 2021 zugeleitet wurden. Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung (einzelne Antworten der Datenschutzbehörden).
[87] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 50.
[88] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 33.
[89] Drei Organisationen berichteten (im Rahmen der Antworten auf die Fragebögen, die ihnen von der Grundrechteagentur zugesandt wurden), dass sie eine Aufforderung erhalten hatten, und eine Organisation meldete, dass bei ihr mehr als eine Aufforderung eingegangen war.

Einzelpersonen nehmen des Weiteren zunehmend ihr Recht in Anspruch, Beschwerden bei Datenschutzaufsichtsbehörden einzureichen, einschließlich in Fällen, in denen zuständige Behörden die Ausübung der Rechte betroffener Personen einschränken. Mehr als ein Drittel der Datenschutzaufsichtsbehörden meldete eine gestiegene Anzahl an eingegangenen Beschwerden nach der Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung im jeweiligen Mitgliedstaat.[90] Einige der am häufigsten bei den Datenschutzaufsichtsbehörden eingegangenen Beschwerden betrafen die Einschränkung des Auskunftsrechts[91], das Recht auf Berichtigung oder Löschung[92] und das Recht auf Unterrichtung sowie dessen Einschränkungen[93]. Ferner betrafen die Beschwerden häufig den Grundsatz der Speicherbegrenzung, nach dem zuständige Behörden personenbezogene Daten nicht länger als erforderlich speichern dürfen.

3.2 Stärkeres Bewusstsein für den Datenschutz in den zuständigen Behörden

Die Mitgliedstaaten berichten, dass die Einführung der Richtlinie zum Datenschutz bei der Strafverfolgung zu einer deutlichen Sensibilisierung der zuständigen Behörden für die Bedeutung des Datenschutzes geführt hat und dies auch weiterhin tut.[94] Mehrere Datenschutzaufsichtsbehörden waren der Auffassung, dass die größte Auswirkung der Richtlinie darin bestand, für Datenschutzfragen und die Rechte betroffener Personen zu sensibilisieren und die Aufmerksamkeit auf diese Themen zu lenken.[95] Dies belegte auch der Austausch zwischen den Datenschutzaufsichtsbehörden und den zuständigen Behörden über die Rechte betroffener Personen und die Modalitäten für die Ausübung dieser Rechte.[96] Einige zuständige Behörden berichteten, dass sie aufgrund der Richtlinie mehr Ressourcen für den Datenschutz bereitgestellt hatten.[97] Dies umfasste Investitionen in die Einbeziehung des Grundsatzes des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in ihre IT-Systeme, die Festlegung von Fristen für die Vorratsdatenspeicherung, die Anwendung des Grundsatzes der Datenminimierung und die Meldung von Verstößen. Die allgemeine Sicherheit der verarbeiteten Daten soll sich in der Folge verbessert haben.[98]

Schulungen und Sensibilisierungsmaßnahmen der Datenschutzaufsichtsbehörden tragen auch zur ordnungsgemäßen Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung bei, und

---

[90] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 31.
[91] Artikel 15 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[92] Artikel 16 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[93] Artikel 13 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[94] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 21.
[95] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung (einzelne Antworten der Datenschutzbehörden).
[96] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 40, sowie Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, S. 9.
[97] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 70.
[98] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 70.

die Aufsichtsbehörden haben die Aufgabe, die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Richtlinie entstehenden Pflichten zu sensibilisieren[99].

Viele Datenschutzaufsichtsbehörden leisten Sensibilisierungsarbeit, indem sie Leitlinien veröffentlichen. Unter anderem werden von den verschiedenen Datenschutzaufsichtsbehörden folgende Themen behandelt: Unterstützung der Gerichte, der Staatsanwaltschaften und der Polizeibehörden bei der Einhaltung des Grundsatzes der Rechenschaftspflicht, Austausch personenbezogener Daten mit der Polizei, Bestellung eines Datenschutzbeauftragten, Durchführung einer Datenschutz-Folgenabschätzung, Verarbeitung von Daten im strafrechtlichen Bereich, etwa im Zusammenhang mit organisierter Kriminalität und Terrorismus, Führung eines Verzeichnisses von Verarbeitungstätigkeiten und Protokollierung, Durchführung einer Videoüberwachung, Unterrichtung betroffener Personen, Meldung von Datenschutzverletzungen, Pflichten von Verantwortlichen und Ausübung von Rechten durch natürliche Personen.

Acht Datenschutzaufsichtsbehörden haben jedoch noch keine Leitlinien und/oder praktischen Instrumente ausgearbeitet, um die zuständigen Behörden und Auftragsverarbeiter bei der Erfüllung ihrer Pflichten zu unterstützen.

Ferner haben zwölf Datenschutzaufsichtsbehörden den zuständigen Behörden oder Auftragsverarbeitern im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung weder Schulungen angeboten noch Sensibilisierungsmaßnahmen durchgeführt.[100] Von den Datenschutzaufsichtsbehörden, die solche Maßnahmen durchgeführt haben, wurden unter anderem die folgenden Themen am häufigsten behandelt: Datenverarbeitung durch die Polizei, die Staatsanwaltschaften und die Justiz- und Justizvollzugsbehörden, Definition der jeweiligen Anwendungsbereiche der DSGVO und der Richtlinie zum Datenschutz bei der Strafverfolgung, Verwendung personenbezogener Daten aus sozialen Medien, Verarbeitung von Daten aus Polizeiakten, Videoüberwachungsmethoden und Massendaten, Umgang mit den Rechten betroffener Personen und Verarbeitung personenbezogener Daten von Gefangenen.[101]

Eine weitere Neuerung der Richtlinie zum Datenschutz bei der Strafverfolgung ist die Anforderung, dass Verantwortliche einen Datenschutzbeauftragten (DSB) benennen müssen, zu dessen Pflichten unter anderem die Unterrichtung und Beratung zu Datenschutzanforderungen, die Überwachung der Einhaltung der Richtlinie, die Beratung zu Datenschutz-Folgenabschätzungen und die Überwachung ihrer Durchführung gehören.[102] Dies hat zu einer Sensibilisierung der zuständigen Behörden für ihre Datenschutzpflichten geführt und ihre

[99] Artikel 46 Absatz 1 Buchstabe d der Richtlinie zum Datenschutz bei der Strafverfolgung.
[100] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung (einzelne Antworten der Datenschutzbehörden).
[101] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummern 41–42.
[102] Artikel 32–34 der Richtlinie zum Datenschutz bei der Strafverfolgung.

Einhaltung der Datenschutzvorschriften positiv beeinflusst, was auch vom Rat anerkannt wurde.[103]

Es ist wichtig, in die Entwicklung und Optimierung des Fachwissens und der Kenntnisse der DSB zu investieren, um den zuständigen Behörden bei der kohärenten Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung zu helfen.[104] Die Kommission hat daher das Netz der Datenschutzbeauftragten der zuständigen Behörden, der Agenturen im Bereich Justiz und Inneres und der Europäischen Staatsanwaltschaft eingerichtet und unterstützt dieses. Das Netz ist eine ständige Initiative, deren Schwerpunkt auf der Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung durch die zuständigen Behörden der Mitgliedstaaten liegt. Es dient dazu, eine Plattform für die Zusammenarbeit und den Austausch von Fachwissen zwischen den DSB der Mitgliedstaaten zu bieten. Das Europol-Netzwerk der Datenschutzexperten (EDEN) und die Netze der nationalen DSB für die zuständigen Behörden sind wichtige Initiativen, die den DSB der zuständigen Behörden dabei helfen, den Austausch von bewährten Verfahren und Informationen zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung zu fördern.

3.3 Verbesserte Datensicherheit, aber Unterschiede bei der Meldung von Datenschutzverletzungen

Die Richtlinie zum Datenschutz bei der Strafverfolgung hat die Sicherheit personenbezogener Daten verbessert, indem von zuständigen Behörden verlangt wird, Maßnahmen zu ergreifen, um spezifische Sicherheitsziele zu erreichen. Beispielsweise müssen zuständige Behörden Datenschutz-Folgenabschätzungen durchführen, wenn eine Datenverarbeitungstätigkeit voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. Im Rahmen der Folgenabschätzungen werden Risiken ermittelt und Maßnahmen zu ihrer Eindämmung bestimmt. Diese Anforderung sowie die Verpflichtung zur Einhaltung des Grundsatzes des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie der Vorschriften zur Meldung von Datenschutzverletzungen haben eine Verbesserung der Sicherheit der Verarbeitung personenbezogener Daten bewirkt.[105]

Der Rat hat dies ebenfalls anerkannt und war der Auffassung, dass die Richtlinie zum Datenschutz bei der Strafverfolgung das Maß an Datensicherheit unter anderem durch Sicherheitspläne, die Aktualisierung von IT-Systemen und organisatorischen Maßnahmen,

---

[103] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 22.
[104] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 25.
[105] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummern 70 und 71 sowie einzelne Antworten der Datenschutzbehörden (Deutschland, Finnland, Frankreich, Malta, Ungarn).

Datenschutz-Folgenabschätzungen und die Verpflichtung der zuständigen Behörden zur Führung von Protokollen für bestimmte Verarbeitungsvorgänge verbessert hat.[106]

In der Richtlinie zum Datenschutz bei der Strafverfolgung wird dargelegt, unter welchen Umständen Verantwortliche ihrer Datenschutzaufsichtsbehörde und der betroffenen Person eine Verletzung des Schutzes personenbezogener Daten melden müssen.[107] Trotz dieser Verpflichtung gibt es große Unterschiede bei der Anzahl an Datenschutzverletzungen, die den Datenschutzaufsichtsbehörden seit der Einführung der Richtlinie gemeldet wurden.[108] Sechs Datenschutzaufsichtsbehörden berichteten, dass bei ihnen keine Meldungen von Datenschutzverletzungen eingegangen waren[109], und andere berichteten, dass sie nur sehr wenige dieser Meldungen erhalten hatten. Beispielsweise waren es bei der italienischen Behörde nur drei und bei der französischen Behörde acht Meldungen von Datenschutzverletzungen, bei der niederländischen Behörde hingegen über 500.

Die Unterschiede bei der Zahl der Meldungen von Datenschutzverletzungen lassen (nach Berücksichtigung von Faktoren wie der Bevölkerungsgröße) darauf schließen, dass es scheinbar unterschiedliche Verfahrensweisen zwischen den zuständigen Behörden der Mitgliedstaaten in Bezug darauf gibt, was als Verletzung angesehen wird und wann eine Verletzung einer Datenschutzaufsichtsbehörde gemeldet werden muss. Die Kommission stellte dies in ihrem Bericht über die DSGVO ebenfalls fest.[110] Der EDSA hat kürzlich Leitlinien zu Datenschutzverletzungen im Rahmen der DSGVO veröffentlicht.[111] Diese Leitlinien sind für Datenschutzverletzungen im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung zwar nicht unmittelbar anwendbar, aber ebenfalls von Bedeutung. Sie sollten daher zu einer einheitlicheren Vorgehensweise beim Umgang mit Datenschutzverletzungen gemäß der Richtlinie in den Mitgliedstaaten beitragen.

3.4 Aufsicht durch die Datenschutzaufsichtsbehörden

---

[106] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 26.
[107] Artikel 30 und 31 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[108] Die Zahlen umfassen alle Datenschutzverletzungen, die seit der Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung bis Dezember 2021 gemeldet wurden. Die Daten wurden im Dezember 2021 von den Datenschutzaufsichtsbehörden eingeholt.
[109] Spanien, Kroatien, Litauen, Portugal, Slowakei und Slowenien.
[110] Arbeitsunterlage der Kommissionsdienststellen, Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung“ (COM(2020) 264 final).
[111] EDSA, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification (Leitlinien 01/2021 zu Beispielen in Bezug auf die Meldung von Verletzungen des Schutzes personenbezogener Daten), angenommen am 14. Dezember 2021. https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

3.4.1 Ressourcen der Datenschutzaufsichtsbehörden

Die Ausstattung jeder Datenschutzbehörde mit den erforderlichen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ist Voraussetzung, damit sie ihre Aufgaben und Befugnisse effektiv wahrnehmen kann, und bildet somit die Grundlage für ihre Unabhängigkeit.[112] Die Kommission hat immer wieder betont, dass die Mitgliedstaaten verpflichtet sind, den Datenschutzaufsichtsbehörden ausreichende personelle, finanzielle und technische Ressourcen bereitzustellen.[113] Der Rat hat von den Mitgliedstaaten ebenfalls ausdrücklich gefordert, dass sie den Datenschutzaufsichtsbehörden ausreichende personelle, technische und finanzielle Ressourcen zur Verfügung stellen.[114]

Die allgemeine Personalaufstockung der Datenschutzaufsichtsbehörden in den letzten Jahren[115] scheint die Aufgaben im Zusammenhang mit der Richtlinie zum Datenschutz bei der Strafverfolgung jedoch nicht zu betreffen. Die Anzahl der Mitarbeiter, die sich mit der Richtlinie befassen, ist in der Hälfte der Datenschutzaufsichtsbehörden gleich geblieben oder sogar gesunken.[116] Die jeweiligen Aufstockungen waren äußerst bescheiden und entsprachen durchschnittlich weniger als zwei Personen in Vollzeitäquivalenten (VZÄ).[117] In fast der Hälfte der Datenschutzaufsichtsbehörden (einschließlich derer mit einer Gesamtzahl an Beschäftigten von mehr als 100 VZÄ) befassen sich zwischen weniger als 1 % und 7 % des gesamten Personals mit der Richtlinie zum Datenschutz bei der Strafverfolgung.[118] In absoluten Zahlen sieht etwa die Hälfte der Datenschutzaufsichtsbehörden zwischen 1 und 4 VZÄ für Aufgaben im Zusammenhang mit der Richtlinie vor, während es bei acht Datenschutzaufsichtsbehörden zwischen 7 und 15 VZÄ sind. In einer Datenschutzaufsichtsbehörde beschäftigen sich jedoch 53 VZÄ mit der Richtlinie.[119] Ähnlich ist die Situation beim Sekretariat des EDSA, das für

---

[112] Artikel 42 Absatz 4 der Richtlinie zum Datenschutz bei der Strafverfolgung.

[113] Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung“ (COM(2020) 264 final).

[114] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 12.

[115] Contribution of the EDPB to the evaluation of the GDPR under Article 97 (Beitrag des EDSA zur Bewertung der DSGVO nach Artikel 97), 18. Februar 2020, S. 26–29.
https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf;
EDSA, Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities (Überblick über die Ressourcen, die den Datenschutzbehörden von den Mitgliedstaaten zur Verfügung gestellt wurden, und die Durchsetzungsmaßnahmen der Datenschutzbehörden, im Folgenden „Überblick des EDSA über die Ressourcen“), 5. August 2021, S. 4–5.
https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/overview-resources-made-available-member-states-data_en

[116] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 65 sowie Abbildung zu Q41, S. 20.

[117] Deutschland meldete eine erhebliche Aufstockung von 33 auf 53 VZÄ zwischen 2017 und 2021.

[118] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Abbildung zu Q41, S. 20. Überblick des EDSA über die Ressourcen, S. 5.

[119] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Abbildung zu Q41, S. 19.

Fragen, die ausschließlich mit der Richtlinie im Zusammenhang stehen, weniger als 1,5 VZÄ zugewiesen hat.

Diese Situation ist nicht zufriedenstellend, auch wenn zehn Datenschutzaufsichtsbehörden angegeben haben, dass sie über ausreichende finanzielle, personelle und technische Ressourcen verfügen.[120] 16 Datenschutzaufsichtsbehörden waren hingegen der Ansicht, dass die ihnen zur Verfügung stehenden Ressourcen nicht ausreichen. Von diesen Behörden wiesen manche darauf hin, dass sich dies negativ auf ihre Untersuchungen aus eigener Initiative[121], ihre Bearbeitung von Beschwerden[122], die Prüfung von IT-Großsystemen (SIS, VIS) und die Abgabe von Stellungnahmen aus eigener Initiative[123] auswirkte. Tatsächlich ist es aufgrund der Besonderheiten des Sektors so, dass die wirksame Durchsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung eine systematische Prüfung der oft komplexen Verarbeitungstätigkeiten erfordert und dass es nicht genügt, sich auf einzelne Beschwerden zu stützen (von denen es deutlich weniger gibt als im Falle der DSGVO).[124]

Darüber hinaus haben die Datenschutzaufsichtsbehörden auf die mangelnden IT-Fachkenntnisse hingewiesen, die benötigt werden, um die ständig zunehmende Komplexität der im Bereich der Strafverfolgung verwendeten IT-Technologien zu bewältigen.[125]

3.4.2 Ausübung von Befugnissen

Ausübung von Abhilfebefugnissen

Insgesamt 19 Datenschutzaufsichtsbehörden wandten ihre Untersuchungsbefugnisse an, entweder aus eigener Initiative oder auf der Grundlage einer Beschwerde.[126] Die Datenschutzaufsichtsbehörden meldeten nur in sehr wenigen Fällen Schwierigkeiten (z. B. wenn ein Verantwortlicher nicht alle maßgeblichen Informationen zur Verfügung stellte oder den Zugriff auf Informationen verweigerte).[127]

---

[120] Belgien, Dänemark, Irland, Griechenland, Lettland, Luxemburg, Ungarn, Malta, Österreich und Finnland.
[121] Deutschland und Frankreich.
[122] Frankreich und Schweden.
[123] Die Niederlande.
[124] Seit 2018 haben Irland und Ungarn 135 bzw. 141 Beschwerden im Zusammenhang mit der Richtlinie zum Datenschutz bei der Strafverfolgung erhalten, in Dänemark gingen seit 2017 insgesamt 223 solcher Beschwerden ein. Im Zusammenhang mit der DSGVO gab es dagegen Tausende Beschwerden (siehe Überblick des EDSA über die Ressourcen, S. 10).
[125] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 69.
[126] Die Datenschutzaufsichtsbehörden von Irland, Malta und den Niederlanden berichteten, dass sie Untersuchungen aus eigener Initiative durchgeführt hatten. Die Datenschutzaufsichtsbehörden von Griechenland, Spanien, Litauen und Ungarn nahmen Untersuchungen auf der Grundlage von Beschwerden vor. Die Datenschutzaufsichtsbehörden von Belgien, Bulgarien, Dänemark, Deutschland, Frankreich, Italien, Luxemburg, Österreich, Polen, Slowenien und Schweden führten Untersuchungen sowohl aus eigener Initiative als auch auf der Grundlage von Beschwerden durch.
[127] Die Datenschutzaufsichtsbehörden von Deutschland und Ungarn gaben an, dass sie nicht alle erforderlichen Informationen erhalten hatten und/oder dass der Verantwortliche ihnen den Zugriff auf erforderliche Informationen

Dieselben 19 Datenschutzaufsichtsbehörden wandten auch ihre Abhilfebefugnisse an. Die bei Weitem am häufigsten ausgeübte Befugnis war die Erteilung von Anweisungen, die Verarbeitung mit dem Recht in Einklang zu bringen, einschließlich Anweisungen zur Berichtigung oder Löschung personenbezogener Daten oder zur Einschränkung ihrer Verarbeitung. Die Datenschutzaufsichtsbehörden machten von dieser Befugnis in 114 Fällen Gebrauch. Die Tatsache, dass die Befugnis zur Anweisung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung (einschließlich eines Verbots) nur in vier Fällen genutzt wurde[128], zeigt, dass die Datenschutzaufsichtsbehörden diese Befugnisse sorgfältig angewandt haben.

Ausübung von beratenden Befugnissen

Die systematische Durchführung vorheriger Konsultationen der Datenschutzaufsichtsbehörden und das Ersuchen dieser Behörden um Stellungnahmen zu Entwürfen von legislativen und administrativen Maßnahmen sind wirksame Mittel, um ein hohes Schutzniveau für das Recht auf Schutz personenbezogener Daten sicherzustellen und die Anzahl der späteren Beschwerden zu verringern. Die vorherige Konsultation der Datenschutzaufsichtsbehörden ist von besonderer Bedeutung, wenn neue Technologien eingesetzt werden, die erhebliche Auswirkungen auf die Grundrechte haben können.

Die Hälfte der Datenschutzaufsichtsbehörden berichtete, dass sie zu Datenschutz-Folgenabschätzungen konsultiert wurden. Je nach Mitgliedstaat ist die Anzahl der vorherigen Konsultationen unterschiedlich. Manche Behörden wurden nur einmal konsultiert, eine andere Behörde hingegen in 59 Fällen.[129] Die Datenschutzaufsichtsbehörden erteilten in den meisten Fällen schriftlichen Rat und übten in einigen Fällen ihre Abhilfebefugnisse in Bezug auf die Verarbeitung aus, insbesondere durch Warnungen oder die Anweisung von Maßnahmen, um die Datenverarbeitung mit dem Recht in Einklang zu bringen. In einem Fall gab die Datenschutzaufsichtsbehörde eine negative Stellungnahme ab, die scheinbar die gleiche Wirkung wie ein Verbot der Verarbeitung hatte.

Des Weiteren scheinen sich die Datenschutzaufsichtsbehörden auch außerhalb des Verfahrens der vorherigen Konsultation mit Ersuchen um Beratung zu befassen. Am häufigsten wandten sich die zuständigen Behörden für Beratung an die Datenschutzaufsichtsbehörden, wenn es um spezifische Arten der Verarbeitung ging (insbesondere um die Nutzung neuer Technologien, Mechanismen oder Verfahren, dicht gefolgt von angemessenen Sicherheitsmaßnahmen, der Verarbeitung besonderer Kategorien personenbezogener Daten, der Bestimmung der

---

verweigerte. Die deutschen Behörden erwähnten, dass eine ähnliche Befugnis wie die nach Artikel 58 Absatz 1 Buchstabe a der DSGVO nicht vorgesehen ist.

[128] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 30 sowie auch die einzelnen Antworten der Behörden von Österreich und Luxemburg.

[129] Die Datenschutzaufsichtsbehörden von Dänemark und Litauen berichteten, dass sie nur einmal konsultiert wurden. Die Datenschutzaufsichtsbehörde Belgiens wurde in 59 Fällen konsultiert.

Rechtsgrundlage der Verarbeitung, dem Grundsatz der Speicherbegrenzung und angemessenen Fristen[130]).

Ferner gaben 22 Datenschutzaufsichtsbehörden für ihre nationalen Parlamente und Regierungen Stellungnahmen zu legislativen und administrativen Maßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten ab. Einige Datenschutzaufsichtsbehörden gaben an, dass sie gelegentlich konsultiert werden.[131]

3.4.3 Gerichtliche Überprüfung der Maßnahmen von Datenschutzaufsichtsbehörden

Fast die Hälfte der Datenschutzaufsichtsbehörden gab an, dass sie in einigen wenigen Fällen mit Gerichtsverfahren aufgrund ihrer Beschlüsse oder ihrer Untätigkeit konfrontiert waren. Die Verfahren wurden hauptsächlich von betroffenen Personen eingeleitet, vereinzelt auch von zuständigen Behörden.[132] Einige Fälle wurden von den Gerichten für unzulässig erklärt oder von den Klägern zurückgezogen. Die Gerichte bestätigten die Beschlüsse der Datenschutzaufsichtsbehörden in den meisten übrigen Fällen, machten jedoch auch manche rückgängig (weitere Fälle waren zudem noch anhängig). Aufgrund der geringen Anzahl von Urteilen ist es bislang noch nicht möglich, einen klaren Trend festzustellen.

3.4.4 EDPB-Leitlinien

Einheitlichkeit und ein hohes Schutzniveau in den Mitgliedstaaten sind für den Zweck der wirksamen justiziellen Zusammenarbeit in Strafsachen und der wirksamen polizeilichen Zusammenarbeit entscheidend.[133] Die Richtlinie zum Datenschutz bei der Strafverfolgung sieht vor, dass der EDSA Leitlinien, Empfehlungen und bewährte Verfahren zwecks Sicherstellung einer einheitlichen Anwendung dieser Richtlinie durch die Mitgliedstaaten ausarbeitet (von sich aus oder auf Ersuchen der Kommission). Der EDSA hat spezifische Leitlinien zur Richtlinie, die für Kapitel V (grenzüberschreitende Datenübermittlungen) relevant sind[134], Leitlinien zum Einsatz von Gesichtserkennungstechnologien[135] sowie (in seiner früheren Funktion als Artikel-

---

[130] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 39.
[131] Die Datenschutzaufsichtsbehörden von Tschechien, Griechenland, Kroatien, Lettland und Schweden berichteten, dass sie keine Stellungnahmen abgegeben hatten. Die Datenschutzaufsichtsbehörden von Griechenland, Kroatien, Lettland, Polen, Rumänien, Slowenien und der Slowakei wurden nur gelegentlich konsultiert.
[132] Diese Beobachtung beruht auf den Antworten der Datenschutzaufsichtsbehörden aus Belgien, Bulgarien, Deutschland, Estland, Irland, Italien, Ungarn, den Niederlanden, Österreich, Polen, Finnland und Schweden.
[133] Erwägungsgrund 7 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[134] EDSA, Empfehlungen 01/2021 zu der Referenzgrundlage für den Begriff „Angemessenheit“ in der Richtlinie zum Datenschutz bei der Strafverfolgung, angenommen am 2. Februar 2021.
https://edpb.europa.eu/system/files/2021-06/recommendations012021onart.36led.pdf_de.pdf
[135] EDSA, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Leitlinien 05/2022 zum Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung), angenommen am 12. Mai 2022, Version für die öffentliche Konsultation, verfügbar unter https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

29-Datenschutzgruppe) eine Stellungnahme zu einigen wesentlichen Aspekten der Richtlinie[136] erstellt.

Viele der Leitlinien des EDSA zur DSGVO sind auch insofern für die Richtlinie zum Datenschutz bei der Strafverfolgung relevant, als sie sich auf gemeinsame Begriffe oder Technologien stützen. Zu diesen Leitlinien gehören etwa die zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“[137], zu den Rechten betroffener Personen[138], zur Meldung von Verletzungen des Schutzes personenbezogener Daten[139], zur Datenschutz-Folgenabschätzung[140], zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[141] und zu automatisierten Entscheidungen im Einzelfall[142].

Die Erarbeitung umfassender und praktischer Leitlinien erfordert erhebliche Arbeit und Ressourcen, allerdings sind Leitlinien von wesentlicher Bedeutung (was auch der Rat festgestellt hat[143]). Es ist daher äußerst positiv, dass der EDSA signalisiert hat, dass er demnächst zusätzliche Leitlinien bieten wird, einschließlich zum Konzept der wirksamen Untersuchungs- und Abhilfebefugnisse der Datenschutzaufsichtsbehörden und zu grenzüberschreitenden Datenübermittlungen, die geeigneten Garantien unterliegen.

---

[136] Artikel-29-Datenschutzgruppe, Stellungnahme zu einigen wesentlichen Aspekten der Richtlinie zum Datenschutz bei der Strafverfolgung (EU 2016/680), WP 258, angenommen am 29. November 2017, verfügbar unter https://ec.europa.eu/newsroom/article29/items/610178/en.

[137] EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, angenommen am 7. Juli 2021, verfügbar unter https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf.

[138] EDSA, Guidelines 01/2022 on data subject rights – Right of access (Leitlinien 01/2022 zu den Rechten betroffener Personen – Auskunftsrecht), angenommen am 18. Januar 2022, Version für die öffentliche Konsultation, verfügbar unter https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

[139] Artikel-29-Datenschutzgruppe, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250rev.01, zuletzt überarbeitet am 6. Februar 2018 und vom EDSA gebilligt am 25. Mai 2018, verfügbar unter https://ec.europa.eu/newsroom/article29/items/612052/en; EDSA, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification (Leitlinien 01/2021 zu Beispielen in Bezug auf die Meldung von Verletzungen des Schutzes personenbezogener Daten), angenommen am 14. Dezember 2021, verfügbar unter https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf.

[140] Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob
eine Verarbeitung im Sinne der Verordnung (EU) 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev. 01, zuletzt überarbeitet am 4. Oktober 2017 und vom EDSA gebilligt am 25. Mai 2018, verfügbar unter https://ec.europa.eu/newsroom/article29/items/611236.

[141] EDSA, Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, angenommen am 20. Oktober 2020, verfügbar unter https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf.

[142] Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP251rev.01, zuletzt überarbeitet am 6. Februar 2018 und vom EDSA gebilligt am 25. Mai 2018, verfügbar unter https://ec.europa.eu/newsroom/article29/items/612053/en.

[143] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 14.

Die EDSA-Leitlinien können auch die Arbeitsbelastung der Datenschutzaufsichtsbehörden verringern (z. B. in Bezug auf Aufgaben wie die Beratung von Verantwortlichen oder die Bearbeitung von Beschwerden). Beispielsweise gehören einige der Themen, die in der Stellungnahme der Artikel-29-Datenschutzgruppe zu einigen wesentlichen Aspekten der Richtlinie zum Datenschutz bei der Strafverfolgung behandelt werden (etwa angemessene Fristen, die Rechtsgrundlage für die Verarbeitung oder die Bedingungen für die Verarbeitung besonderer Kategorien von Daten), auch zu den Themen, aufgrund derer die Datenschutzaufsichtsbehörden von den zuständigen Behörden am häufigsten um Rat ersucht wurden.[144]

3.4.5 Gegenseitige Amtshilfe

Zur Sicherstellung der einheitlichen Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung müssen die Datenschutzaufsichtsbehörden einander Amtshilfe gewähren. Diese Hilfe bezieht sich unter anderem auf Auskunftsersuchen sowie Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.[145] Die gegenseitige Amtshilfe wurde bisher jedoch äußerst selten genutzt. Nur sechs Datenschutzaufsichtsbehörden haben von ihr Gebrauch gemacht, hauptsächlich durch Antworten auf Auskunftsersuchen anderer Datenschutzaufsichtsbehörden. Die Mehrheit der Datenschutzaufsichtsbehörden gab an, dass bei ihnen nur ein Auskunftsersuchen eingegangen war. Alle diese Datenschutzaufsichtsbehörden berichteten, dass sie dem eingegangenen Ersuchen nachgekommen waren. Der freiwillige Austausch gegenseitiger Amtshilfe, der keine vorgeschriebene Frist und keine strenge Antwortpflicht mit sich bringt, wurde auch nicht genutzt. Der EDSA hat mitgeteilt, dass er Leitlinien zum Rahmen für die gegenseitige Amtshilfe gemäß der DSGVO und der Richtlinie zum Datenschutz bei der Strafverfolgung veröffentlichen wird.[146]

3.5 Flexibles Instrument für grenzüberschreitende Datenübermittlungen

In Kapitel V der Richtlinie zum Datenschutz bei der Strafverfolgung geht es um die Übermittlung personenbezogener Daten an zuständige Behörden in Drittländern und internationalen Organisationen. Dieses Kapitel sorgt im Wesentlichen für einen kontinuierlichen Schutz personenbezogener Daten, wenn diese zum Zwecke der Strafverfolgung von einem Mitgliedstaat an ein Drittland oder eine internationale Organisation übermittelt werden. Wie bereits erwähnt, ist eine solche Kontinuität des Schutzes eine wichtige Voraussetzung für eine schnelle, wirksame und rechtssichere Zusammenarbeit auf dem Gebiet der Strafverfolgung zwischen Vertrauenspartnern.

---

[144] Beitrag des EDSA zur Bewertung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 39.
[145] Artikel 50 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[146] EDPB Work Programme 2021/2022 (Arbeitsprogramm des EDSA 2021/2022), https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf.

Insbesondere müssen grenzüberschreitende Datenübermittlungen zwischen zuständigen Behörden im Sinne der Richtlinie zum Datenschutz bei der Strafverfolgung nach den einschlägigen Vorschriften der Richtlinie[147] auf einem der verschiedenen Datenübermittlungsinstrumente gemäß den Artikeln 36 bis 38 der Richtlinie beruhen (stammen die Daten von einem anderen Mitgliedstaat, ist auch die vorherige Genehmigung dieses Mitgliedstaats für die Datenübermittlung erforderlich). Diese Instrumente umfassen Angemessenheitsbeschlüsse, Datenübermittlungen auf der Grundlage geeigneter Garantien und Ausnahmen in bestimmten Fällen. Artikel 39 der Richtlinie zum Datenschutz bei der Strafverfolgung ermöglicht auch im speziellen Einzelfall und unter bestimmten Bedingungen direkte Datenübermittlungen an in Drittländern niedergelassene Empfänger, die keine Strafverfolgungsbehörden sind.

3.5.1 Angemessenheitsbeschlüsse

Die Kommission hat ihre Arbeiten beschleunigt, um das Potenzial der im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung zur Verfügung stehenden Instrumente voll auszuschöpfen. In diesem Zusammenhang wurde im Juni 2021 erstmals ein „Angemessenheitsbeschluss“ mit Blick auf Datenverarbeitungstätigkeiten zum Zwecke der Strafverfolgung gemäß Artikel 36 der Richtlinie angenommen, in dem es um das Vereinigte Königreich ging.[148] Dieser Angemessenheitsbeschluss ermöglicht den sicheren und freien Verkehr personenbezogener Daten zu den zuständigen Behörden des betreffenden Drittlands, ohne dass weitere Garantien oder eine besondere Genehmigung notwendig sind (es sei denn, dass ein anderer Mitgliedstaat, von dem die Daten stammen, die Übermittlung zu genehmigen hat[149]). Der im Juni 2021 erlassene Angemessenheitsbeschluss für das Vereinigte Königreich ist eine entscheidende Grundlage für die polizeiliche und justizielle Zusammenarbeit nach dem Brexit, die laut dem Abkommen über Handel und Zusammenarbeit zwischen der EU und dem Vereinigten Königreich „auf dem langjährigen Engagement der Vertragsparteien zur Gewährleistung eines hohen Schutzniveaus für personenbezogene Daten“[150] beruht. Gemäß Artikel 36 Absatz 4 der Richtlinie zum Datenschutz bei der Strafverfolgung überwacht die

---

[147] Siehe Artikel 35 Absatz 3 und Erwägungsgrund 64 der Richtlinie zum Datenschutz bei der Strafverfolgung. In Bezug auf Weiterübermittlungen siehe Artikel 35 Absatz 1 Buchstabe e und Erwägungsgrund 65 der Richtlinie.

[148] Durchführungsbeschluss der Kommission vom 28. Juni 2021 gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, verfügbar unter https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_de.pdf.

[149] Siehe Artikel 35 Absatz 1 Buchstabe c, Artikel 35 Absatz 2 und Erwägungsgrund 66 der Richtlinie zum Datenschutz bei der Strafverfolgung.

[150] Siehe Artikel 525 Absatz 1 des Abkommens über Handel und Zusammenarbeit zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits.

Kommission die Entwicklungen im Rechtsrahmen des Vereinigten Königreichs, die diesen Angemessenheitsbeschluss beeinträchtigen könnten. Der Angemessenheitsbeschluss in Bezug auf das Vereinigte Königreich gilt ab seinem Inkrafttreten für einen Zeitraum von vier Jahren und ist grundsätzlich um vier weitere Jahre verlängerbar, wenn durch die Überwachung der Kommission bestätigt wird, dass das Schutzniveau des Vereinigten Königreichs weiterhin angemessen ist.[151]

Des Weiteren hat der EDSA auch zur Entwicklung dieses Instruments beigetragen, indem er mit seinen Empfehlungen zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung durch Leitlinien zu den Elementen, die bei der Beurteilung der Angemessenheit im Kontext der Strafverfolgung berücksichtigt werden müssen, die Rechtsnorm erläutert hat.[152] Insbesondere muss das Drittland durchsetzbare Rechte des Einzelnen, wirksame gerichtliche Rechtsbehelfe und eine unabhängige Überwachung sicherstellen.

Die Kommission fördert aktiv die Möglichkeit von Angemessenheitsfeststellungen für andere wichtige internationale Partner, insbesondere für Länder, mit denen eine enge und rasche Zusammenarbeit bei der Bekämpfung von Kriminalität und Terrorismus erforderlich ist und bereits ein umfangreicher Austausch personenbezogener Daten stattfindet.[153] Bisher wurden keine weiteren Angemessenheitsbeschlüsse erlassen, was aber hauptsächlich darauf zurückzuführen ist, dass dieses Instrument erst vor Kurzem eingeführt wurde. Darüber hinaus beginnt die globale Angleichung der Datenschutzvorschriften im Bereich der Strafverfolgung (anders als im Falle der Datenverarbeitung durch Wirtschaftsteilnehmer) gerade erst, sich zu entwickeln (beispielsweise durch multilaterale Vereinbarungen wie die modernisierte Konvention 108 des Europarats oder das Zweite Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität). Dennoch werden die Erkenntnisse, die durch die Annahme des Angemessenheitsbeschlusses für das Vereinigte Königreich gewonnen wurden, dabei helfen, den Weg für ähnliche Initiativen in den kommenden Jahren zu ebnen. Die Kommission wird im Rahmen ihrer internationalen Strategie weitere mögliche Kandidaten für zukünftige Angemessenheitsbeschlüsse gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung in Betracht ziehen und sich dabei unmittelbar mit den anderen einschlägigen

---

[151] Siehe die Absätze 172 bis 174 des Durchführungsbeschlusses der Kommission vom 28. Juni 2021 gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, verfügbar unter https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-law-enforcement-directive_de.

[152] EDSA, Empfehlungen 01/2021 zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung, angenommen am 2. Februar 2021. Siehe auch Artikel 36 Absatz 2 und Erwägungsgrund 67 der Richtlinie zum Datenschutz bei der Strafverfolgung.

[153] Siehe die Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Austausch und Schutz personenbezogener Daten in einer globalisierten Welt" (COM(2017) 7 final, S. 15).

Organen und Einrichtungen der EU austauschen.[154] Zu diesem Zweck und im Einklang mit dem Erwägungsgrund 68 der Richtlinie wird die Kommission besonderes Augenmerk auf die internationalen Verpflichtungen der geprüften Länder im Hinblick auf den Schutz personenbezogener Daten legen, einschließlich des Beitritts zu den oben erwähnten multilateralen Vereinbarungen oder zu anderen Strafverfolgungsinstrumenten, die geeignete Datenschutzgarantien bieten.

3.5.2 Geeignete Garantien

Zusätzlich zur umfassenden Lösung eines Angemessenheitsbeschlusses enthält die Richtlinie zum Datenschutz bei der Strafverfolgung weitere Instrumente für die Datenübermittlung. Die Flexibilität dieses „Werkzeugkastens" spiegelt sich in Artikel 37 der Richtlinie wider, der Datenübermittlungen vorbehaltlich „geeigneter Garantien" für den Schutz personenbezogener Daten regelt. Solche geeigneten Garantien lassen sich entweder durch ein rechtsverbindliches Instrument oder dadurch bieten, dass der Verantwortliche auf der Grundlage einer Beurteilung aller Umstände, die bei der Datenübermittlung eine Rolle spielen, zu der Auffassung gelangt, dass geeignete Garantien bestehen (hierbei spricht man von der sogenannten „Selbstbeurteilung" für Datenübermittlungen).

In den ersten Jahren der Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung arbeitete die Kommission insbesondere an verbindlichen Rechtsinstrumenten in Form von internationalen Übereinkünften, die geeignete Garantien vorsehen. Diese Übereinkünfte spielen im Kontext sowohl „traditioneller" (d. h. der Zusammenarbeit zwischen zuständigen Behörden) als auch anderer Formen der Zusammenarbeit auf dem Gebiet der Strafverfolgung (d. h. der Zusammenarbeit, in die Dritte wie private Unternehmen eingebunden sind) eine wichtige Rolle. Sie können auch als Grundlage für Datenübermittlungen durch Europol und Eurojust nach ihren jeweiligen Rechtsrahmen dienen, deren Vorschriften zu grenzüberschreitenden Datenübermittlungen denen in der Richtlinie zum Datenschutz bei der Strafverfolgung stark ähneln.

In Bezug auf traditionelle Formen der Zusammenarbeit auf dem Gebiet der Strafverfolgung überprüft die Kommission internationale Übereinkünfte, die vor dem Inkrafttreten der Richtlinie zum Datenschutz bei der Strafverfolgung angenommen wurden, um die Kohärenz mit den modernisierten Datenschutzregelungen der EU sicherzustellen.[155]

---

[154] Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 18.

[155] In ihrer Mitteilung mit dem Titel „Weiteres Vorgehen hinsichtlich der Angleichung des früheren Besitzstands des dritten Pfeilers an die Datenschutzvorschriften" kam die Kommission zu dem Schluss, dass einige bestehende Übereinkünfte keiner weiteren Angleichung an die Richtlinie zum Datenschutz bei der Strafverfolgung bedürfen (z. B. das Abkommen zwischen der Europäischen Union sowie der Republik Island und dem Königreich Norwegen

Erstens bewertet die Kommission die Datenschutzbestimmungen, die in den bestehenden Kooperationsabkommen von Europol[156] enthalten sind, die vor dem 1. Mai 2017 mit Drittstaaten geschlossen wurden, wie es in der Verordnung (EU) 2016/794 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (im Folgenden „Europol-Verordnung“) verlangt wird[157]. Im Einklang mit Artikel 9 des dem Vertrag über die Europäische Union[158] und dem AEUV beigefügten Protokolls Nr. 36 (über die Übergangsbestimmungen) behalten diese Übereinkünfte weiterhin Rechtswirkung, bis sie aufgehoben, für nichtig erklärt oder geändert werden.[159] Die Kommission unterrichtet das Europäische Parlament und den Rat über das Ergebnis dieser Bewertung und legt dem Rat gegebenenfalls nach Artikel 218 AEUV eine Empfehlung für einen Beschluss über die Ermächtigung zur Aufnahme von Verhandlungen zur Änderung der jeweiligen Übereinkünfte vor. Dies ist eine komplexe Aufgabe, die die Prüfung von 18 Übereinkünften erfordert und sich durch die Beeinträchtigungen aufgrund der COVID-19-Pandemie verzögert hat. Die Kommission geht davon aus, ihre Bewertung im zweiten Halbjahr 2022 abschließen zu können.

Die Kohärenz aller Mechanismen der Zusammenarbeit auf dem Gebiet der Strafverfolgung mit den Vorschriften der Richtlinie zum Datenschutz bei der Strafverfolgung ist ein Leitprinzip, das die Kommission auch berücksichtigt, wenn sie neue Übereinkünfte für die Übermittlung personenbezogener Daten durch Europol an Drittländer oder internationale Organisationen aushandelt. Seit dem Inkrafttreten der aktuellen Europol-Verordnung im Jahr 2017 ist Artikel 218 AEUV die Rechtsgrundlage für solche internationalen Übereinkünfte zur Sicherstellung angemessener Garantien. 2018 und 2019 erteilte der Rat der Kommission neun Mandate für Verhandlungen mit Drittländern im Namen der Union. Die Kommission wurde außerdem ermächtigt, Verhandlungen mit Interpol über ein Kooperationsabkommen zum Austausch von Daten mit verschiedenen Einrichtungen und sonstigen Stellen der EU aufzunehmen. In all diesen Fällen hat der Rat Verhandlungsrichtlinien für die Kommission verabschiedet, um dafür zu sorgen, dass die erforderlichen Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und -freiheiten natürlicher Personen berücksichtigt werden. Auf dieser Grundlage hat die Kommission bereits die Verhandlungen mit Neuseeland abgeschlossen und am 30. Juni 2022 ein entsprechendes Kooperationsabkommen

---

über die Anwendung einiger Bestimmungen des Übereinkommens vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union und das dazugehörige Protokoll von 2001).

[156] Für weitere Informationen zu den bestehenden Abkommen von Europol siehe die Europol-Website unter https://www.europol.europa.eu/partners-collaboration/agreements.

[157] Siehe Artikel 25 Absatz 4 der 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).

[158] Konsolidierte Fassung des Vertrags über die Europäische Union (ABl. C 202 vom 7.6.2016), verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02016M/TXT-20200301.

[159] Erwägungsgrund 35 der Europol-Verordnung.

unterzeichnet. Darüber hinaus wurden auch Fortschritte bei den Verhandlungen mit Israel erzielt. Bezüglich der Türkei befinden sich die Verhandlungen in einem fortgeschrittenen Stadium, können jedoch nicht abgeschlossen werden, solange die Türkei nicht die notwendigen Reformen in ihrer Datenschutzgesetzgebung verabschiedet. Ähnliche Ermächtigungen wurden im März 2021 erteilt, um Kooperationsabkommen zur Ermöglichung des Datenaustauschs zwischen Eurojust und 13 Drittländern auszuhandeln.

Zweitens führt die Kommission die erste gemeinsame Überprüfung des Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten (im Folgenden „Rahmenabkommen“) durch. Das im Februar 2017 in Kraft getretene Rahmenabkommen enthält eine Reihe umfassender und harmonisierter Datenschutzvorschriften, die für jeden transatlantischen Austausch zwischen zuständigen Behörden gelten. Es ergänzt die bestehenden Abkommen zwischen den Strafverfolgungsbehörden der EU und der USA sowie der EU-Mitgliedstaaten und der USA, legt einen Standard für ein hohes Schutzniveau mit Blick auf zukünftige Abkommen in diesem Bereich fest und stärkt die Zusammenarbeit auf dem Gebiet der Strafverfolgung durch die Erleichterung des Informationsaustauschs. Mit der gemeinsamen Überprüfung soll die wirksame Umsetzung des Rahmenabkommens beurteilt werden, insbesondere bezüglich der Bestimmungen zu Weiterleitungen, Rechten von Einzelpersonen und Rechtsbehelfen. Der Zeitrahmen für die gemeinsame Überprüfung wurde durch die Beeinträchtigungen im Zusammenhang mit der COVID-19-Pandemie sowie die parallelen Verhandlungen über das Zweite Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität[160] beeinflusst. Die Kommission erwartet, dass die gemeinsame Überprüfung im zweiten Halbjahr 2022 abgeschlossen wird.

Als erstes bilaterales internationales Abkommen mit einem umfassenden Katalog von Rechten und Pflichten auf dem Gebiet des Datenschutzes eignet sich das Rahmenabkommen als Vorbild für die Aushandlung ähnlicher Rahmenabkommen mit wichtigen Partnern im Bereich der Strafverfolgung.[161] Dabei berücksichtigt die Kommission auch relevante Entwicklungen, darunter die EDSA-Leitlinien, die Rechtsprechung des EuGH und die Ergebnisse internationaler Verhandlungen zu Datenschutzgarantien in diesem Bereich (beispielsweise das Zweite Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität oder das Europol-Abkommen mit Neuseeland[162]).

---

[160] Die Kommission im Namen der Europäischen Union und die Vereinigten Staaten waren maßgeblich an diesen Verhandlungen beteiligt, einschließlich in der speziellen Untergruppe zum Datenschutz (dieser war eines der am eingehendsten diskutierten Themen).

[161] Siehe die Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Austausch und Schutz personenbezogener Daten in einer globalisierten Welt“ (COM(2017) 7 final, S. 15–16).

[162] Abkommen zwischen der Europäischen Union einerseits und Neuseeland andererseits über den Austausch personenbezogener Daten zwischen der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet

Drittens hat die Kommission festgestellt, dass das Abkommen zwischen der Europäischen Union und Japan über die Rechtshilfe in Strafsachen[163] einen EU-Rechtsakt zur Regelung der Datenverarbeitung (Datenübermittlung) zum Zwecke der Strafverfolgung darstellt, der geändert werden muss, um geeignete Datenschutzgarantien im Einklang mit der Richtlinie zum Datenschutz bei der Strafverfolgung sicherzustellen. Nach der Annahme eines Beschlusses[164] über die Ermächtigung zur Aufnahme von Verhandlungen über die Änderung des Abkommens zwischen der Europäischen Union und Japan über die Rechtshilfe in Strafsachen durch den Rat setzt die Kommission ihre Kontakte mit den japanischen Behörden fort, um so rasch wie möglich mit den Verhandlungen zu beginnen.

Ferner stützt man sich mittlerweile auch zunehmend auf andere Formen der Zusammenarbeit, die an die spezifischen Herausforderungen und Bedürfnisse strafrechtlicher Ermittlungen in der heutigen digitalen Wirtschaft angepasst sind. Hierbei geht es hauptsächlich um eine verstärkte Zusammenarbeit im Bereich der Cyberkriminalität und für die Erhebung von Beweismitteln in elektronischer Form in Bezug auf Straftaten. Dies umfasst die direkte Zusammenarbeit mit privaten Akteuren für den Zugang zu elektronischen Beweismitteln.

Die Kommission hat sich auch mit den internationalen Partnern darum bemüht, sicherzustellen, dass diese anderen (wichtigen) Formen der Zusammenarbeit auf der Grundlage geeigneter Datenschutzgarantien erfolgen können.

Erstens vertrat die Kommission die EU bei den Verhandlungen[165] im Rahmen des Europarats über das Zweite Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität[166]. Das Protokoll, das am 17. November 2021 vom Ministerkomitee des Europarats angenommen wurde, enthält starke Garantien für den Schutz der Grundrechte, darunter einen Artikel[167] mit detaillierten Bestimmungen zum Schutz der nach dem Protokoll übermittelten personenbezogenen Daten. Diese Bestimmungen umfassen alle wesentlichen Grundsätze, Rechte

---

der Strafverfolgung (Europol) und den für die Bekämpfung von schwerer Kriminalität und Terrorismus zuständigen neuseeländischen Behörden.

[163] Abkommen zwischen der Europäischen Union und Japan über die Rechtshilfe in Strafsachen (ABl. L 39 vom 12.2.2010, S. 20). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A22010A0212%2801%29.

[164] Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen mit Japan über die Änderung des Abkommens zwischen der Europäischen Union und Japan über die Rechtshilfe in Strafsachen (Dokument LT 223/21).

[165] Zuvor hatte der Rat der Europäischen Union am 6. Juni 2019 ein entsprechendes Mandat angenommen. Das Mandat ist verfügbar unter https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.

[166] Das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Verstärkung der Zusammenarbeit und der Weitergabe von elektronischem Beweismaterial wurde am 17. November 2021 vom Ministerkomitee des Europarates angenommen. Es wurde zwischen September 2017 und Mai 2021 vom Ausschuss des Übereinkommens über Computerkriminalität (T-CY) ausgearbeitet. Der Wortlaut des Protokolls (beglaubigte Abschrift) ist verfügbar unter https://rm.coe.int/1680a4b2e1. Der erläuternde Bericht zum Protokoll ist zudem verfügbar unter https://rm.coe.int/1680a49c9d.

[167] Siehe Artikel 14 des Zusatzprotokolls sowie die Absätze 220–287 des erläuternden Berichts.

und Pflichten auf dem Gebiet des Datenschutzes, die im EU-Recht anerkannt sind. Ergänzt werden sie durch eine Aufsichtsbestimmung und die Möglichkeit, Datenübermittlungen im Falle eines systematischen oder schwerwiegenden Verstoßes gegen die im Protokoll enthaltenen Garantien auszusetzen, etwa beim Fehlen wirksamer Rechtsbehelfe. Durch diese Bestimmungen bietet das Protokoll geeignete Garantien im Einklang mit den Anforderungen von Artikel 37 Absatz 1 Buchstabe a der Richtlinie zum Datenschutz bei der Strafverfolgung.[168] Dies ist angesichts der vielfältigen Parteien des Budapester Übereinkommens, das derzeit 66 Vertragsstaaten mit unterschiedlichen rechtlichen Hintergründen und Traditionen hat, eine bedeutende Errungenschaft. Die zuständigen Behörden der Mitgliedstaaten können dadurch von einer wirksamen grenzüberschreitenden Zusammenarbeit bei der Bekämpfung von Cyberkriminalität profitieren, während gleichzeitig sichergestellt wird, dass die Werte der EU gemäß der Charta der Grundrechte der Europäischen Union, den EU-Verträgen und dem EU-Sekundärrecht geachtet werden. Aufgrund der Vielzahl von Vertragsparteien des Budapester Übereinkommens, wozu derzeit Länder aus aller Welt gehören, wird das Protokoll auch dazu beitragen, hohe Datenschutzstandards für die Datenverarbeitung im Bereich der Strafverfolgung auf globaler Ebene zu fördern. Das Protokoll wurde am 12. Mai 2022 zur Unterzeichnung aufgelegt, wobei es bereits von insgesamt 22 Vertragsparteien des Budapester Übereinkommens (darunter 13 Mitgliedstaaten der EU) gezeichnet wurde.

Zweitens hat die Kommission Verhandlungen über ein bilaterales Abkommen mit den Vereinigten Staaten über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen aufgenommen.[169] Dieses Abkommen soll sich auf elektronische Beweismittel in Form von sowohl nicht personenbezogenen als auch personenbezogenen Daten beziehen, einschließlich Verkehrs- und Inhaltsdaten. Wichtig ist, dass die Verhandlungen auch darauf abzielen, zusätzliche Datenschutzgarantien zur Ergänzung der Garantien im Rahmenabkommen einzubeziehen, wobei insbesondere die Sensibilität der betreffenden Datenkategorien sowie die Anforderungen für die direkte Übermittlung elektronischer Beweismittel durch Dienstleister zu berücksichtigen sind. Der Fortschritt bei

[168] In seiner Stellungnahme 1/2022 vom 20. Januar 2022 zu zwei Vorschlägen für Beschlüsse des Rates zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu unterzeichnen und zu ratifizieren, „nimmt der EDSB die zahlreichen Garantien, die in das Protokoll aufgenommen wurden, positiv zur Kenntnis“.

[169] Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen mit dem Ziel des Abschlusses eines Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen. Das Mandat ist unter folgendem Link abrufbar: https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/de/pdf.

diesen Verhandlungen wird weitgehend vom Fortschritt beim laufenden Gesetzgebungsverfahren zum Paket der EU über elektronische Beweismittel[170] abhängen.

Diese verschiedenen Initiativen der Kommission zur Entwicklung internationaler Instrumente, mit denen die Zusammenarbeit auf dem Gebiet der Strafverfolgung mit internationalen Partnern erleichtert wird, während gleichzeitig geeignete Datenschutzgarantien sichergestellt werden, wurden durch die Arbeit des EDSA und des EDSB unterstützt. Vorgelegt wurden im Rahmen dieser Arbeit unter anderem die Stellungnahme des EDSA zum Entwurf des Zweiten Zusatzprotokolls zum Budapester Übereinkommen[171] und die Stellungnahmen des EDSB zu den Entwürfen von Verhandlungsmandaten für internationale Übereinkünfte nach Artikel 218 AEUV, durch die Europol und Eurojust personenbezogene Daten mit Drittländern oder internationalen Organisationen austauschen könnten.[172] Der EDSA gab ferner eine Erklärung ab, in der er die Mitgliedstaaten bat, ihre internationalen Übereinkünfte, die internationale Übermittlungen personenbezogener Daten beinhalten, zu bewerten und erforderlichenfalls zu überprüfen.[173] Diese Erklärung betrifft Übereinkünfte (auch im Bereich der Strafverfolgung), die vor dem 6. Mai 2016 geschlossen wurden, wobei die Mitgliedstaaten ermitteln sollen, ob eine weitere Angleichung an die Rechtsvorschriften und die Rechtsprechung der EU im Bereich des Datenschutzes erforderlich ist.

Erlaubt sind nach Artikel 37 der Richtlinie zum Datenschutz bei der Strafverfolgung auch grenzüberschreitende Datenübermittlungen auf der Grundlage einer Selbstbeurteilung einer zuständigen Behörde, ob ein Drittland (oder eine internationale Organisation) über geeignete Datenschutzgarantien verfügt. In diesen Fällen muss die Behörde die Übermittlung dokumentieren (einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über die empfangende Behörde, Begründung der Übermittlung und übermittelter personenbezogener Daten) und die Dokumentation der Aufsichtsbehörde auf Anforderung zur Verfügung stellen

---

[170] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM(2018) 225 final) und Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren (COM(2018) 226 final).

[171] EDSA, Stellungnahme 02/2021 zum neuen Entwurf von Bestimmungen des Zweiten Zusatzprotokolls zum Übereinkommen des Europarats über Computerkriminalität (Budapester Übereinkommen), angenommen am 2. Februar 2021, verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_de.

[172] EDSB, Stellungnahme 4/2021 zum Vorschlag zur Änderung der Europol-Verordnung, angenommen am 8. März 2021, verfügbar unter https://edps.europa.eu/data-protection/our-work/publications/stellungnahmen-des-edsb/edps-opinion-proposal-amendment-0_de.

[173] EDSA, Erklärung 04/2021 zu internationalen Übereinkünften, die Datenübermittlungen einschließen, angenommen am 13. April 2021. Die Erklärung ist abrufbar unter https://edpb.europa.eu/system/files/2022-05/edpb_statement042021_international_agreements_including_transfers_de_0.pdf.

(Artikel 37 Absatz 3 der Richtlinie). Die Rückmeldungen der Mitgliedstaaten[174] zeigen, dass dieses Instrument selten genutzt wurde.

Damit die Mitgliedstaaten den Werkzeugkasten der Richtlinie zum Datenschutz bei der Strafverfolgung in Bezug auf Datenübermittlungen uneingeschränkt nutzen können, ist es wichtig, dass der EDSA seine laufenden Arbeiten zu den verschiedenen Übermittlungsmechanismen intensiviert. Unter anderem sollte er Leitlinien zu den Mechanismen nach Artikel 37 Absatz 1 der Richtlinie erstellen, insbesondere zu den Datenübermittlungen auf der Grundlage von Selbstbeurteilungen zuständiger Behörden. Der Rat hat ebenfalls betont, dass dies notwendig ist.[175]

3.5.3 Anwendung von Ausnahmen

Die sogenannten „Ausnahmen" schließlich bieten eine wichtige Grundlage für Datenübermittlungen unter bestimmten Bedingungen gemäß Artikel 38 der Richtlinie zum Datenschutz bei der Strafverfolgung. Diese Bedingungen sorgen für ein ausgewogenes Verhältnis zwischen Datenschutzbelangen und den operativen Erfordernissen der zuständigen Behörden. Insbesondere sind nach Artikel 38 Absatz 1 Übermittlungen und sogar Kategorien von Übermittlungen personenbezogener Daten zulässig, wenn sie zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit[176] oder im Einzelfall zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten[177] erforderlich sind. Anders als für Ausnahmen nach Artikel 49 der DSGVO gibt es für Ausnahmen nach Artikel 38 der Richtlinie zum Datenschutz bei der Strafverfolgung derzeit keine Leitlinien.

3.5.4 Wirksame polizeiliche und justizielle Zusammenarbeit über Grenzen hinweg

Die Richtlinie zum Datenschutz bei der Strafverfolgung ist zu einem internationalen Bezugspunkt für den Datenschutz im Kontext der Strafverfolgung geworden und hatte eine Katalysatorwirkung für die Einführung moderner Datenschutzvorschriften in diesem Bereich durch Länder auf der ganzen Welt. Dies ist eine äußerst positive Entwicklung, die neue Möglichkeiten für einen besseren Schutz natürlicher Personen in der EU bringt, wenn ihre Daten

---

[174] Siehe Bericht des Vorsitzes über den Austausch von Polizeidaten mit Drittländern – Erfahrungen bei der Anwendung von Artikel 37 der Richtlinie zum Datenschutz bei der Strafverfolgung. Der EDSA hat angekündigt, dass er die Schlussfolgerungen des Berichts des Vorsitzes zusammen mit weiteren Informationen und Bemerkungen der Mitgliedstaaten in seine Arbeiten zur Formulierung von Leitlinien zu Artikel 37 der Richtlinie einbeziehen wird. Siehe das Schreiben des Vorsitzenden des EDSA an die Ständige Vertretung der Bundesrepublik Deutschland bei der Europäischen Union vom 26. Februar 2021 (Dokument 13555/1/20).

[175] Siehe Standpunkt und Feststellungen des Rates zur Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung, Randnummer 20.

[176] Artikel 38 Absatz 1 Buchstabe c der Richtlinie zum Datenschutz bei der Strafverfolgung.

[177] Artikel 38 Absatz 1 Buchstabe d der Richtlinie zum Datenschutz bei der Strafverfolgung.

zum Zwecke der Strafverfolgung international übermittelt werden, wobei gleichzeitig der Datenverkehr zur Bekämpfung von Kriminalität erleichtert wird.

Allgemeiner muss sichergestellt werden, dass auf dem europäischen Markt tätige Unternehmen, die um eine direkte Zusammenarbeit zur Weitergabe von Daten zu Strafverfolgungszwecken ersucht werden, dies ohne Rechtskollisionen und unter uneingeschränkter Achtung der Grundrechte der EU tun können.[178] Um solche Datenübermittlungen zu verbessern, ist die Kommission entschlossen, mit ihren internationalen Partnern geeignete Rechtsrahmen auszuarbeiten, um Rechtskollisionen zu vermeiden und – insbesondere durch das Vorsehen der erforderlichen Datenschutzgarantien – wirksame Formen der Zusammenarbeit zu unterstützen und auf diese Weise zu einer wirksameren Kriminalitätsbekämpfung beizutragen.

Vor diesem Hintergrund hat sich die Kommission auf bilateraler, regionaler und multilateraler Ebene darum bemüht, die internationale Angleichung bei den Datenschutzstandards für die Zusammenarbeit im Bereich der Strafverfolgung aktiv zu fördern. Im Rahmen ihrer Dialoge mit verschiedenen internationalen Partnerländern über laufende Reformen der Datenschutzgesetze haben die Kommissionsdienststellen auf unterschiedliche Art und Weise (z. B. durch Beiträge in öffentlichen Konsultationsverfahren, die Teilnahme an parlamentarischen Anhörungen sowie spezielle Sitzungen mit Regierungsvertretern und politischen Entscheidungsträgern) an der Ausarbeitung von Vorschriften über die Verarbeitung personenbezogener Daten durch zuständige Behörden mitgewirkt.

Auf regionaler und multilateraler Ebene fördert die Kommission beispielsweise Projekte für den Kapazitätsaufbau im Kontext der Umsetzung des Budapester Übereinkommens des Europarats über Computerkriminalität.[179] Zu diesen Projekten zählt das Programm GLACY+, mit dem die Kapazität der Staaten zur Anwendung der Rechtsvorschriften über Computerkriminalität gestärkt und ihre Fähigkeit zur wirksamen internationalen Zusammenarbeit im Einklang mit dem Budapester Übereinkommen und dessen Zusatzprotokollen verbessert werden soll. Dies umfasst auch die Entwicklung von Datenschutzgesetzen für die Datenverarbeitung in diesem Bereich. Mit dem Programm werden derzeit 17 prioritäre Länder und Schwerpunktländer in Afrika, dem asiatisch-pazifischen Raum, Lateinamerika und der Karibik unterstützt.

Die Kommission hat auch mit Ameripol, einer Organisation für polizeiliche Zusammenarbeit, an der 18 Länder Lateinamerikas beteiligt sind, zusammengearbeitet, um einen Datenschutzrahmen für den Informationsaustausch zwischen Ameripol und ihren Mitgliedstaaten zu erarbeiten. Diese Zusammenarbeit erfolgt im Rahmen von „EL PAcCTO: Support to AMERIPOL“ (EL PAcCTO: Unterstützung für Ameripol), einem Projekt, das darauf abzielt, die internationale

[178] Beispielsweise könnte das Zweite Zusatzprotokoll zum Budapester Übereinkommen als internationale Übereinkunft für die Zwecke von Artikel 48 der DSGVO erachtet werden.
[179] Siehe https://www.coe.int/en/web/cybercrime/glacyplus.

Zusammenarbeit zwischen den Polizei-, Justiz- und Strafverfolgungsbehörden der Partnerländer bei der Bekämpfung der organisierten Kriminalität zu verbessern.

Die Kommission setzt sich zudem für die modernisierte Konvention 108 (bekannt als Konvention 108+)[180] ein, die auch für Datenverarbeitungstätigkeiten zum Zwecke der Strafverfolgung gilt. Diese Konvention, der Nichtmitglieder des Europarats beitreten können, ist nicht nur wichtig, weil sie die einzige verbindliche multilaterale Übereinkunft über den Datenschutz darstellt, sondern auch, weil sie durch den Ausschuss für die Konvention ein Forum für den Austausch bewährter Verfahren und die Festlegung globaler Standards bietet.[181] Im Rahmen ihrer internationalen Strategie zum Datenverkehr ermutigt die Kommission Drittländer dazu, der Konvention 108+ beizutreten.

Schließlich fördert die Kommission eine größere Angleichung auf internationaler Ebene, indem sie unsere Erfahrung mit den Partnern in Bezug auf die Datenschutzaspekte der Zusammenarbeit im Bereich der Strafverfolgung teilt. Die „Datenschutzakademie“ der Kommission, ein Teil des Projekts „Internationale digitale Zusammenarbeit – Verbesserung des Datenschutzes und der Datenflüsse“, das durch das außenpolitische Instrument finanziert wird, ist ein wichtiges Hilfsmittel bei diesem Unterfangen. Die Akademie wurde eingerichtet, um den Austausch zwischen den Regulierungsbehörden aus europäischen Ländern und Drittländern zu fördern und die Zusammenarbeit vor Ort zu verbessern. Die Tätigkeiten der Akademie umfassen alle Aspekte der Überwachung des Datenschutzes, einschließlich im Bereich der Strafverfolgung.

4 DAS WEITERE VORGEHEN

Um für eine effiziente Sicherheitspolitik der EU zu sorgen, in der das Grundrecht auf Schutz personenbezogener Daten uneingeschränkt geachtet wird, wird die Kommission weiterhin kontrollieren, ob die Mitgliedstaaten die Richtlinie zum Datenschutz bei der Strafverfolgung richtig umsetzen, und die Anwendung ihrer Bestimmungen überwachen.

Die Richtlinie zum Datenschutz bei der Strafverfolgung trägt wesentlich zu einem harmonisierteren und höheren Schutzniveau für die Rechte natürlicher Personen und einem kohärenteren Rechtsrahmen für die zuständigen Behörden bei.

---

[180] Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, angenommen vom Ministerkomitee bei seiner 128. Sitzung in Helsingör am 18. Mai 2018. Die Konvention 108+ ist abrufbar unter https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[181] Siehe beispielsweise „Practical guide on the use of personal data in the police sector“ (Praktischer Leitfaden für die Verwendung personenbezogener Daten im Polizeiwesen), verfügbar unter https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

Die Richtlinie zum Datenschutz bei der Strafverfolgung ist insgesamt zufriedenstellend umgesetzt worden, jedoch wurde eine Reihe von Problemen festgestellt. Die Kommission hat bereits Vertragsverletzungsverfahren sowohl in Bezug auf die Nichtumsetzung der Richtlinie als auch die Nichtübereinstimmung nationaler Rechtsvorschriften mit der Richtlinie eingeleitet. Sie wird weiter auf eine vollständige und ordnungsgemäße Umsetzung hinwirken.

Durch die Richtlinie zum Datenschutz bei der Strafverfolgung wird das Bewusstsein und die Aufmerksamkeit der zuständigen nationalen Behörden für den Datenschutz gestärkt, auch was die Sicherheit der Verarbeitung betrifft.

Eine aktive Aufsicht durch die Datenschutzaufsichtsbehörden ist entscheidend, um sicherzustellen, dass die Ziele der Richtlinie zum Datenschutz bei der Strafverfolgung in der Praxis verwirklicht werden. Den Behörden müssen daher alle gemäß der Richtlinie erforderlichen Arten von Befugnissen übertragen sowie angemessene Ressourcen zur Verfügung gestellt werden.

Im jetzigen Stadium sollte der Fokus darauf liegen, das Potenzial der Richtlinie zum Datenschutz bei der Strafverfolgung vollständig auszuschöpfen. In diesem Zusammenhang und angesichts der begrenzten Erfahrung mit diesen neuen Vorschriften vertritt die Kommission die Auffassung, dass es zu früh ist, eine Überarbeitung der Richtlinie in Erwägung zu ziehen.

Die Kommission wird im Hinblick auf die für 2026 vorgesehene nächste Bewertung weiterhin aktiv mit allen relevanten Parteien zusammenarbeiten. Sie wird in der Zwischenzeit weiter auf die Sicherstellung der Kohärenz mit anderen EU-Rechtsvorschriften hinwirken, die für die Verarbeitung personenbezogener Daten zum Zwecke der Strafverfolgung von Bedeutung sind.

Rechtsrahmen

Die Kommission wird

- die Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung durch die Mitgliedstaaten weiterhin bewerten und erforderlichenfalls geeignete Maßnahmen ergreifen (einschließlich der Einleitung von Vertragsverletzungsverfahren),
- sich bilateral mit den Mitgliedstaaten austauschen und
- sicherstellen, dass zukünftige Legislativvorschläge mit der Richtlinie zum Datenschutz bei der Strafverfolgung im Einklang stehen.

Die Mitgliedstaaten sollten

- stellen die vollständige und ordnungsgemäße Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung auf nationaler Ebene sicher, unter anderem, indem sie die erforderlichen Anforderungen der Richtlinie näher ausführen, wenn die nationalen Datenschutzgesetze zur Umsetzung der Richtlinie nicht präzise genug sind.

Aufsicht durch die Datenschutzaufsichtsbehörden

Die Mitgliedstaaten sollten

- stellen den Datenschutzaufsichtsbehörden ausreichende Ressourcen zur Erfüllung ihrer Aufgaben im Zusammenhang mit der Durchsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung zur Verfügung,
- stellen sicher, dass die Datenschutzaufsichtsbehörden alle Arten von Befugnissen ausüben können, die in der Richtlinie dargelegt sind,
- konsultieren ihre Datenschutzaufsichtsbehörden systematisch zu Entwürfen von Rechtsvorschriften und administrativen Maßnahmen mit allgemeiner Geltung in Bezug auf den Schutz personenbezogener Daten und tragen deren Stellungnahmen gebührend Rechnung (insbesondere im Fall neuer Technologien).

Die Datenschutzaufsichtsbehörden werden ersucht,

- ihre Untersuchungsbefugnisse voll auszuschöpfen, unter anderem, indem sie Prüfungen aus eigener Initiative vornehmen,
- spezifische statistische Daten bezüglich ihrer Aufsichtstätigkeiten im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung zu erheben,
- von den Instrumenten zur gegenseitigen Amtshilfe Gebrauch zu machen und praktische Maßnahmen zu entwickeln, um Hilfeersuchen zu erleichtern, einschließlich durch die geplanten EDSA-Leitlinien.

Der EDSA wird ersucht,

- den unterstützenden EDSA-Expertenpool[182] für Aufgaben im Zusammenhang mit der Richtlinie zum Datenschutz bei der Strafverfolgung zu erweitern.

Unterstützung der zuständigen Behörden

Die Kommission wird

- die Gespräche und den Erfahrungsaustausch zwischen den Mitgliedstaaten und der Kommission in der Expertengruppe mit Vertretern der Mitgliedstaaten für die Richtlinie zum Datenschutz bei der Strafverfolgung erleichtern und
- den Meinungsaustausch zwischen den Datenschutzbeauftragten über das Netz der Datenschutzbeauftragten fördern.

Die Mitgliedstaaten werden ersucht,

- sich weiterhin um Schulungen für die zuständigen Behörden zu den Datenschutzanforderungen zu bemühen, einschließlich im Zusammenhang mit neuen Technologien.

Der EDSA und die Datenschutzaufsichtsbehörden werden ersucht,

[182] EDPB Document on Terms of Reference of the EDPB Support Pool of Experts (Dokument des EDSA zum Aufgabenbereich des unterstützenden EDSA-Expertenpools), angenommen am 15. Dezember 2020.

- ihre Anstrengungen zu intensivieren, um einschlägige Leitlinien zu verabschieden (z. B. zur Rolle der Einwilligung im Kontext der Verarbeitung personenbezogener Daten zum Zwecke der Strafverfolgung und zu den Rechten betroffener Personen, einschließlich möglicher Einschränkungen dieser Rechte), entweder durch die Verabschiedung neuer eigenständiger Leitlinien oder durch die Ergänzung der bereits zur DSGVO verabschiedeten Leitlinien.

Grenzüberschreitende Datenübermittlungen

Die Kommission beabsichtigt,

- mögliche neue Angemessenheitsbeschlüsse für wichtige internationale Partner aktiv zu fördern,
- neue Kooperationsabkommen zwischen Europol und Eurojust einerseits und Drittländern andererseits auszuhandeln, wobei sie sich erforderlichenfalls auch darum bemühen wird, bestehende Kooperationsabkommen von Europol neu zu verhandeln, um dafür zu sorgen, dass diese geeignete Datenschutzgarantien enthalten,
- mit Japan zu verhandeln, um das bestehende Abkommen zwischen der EU und Japan über die Rechtshilfe in Strafsachen zu ändern und so geeignete Datenschutzgarantien sicherzustellen,
- die Verhandlungen über ein bilaterales Abkommen mit den Vereinigten Staaten über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen voranzutreiben und abzuschließen, einschließlich durch die Ergänzung der Datenschutzgarantien des Rahmenabkommens zwischen der EU und den USA, um dem spezifischen Kontext der direkten Zusammenarbeit zwischen den Strafverfolgungsbehörden und Dienstleistern Rechnung zu tragen, und
- die Möglichkeit zu prüfen, mit wichtigen Strafverfolgungspartnern Datenschutzrahmenabkommen für die Datenverarbeitung auf dem Gebiet der Strafverfolgung abzuschließen, die auf dem Beispiel des Rahmenabkommens zwischen der EU und den USA aufbauen.

Der EDSA wird ersucht,

- Leitlinien zu verabschieden, um den Begriff „geeignete Garantien“ (Artikel 37 der Richtlinie zum Datenschutz bei der Strafverfolgung) und dessen Inhalt sowie die Anwendung von Ausnahmen (Artikel 38 der Richtlinie) näher zu erläutern.

Förderung der Angleichung und Entwicklung der internationalen Zusammenarbeit

Die Kommission wird

- ihre Zusammenarbeit mit internationalen Partnern ausweiten, um die Angleichung der Datenschutzvorschriften auf dem Gebiet der Strafverfolgung zu stärken, einschließlich durch die Förderung des Beitritts zur Konvention 108+, die die einzige verbindliche globale Übereinkunft über den Datenschutz darstellt, und

- die bilaterale, regionale und multilaterale Zusammenarbeit sowie Projekte für den Kapazitätsaufbau im Bereich des Datenschutzes und der polizeilichen Zusammenarbeit fördern. Dies umfasst Schulungen und den Austausch von Wissen und bewährten Verfahren über die Datenschutzakademie.

Die Mitgliedstaaten werden aufgefordert,

- das Zweite Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität rasch zu ratifizieren, sobald sie mit einem Beschluss des Rates dazu ermächtigt werden.