EUROPÄISCHE
KOMMISSION

Brüssel, den 25.7.2024
COM(2024) 357 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Zweiter Bericht zur Anwendung der Datenschutz-Grundverordnung (DSGVO)

1 EINLEITUNG

Der vorliegende Bericht ist der zweite Bericht der Kommission über die Anwendung der Datenschutz-Grundverordnung (DSGVO), der gemäß Artikel 97 DSGVO angenommen wurde. Der erste Bericht wurde am 24. Juni 2020 angenommen (im Folgenden „Bericht 2020“)[1].

Die DSGVO ist einer der Eckpfeiler des Ansatzes der EU für den digitalen Wandel. Ihre Grundsätze – eine faire, sichere und transparente Verarbeitung personenbezogener Daten, die sicherstellt, dass Einzelpersonen die Kontrolle behalten – liegen allen EU-Maßnahmen zugrunde, die die Verarbeitung personenbezogener Daten betreffen.

Seit dem Bericht 2020 hat die EU eine Reihe von Initiativen angenommen, mit denen die Einzelnen in den Mittelpunkt des digitalen Wandels gestellt werden sollen. Jede Initiative verfolgt ein besonderes Ziel, wie die Schaffung eines sichereren Online-Umfelds, eine gerechtere und wettbewerbsfähigere digitale Wirtschaft, die Erleichterung bahnbrechender Forschung, die Sicherstellung der Entwicklung einer sicheren und vertrauenswürdigen künstlichen Intelligenz (KI) und die Schaffung eines echten Binnenmarkts für Daten. Sind personenbezogene Daten betroffen, bauen diese Initiativen auf der DSGVO auf. Die DSGVO bietet zudem eine Grundlage für sektorspezifische Initiativen, die sich auf die Verarbeitung personenbezogener Daten auswirken, z. B. in den Bereichen Finanzdienstleistungen, Gesundheit, Beschäftigung, Mobilität und Strafverfolgung.

Zwischen den Interessenträgern, den Datenschutzbehörden und den Mitgliedstaaten besteht weitgehend Einigkeit darüber, dass die DSGVO trotz einiger Herausforderungen wichtige Ergebnisse für Einzelpersonen und Unternehmen gebracht hat. Der risikobasierte, technologieneutrale Ansatz bietet einen starken Schutz für betroffene Personen und angemessene Pflichten für Verantwortliche und Auftragsverarbeiter. Gleichzeitig sollten in einer Reihe von Bereichen weitere Fortschritte erzielt werden. In den kommenden Jahren sollte der Schwerpunkt insbesondere darauf liegen, die Bemühungen der Interessenträger – vor allem kleine und mittlere Unternehmen (KMU), kleine Marktteilnehmer, Forscher und Forschungseinrichtungen – zu unterstützen, klarere und umsetzbarere Leitlinien der Datenschutzbehörden bereitzustellen und eine einheitlichere Auslegung und Durchsetzung der DSGVO in der gesamten EU zu erreichen.

Gemäß Artikel 97 DSGVO sollte die Kommission insbesondere die Anwendung und Funktionsweise der internationalen Übermittlung personenbezogener Daten an Drittländer (d. h. Länder außerhalb der EU/des EWR) (Kapitel V DSGVO) sowie die Mechanismen für die Zusammenarbeit und Kohärenz zwischen den nationalen Datenschutzbehörden (Kapitel VII DSGVO) prüfen. Wie der Bericht 2020 enthält auch der vorliegende Bericht eine allgemeine Bewertung der Anwendung der DSGVO, die über diese beiden Elemente hinausgeht: Mehrere Maßnahmen werden ermittelt, die erforderlich sind, um die wirksame Anwendung der DSGVO in vorrangigen Schlüsselbereichen zu unterstützen.

In dem vorliegenden Bericht werden folgende Quellen berücksichtigt: i) der Standpunkt und die Feststellungen des Rates, die im Dezember 2023 angenommen wurden;[2] ii) Beiträge von Interessenträgern, die insbesondere im Rahmen der Multi-Stakeholder-

(1) Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung, 24.6.2020, COM(2020) 264 final.

(2) https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/de/pdf.

Gruppe zur DSGVO[3] und einer öffentlichen Konsultation[4] eingeholt wurden; und iii) Beiträge der Datenschutzbehörden (durch den Beitrag des Europäischen Datenschutzausschusses[5] (im Folgenden „Ausschuss“) und ein Bericht der Agentur der Europäischen Union für Grundrechte (FRA) auf der Grundlage von Befragungen einzelner Datenschutzbehörden[6] (im Folgenden „FRA-Bericht“). Der vorliegende Bericht stützt sich außerdem auf die laufende Überwachung der Anwendung der DSGVO durch die Kommission, einschließlich bilateraler Dialoge mit den Mitgliedstaaten über die Einhaltung der nationalen Rechtsvorschriften, eines aktiven Beitrags zur Arbeit des Ausschusses und enger Kontakte mit einem breiten Spektrum von Interessenträgern zur praktischen Anwendung der Verordnung.

2 DURCHSETZUNG DER DSGVO UND FUNKTIONSWEISE DER VERFAHREN DER ZUSAMMENARBEIT UND KOHÄRENZ

Das System der zentralen Anlaufstelle für die Durchsetzung der DSGVO zielt darauf ab, eine harmonisierte Auslegung und Durchsetzung durch unabhängige Datenschutzbehörden sicherzustellen. Es erfordert in Fällen grenzüberschreitender Verarbeitungen, die auf die betroffenen Personen in mehreren Mitgliedstaaten erhebliche Auswirkungen haben, die Zusammenarbeit zwischen den Datenschutzbehörden. Streitigkeiten zwischen Behörden werden vom Ausschuss im Rahmen des Kohärenzverfahrens der DSGVO beigelegt.

2.1 Effizientere Bearbeitung grenzüberschreitender Fälle: Vorschlag für Verfahrensregeln

Im Bericht 2020 wurde darauf hingewiesen, dass eine effizientere und einheitlichere Bearbeitung grenzüberschreitender Fälle in der gesamten EU erforderlich ist, insbesondere angesichts der großen Unterschiede bei den nationalen Verwaltungsverfahren und der Auslegung von Konzepten im Kooperationsmechanismus der DSGVO. Daher nahm die Kommission im Juli 2023 einen Vorschlag für eine Verordnung über Verfahrensregeln[7] an, der sich auch auf eine Liste von Themen, die der Ausschuss der Kommission im Oktober 2022[8] vorgelegt hat, sowie auf Beiträge von Interessenträgern[9] und Mitgliedstaaten[10] stützt. Der Vorschlag ergänzt die DSGVO, indem detaillierte Regeln für grenzüberschreitende Beschwerden, die Beteiligung des Beschwerdeführers, die Verfahrensrechte der von der Untersuchung betroffenen Parteien (Verantwortliche und Auftragsverarbeiter) und die Zusammenarbeit zwischen den Datenschutzbehörden

---

([3]) Eine Zusammenfassung der Beiträge der Multi-Stakeholder-Expertengruppe zur DSGVO ist abrufbar unter: Report from Multistakeholder Expert group on GDPR application - June 2024.pdf. Die Beiträge, die als Reaktion auf die öffentliche Konsultation und im Rahmen bilateraler Treffen mit Interessenträgern eingingen, entsprechen weitgehend den Ansichten der Mitglieder der Multi-Stakeholder-Expertengruppe zur DSGVO.

([4]) https://ec.europa.eu/info/law/better-regulation/.

([5]) Contribution of the EDPB to the evaluation of the GDPR under Article 97 | European Data Protection Board (europa.eu).

([6]) GDPR in practice – Experiences of data protection authorities | European Union Agency for Fundamental Rights (europa.eu).

([7]) Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679 (COM(2023) 348 final).

([8]) https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_de.

([9]) Im Rahmen der Multi-Stakeholder-Expertengruppe zur DSGVO und einer im Februar 2023 veröffentlichten Aufforderung zur Stellungnahme.

([10]) Insbesondere im Rahmen der Expertengruppe der Datenschutz-Grundverordnung der Mitgliedstaaten: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=de&do=groupDetail.groupDetail&groupID=3461.

festgelegt werden. Die Harmonisierung dieser Verfahrensaspekte würde den fristgerechten Abschluss von Untersuchungen und einen raschen Rechtsbehelf für Einzelpersonen unterstützen. Das Europäische Parlament und der Rat verhandeln derzeit über den Vorschlag.

2.2 Verstärkte Zusammenarbeit zwischen den Datenschutzbehörden und Anwendung des Kohärenzverfahrens

Die Zahl der grenzüberschreitenden Fälle ist in den letzten Jahren erheblich gestiegen. Die Datenschutzbehörden haben sich zunehmend bereit gezeigt, die in der DSGVO vorgesehenen Instrumente für die Zusammenarbeit zu nutzen. Alle Datenschutzbehörden

nutzten das Amtshilfeinstrument[11] sowie „informelle“ Ersuchen zur gegenseitigen Unterstützung auf freiwilliger Basis. Die Datenschutzbehörden befürworten informelle Ersuchen, die weder eine Frist noch eine strikte Beantwortungspflicht vorschreiben. Zwar hat der Ausschuss im Jahr 2021 Leitlinien für gemeinsame Maßnahmen[12] angenommen, jedoch haben die Behörden dieses Instrument[13] immer noch nicht in nennenswertem Umfang genutzt und führen Unterschiede bei den nationalen Verfahren und mangelnde Klarheit in Bezug auf das Verfahren als Hauptgründe für seine begrenzte Nutzung an.

Die DSGVO bietet den betroffenen Datenschutzbehörden die Möglichkeit, einen maßgeblichen und begründeten Einspruch zu erheben, wenn sie mit dem Entwurf eines Beschlusses der federführenden Datenschutzbehörde in einem grenzüberschreitenden Fall nicht einverstanden sind. Für den Fall, dass die Datenschutzbehörden keinen Konsens über einen maßgeblichen und begründeten Einspruch erzielen können, sieht die DSGVO eine Streitbeilegung durch den Ausschuss vor.[14] Am häufigsten wurden bei maßgeblichen und begründeten Beschwerden folgende Themen angesprochen: i) die Rechtsgrundlage der Verarbeitung; ii) Informations- und Transparenzpflichten; iii) die Meldung von Datenschutzverletzungen; iv) Rechte der betroffenen Personen; v) Ausnahmeregelungen für internationale Datenübermittlungen; vi) die Anwendung von Korrekturmaßnahmen; und vii) die Höhe einer Geldbuße.

Das Durchsetzungssystem der DSGVO beruht auf der Prämisse einer loyalen und wirksamen Zusammenarbeit zwischen den Datenschutzbehörden. Das Streitbeilegungsverfahren spielt zwar eine wichtige Rolle in dieser Durchsetzungsarchitektur, sollte jedoch in dem Geist eingesetzt werden, in dem es konzipiert wurde, nämlich unter gebührender Berücksichtigung der Aufteilung der Zuständigkeiten zwischen den Datenschutzbehörden, der Notwendigkeit, die Verfahrensrechte zu wahren, und des Interesses an einer zeitnahen Beilegung des Falls für die betroffenen Personen. Jedes Streitbeilegungsverfahren erfordert erhebliche Ressourcen der federführenden Behörde, der betroffenen Behörden und des Sekretariats des Ausschusses und verzögert die Einlegung eines Rechtsbehelfs für betroffene Personen.

Verstärkter Einsatz von Kooperationsinstrumenten durch Datenschutzbehörden

- Fast 2 400 Falleinträge wurden im Informationsaustauschsystem des Ausschusses registriert.[15]
- Die federführenden Datenschutzbehörden haben rund 1 500 Beschlussentwürfe[16] herausgegeben, von denen 990 zu endgültigen Beschlüssen führten, mit denen ein Verstoß gegen die DSGVO[17] festgestellt wurde.
- Die Datenschutzbehörden haben fast 1 000 „formelle“ Amtshilfeersuchen[18] und rund 12 300 „informelle“ Ersuchen[19] gestellt.
- Es wurden fünf gemeinsame Maßnahmen eingeleitet, an denen Datenschutzbehörden aus sieben Mitgliedstaaten beteiligt waren.
- Datenschutzbehörden aus 18 Mitgliedstaaten erhoben maßgebliche und begründete Beschwerden.[20]

(11) Artikel 61 DSGVO.
(12) internal_edpb_document_1_2021_on_art_62_joint_operations_en.pdf (europa.eu)
(15) Ab dem 3. November 2023 (Beitrag des Ausschusses).
(16) Nach Artikel 60 Absatz 3 DSGVO.
(17) Stand: 3. November 2023.

Das Kohärenzverfahren der DSGVO wird von den Datenschutzbehörden zunehmend genutzt. Es besteht aus drei Komponenten: i) Stellungnahmen des Ausschusses; ii) Streitbeilegung durch den Ausschuss; und iii) das Dringlichkeitsverfahren.[21]

Der Ausschuss befasst sich in seinen Stellungnahmen[22] zunehmend mit wichtigen Fragen allgemeiner Anwendung. Vor der Annahme dieser Stellungnahmen sollte der Ausschuss eine rechtzeitige und sinnvolle Konsultation sicherstellen. Die zur Streitbeilegung vorgelegten Fälle betrafen Fragen wie die Rechtsgrundlage für die Verarbeitung von Daten für verhaltensorientierte Werbung in sozialen Medien und die Online-Verarbeitung der Daten von Kindern. Die meisten nachfolgenden verbindlichen Beschlüsse wurden vor dem Gericht angefochten.

Transparenz im Entscheidungsprozess des Ausschusses ist ausschlaggebend, um gemäß der Charta der Grundrechte der Europäischen Union für die Achtung des Rechts auf eine gute Verwaltung zu sorgen. Das Dringlichkeitsverfahren der DSGVO ermöglicht es den Datenschutzbehörden, vom Verfahren der Zusammenarbeit und Kohärenz abzuweichen, um soweit erforderlich dringende Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen zu ergreifen. Abweichend vom normalen Verfahren der Zusammenarbeit nach der DSGVO sollen Instrumente wie das Dringlichkeitsverfahren nur unter außergewöhnlichen Umständen angewandt werden, wenn das normale Verfahren der Zusammenarbeit die Rechte und Freiheiten der betroffenen Personen nicht schützen kann.

Das Kohärenzverfahren

- Der Ausschuss hat 190 Kohärenzstellungnahmen angenommen.
- Im Rahmen der Streitbeilegung wurden neun verbindliche Entscheidungen erlassen.[23] Durch alle wurde die federführende Datenschutzbehörde angewiesen, ihren Beschlussentwurf zu ändern, und mehrere haben zu erheblichen Geldbußen geführt.
- Fünf Datenschutzbehörden haben im Dringlichkeitsverfahren vorläufige Maßnahmen erlassen (Deutschland, Finnland, Italien, Norwegen und Spanien).
- Zwei Datenschutzbehörden ersuchten den Ausschuss um einen verbindlichen Beschluss im Dringlichkeitsverfahren [24], und der Ausschussordnete in einem Fall endgültige Sofortmaßnahmen an.

(16) Nach Artikel 60 Absatz 3 DSGVO.
(17) Stand: 3. November 2023.
(18) Die irische Behörde stellte die meisten formellen Ersuchen (246), während bei den deutschen Behörden die meisten Ersuchen eingegangen sind (516).
(19) Die irische Behörde stellte die meisten informellen Ersuchen (4 245), gefolgt von den deutschen Behörden (2 036).
(20) Von den 289 von den Behörden gemeldeten maßgeblichen und begründeten Beschwerden wurden 101 (35 %) von den deutschen Behörden erhoben. Die Erfolgsquote bei der Erzielung eines Konsenses über maßgebliche und begründete Beschwerden reicht von 15 % (der von den deutschen Behörden eingelegten Beschwerden) bis zu 100 % (der Beschwerden der polnischen Behörde).
(21) Jeweils Artikel 64, 65 und 66 DSGVO.
(22) Stellungnahmen nach Artikel 64 Absatz 2 DSGVO.
(23) Nach Artikel 65 Absatz 1 Buchstabe a DSGVO.
(24) Gemäß Artikel 66 Absatz 2 DSGVO.

2.3 Strengere Durchsetzung

Die Durchsetzungstätigkeit der Datenschutzbehörden hat in den letzten Jahren erheblich zugenommen, unter anderem durch die Verhängung erheblicher Geldbußen in bahnbrechenden Fällen gegen multinationale Technologieriesen. So wurden beispielsweise Geldbußen verhängt für i) den Verstoß gegen die Rechtmäßigkeit und Sicherheit der Verarbeitung; ii) den Verstoß gegen die Verarbeitung besonderer Kategorien personenbezogener Daten; und iii) die Verletzung der Rechte des Einzelnen.[25] Dies hat Privatunternehmen dazu veranlasst, den Datenschutz ernst zu nehmen,[26] und dazu beigetragen, eine Compliance-Kultur in Organisationen zu verankern. Die Datenschutzbehörden erlassen Beschlüsse, mit denen in beschwerdebasierten und auf eigene Initiative eingeleiteten Fällen Verstöße gegen die DSGVO festgestellt werden. Zwar stehen sie nicht in allen Mitgliedstaaten zur Verfügung, doch haben viele Datenschutzbehörden wirksam von Verfahren zur gütlichen Beilegung von Beschwerdefällen Gebrauch gemacht, um solche Fälle rasch und zur Zufriedenheit des jeweiligen Beschwerdeführers zu regeln. Im Vorschlag für Verfahrensregeln wird die Möglichkeit einer gütlichen Beilegung von Beschwerden anerkannt.[27]

Die Datenschutzbehörden haben umfassend von ihren Abhilfebefugnissen Gebrauch gemacht, auch wenn die Zahl der auferlegten Abhilfemaßnahmen in den einzelnen Behörden sehr unterschiedlich ist. Neben Geldbußen wurden am häufigsten Warnungen, Verweise und Anordnungen zur Einhaltung der DSGVO eingesetzt. Verantwortliche und Auftragsverarbeiter fechten Beschlüsse, in denen Verstöße gegen die Datenschutz-Grundverordnung festgestellt werden, häufig vor nationalen Gerichten an, meist aus Verfahrensgründen.[28]

Strengere Durchsetzung

- Die Datenschutzbehörden haben über 20 000 Untersuchungen aus eigener Initiative eingeleitet.[29]
- Insgesamt gehen bei ihnen mehr als 100 000 Beschwerden pro Jahr ein.[30]
- Die durchschnittliche Zeit für die Bearbeitung von Beschwerden durch die Datenschutzbehörden (vom Eingang bis zum Abschluss des Falls) beträgt ein bis zwölf Monate und in fünf Mitgliedstaaten (Dänemark (1 Monat), Spanien (1,5 Monate), Estland (3 Monate), Griechenland (3 Monate) und Irland (3 Monate) drei Monate oder weniger.
- Über 20 000 Beschwerden wurden im Wege einer gütlichen Einigung beigelegt. Diese wird am häufigsten wird sie in Österreich, Ungarn, Luxemburg und Irland angewandt.
- Im Jahr 2022 erließen die Datenschutzbehörden in Deutschland die meisten Beschlüsse zur Verhängung einer Abhilfemaßnahme (3 261), gefolgt von Spanien

(25) Siehe 5.3.4 Beitrag des Ausschusses.
(26) FRA-Bericht, Seite 36.
(27) Vorschlag für Verfahrensregeln, Artikel 5.
(28) In Rumänien wurden alle 26 Beschlüsse, mit denen ein Verstoß festgestellt wurde, vor Gericht angefochten, während die Quote in den Niederlanden bei 23 % lag. In Belgien war die Erfolgsquote bei den Anfechtungen am höchsten (39 %).
(29) Die Datenschutzbehörden in Deutschland leiteten die meisten Untersuchungen aus eigener Initiative ein (7 647), gefolgt von Ungarn (3 332), Österreich (1 681) und Frankreich (1 571).
(30) Im Jahr 2022 gingen bei neun Datenschutzbehörden über 2 000 Beschwerden ein. Die meisten Beschwerden wurden von Deutschland (32 300), Italien (30 880), Spanien (15 128), den Niederlanden (13 133) und Frankreich (12 193) registriert, während die niedrigsten Zahlen in Liechtenstein (40), Island (140) und Kroatien (271) registriert wurden.

(774), Litauen (308) und Estland (332). Am wenigsten wurden Abhilfemaßnahmen in Liechtenstein (8), Tschechien (8), Island (10), den Niederlanden (17) und Luxemburg (22) auferlegt.

- Die Datenschutzbehörden haben über 6 680 Geldbußen in Höhe von rund 4,2 Mrd. EUR verhängt.[31] Die irische Behörde hat den höchsten Gesamtbetrag an Geldbußen (2,8 Mrd. EUR) verhängt, gefolgt von Luxemburg (746 Mio. EUR), Italien (197 Mio. EUR) und Frankreich (131 Mio. EUR). Liechtenstein (9 600 EUR), Estland (201 000 EUR) und Litauen (435 000 EUR) haben die niedrigsten Gesamtbeträge an Geldbußen verhängt.

Während die meisten Datenschutzbehörden ihre Ermittlungsinstrumente für angemessen halten, benötigen einige zusätzliche Instrumente auf nationaler Ebene, z. B. angemessene Sanktionen für den Fall, dass die Verantwortlichen nicht kooperieren oder die erforderlichen Informationen nicht bereitstellen.[32] Die Datenschutzbehörden halten unzureichende Ressourcen und fehlendes technisches und juristisches Fachwissen für den Hauptfaktor, der ihre Durchsetzungskapazität beeinträchtigt.[33]

2.4 Der Ausschuss

Der Ausschuss setzt sich aus dem Leiter einer Datenschutzbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten zusammen, während die Kommission ohne Stimmrecht teilnimmt. Der Ausschuss hat – unterstützt durch sein Sekretariat – die Aufgabe, die einheitliche Anwendung der DSGVO sicherzustellen.[34] Die meisten Datenschutzbehörden sind der Ansicht, dass der Ausschuss bei der Stärkung der Zusammenarbeit zwischen ihnen eine positive Rolle gespielt hat.[35] Viele Datenschutzbehörden stellen erhebliche Ressourcen für die Tätigkeiten des Ausschusses bereit, auch wenn kleinere Behörden darauf hinweisen, dass ihre Größe sie daran hindert, sich in vollem Umfang zu engagieren.[36] Einige Behörden sind der Ansicht, dass die Effizienz der Verfahren des Ausschusses verbessert werden sollte, insbesondere durch eine verringerte Zahl an Sitzungen und durch weniger Aufmerksamkeit für geringfügige Angelegenheiten.[37] Je nach Ergebnis der Verhandlungen über den Vorschlag für Verfahrensregeln der DSGVO, mit dem die Zahl der dem Ausschuss zur Streitbeilegung vorgelegten Fälle verringert werden soll, könnte es notwendig sein, darüber nachzudenken, ob der Ausschuss zusätzliche Ressourcen benötigt.

Bis November 2023 hatte der Ausschuss 35 Leitlinien angenommen. Die Interessenträger und die Datenschutzbehörden haben die Leitlinien zwar als nützlich erachtet, sind jedoch der Ansicht, dass sie schneller bereitgestellt und die Qualität verbessert werden sollte.[38] Die Interessenträger stellen fest, dass sie oft zu theoretisch und zu lang sind und den

(31) Mit Ausnahme Dänemarks, das keine Geldbußen vorsieht, verhängten alle Behörden Geldbußen. Die meisten Geldbußen wurden in Deutschland (2 106) und Spanien (1 596) verhängt. Die wenigsten Geldbußen wurden in Liechtenstein (3), Island (15) und Finnland (20) verhängt.
(32) FRA-Bericht, Seite 38.
(33) FRA-Bericht, S. 20 und 23. Siehe auch Standpunkt und Feststellungen des Rates, Rn. 17.
(34) Artikel 70 Absatz 1 DSGVO.
(35) FRA-Bericht, Seite 64.
(36) FRA-Bericht, Seite 67. Im Jahr 2023 stellten die deutschen Datenschutzbehörden die meisten Ressourcen für die Tätigkeiten des Ausschusses bereit (26 Vollzeitäquivalente (VZÄ)), gefolgt von Irland (16) und Frankreich (12) (Beitrag des Ausschusses).
(37) FRA-Bericht, Seite 67.
(38) FRA-Bericht, Seite 67; Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

risikobasierten Ansatz der DSGVO nicht widerspiegeln.[39] Die Datenschutzbehörden und der Ausschuss sollten präzise und praktische Leitlinien bereitstellen, die Antworten auf konkrete Probleme geben und ein ausgewogenes Verhältnis zwischen Datenschutz und anderen Grundrechten widerspiegeln. Die Leitlinien sollten auch für Personen ohne juristische Ausbildung, z. B. in KMU und Freiwilligenorganisationen, leicht verständlich sein.[40] Eine Möglichkeit, dies zu erreichen, besteht darin, die Ausarbeitung der Leitlinien transparenter zu gestalten und frühzeitig Konsultationen durchzuführen, um ein besseres Verständnis der Marktdynamik, der geschäftlichen Gepflogenheiten und der praktischen Anwendung der Leitlinien zu ermöglichen.[41] Es wird begrüßt, dass der Ausschuss im Rahmen seiner Strategie 2024–2027 sein Ziel hervorgehoben hat, praktische Leitlinien bereitzustellen, die für die jeweilige Zielgruppe zugänglich sind.[42]

Die Interessenträger betonen die Notwendigkeit zusätzlicher Leitlinien, insbesondere in Bezug auf Anonymisierung und Pseudonymisierung[43], berechtigte Interessen sowie wissenschaftliche Forschung.[44] Im Bericht 2020 forderte die Kommission den Ausschuss auf, Leitlinien für die wissenschaftliche Forschung anzunehmen, jedoch wurden die Leitlinien noch nicht angenommen. In Anerkennung der Bedeutung der wissenschaftlichen Forschung in der Gesellschaft, insbesondere für die Überwachung von Krankheiten, die Entwicklung von Behandlungen und die Förderung von Innovationen, ist es von entscheidender Bedeutung, dass die Datenschutzbehörden unverzüglich tätig werden, um diese Fragen zu klären.[45] Die Behörden würden auch von Leitlinien zur Bewältigung der besonderen Herausforderungen profitieren, mit denen sie konfrontiert sind.[46]

2.5 Datenschutzbehörden

2.5.1 Unabhängigkeit und Ressourcen

Die Unabhängigkeit der Datenschutzbehörden ist in der Charta der Grundrechte der Europäischen Union und im Vertrag über die Arbeitsweise der EU verankert. In der DSGVO sind Anforderungen zur Sicherstellung der „vollständigen Unabhängigkeit“ der Datenschutzbehörden festgelegt.[47] Im FRA-Bericht wurde festgestellt, dass die meisten Datenschutzbehörden unabhängig von Regierung, Parlament oder anderen öffentlichen Stellen tätig sind.[48]

Die Datenschutzbehörden benötigen angemessene personelle, technische und finanzielle Ressourcen, um ihre Aufgaben im Rahmen der DSGVO wirksam und unabhängig wahrnehmen zu können. Im Bericht 2020 stellte die Kommission fest, dass die Bereitstellung von Ressourcen für die Datenschutzbehörden immer noch nicht zufriedenstellend ist, und hat dieses Problem gegenüber den Mitgliedstaaten immer wieder zur Sprache gebracht. Seitdem hat sich die Lage verbessert.

Aufstockung der Ressourcen für Datenschutzbehörden[49]

(39) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
(40) Siehe auch Standpunkt und Feststellungen des Rates, Rn. 45.
(41) Siehe auch Standpunkt und Feststellungen des Rates, Rn. 34.
(42) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf.
(43) Siehe auch Standpunkt und Feststellungen des Rates, Rn. 31 Buchstabe d.
(44) Sie erfordern insbesondere Klarheit in Bezug auf die Bedeutung des Begriffs „wissenschaftliche Forschung“, die Rolle der Einwilligung in die Verarbeitung personenbezogener Daten zu Forschungszwecken, die einschlägige Rechtsgrundlage sowie die Rolle und Verantwortung der beteiligten Akteure.
(45) Siehe auch Standpunkt und Feststellungen des Rates, Rn. 31 Buchstabe b.
(46) Standpunkt und Feststellungen des Rates, Rn. 27 und 28.
(47) Artikel 52 DSGVO.
(48) FRA-Bericht, Seite 31.
(49) Siehe Abschnitt 4.4.1 Beitrag des Ausschusses, auch zu den absoluten Zahlen.

- Zwischen 2020 und 2024 profitierten alle Datenschutzbehörden bis auf zwei von einer Aufstockung des Personals, und in 14 Mitgliedstaaten lag der Anstieg bei über 25 %.
- Die Datenschutzbehörde in Irland verzeichnete den höchsten Personalzuwachs (79 %), gefolgt von Estland, Schweden (beide 57 %) und Bulgarien (56 %).
- In Tschechien war ein leichter Personalabbau zu verzeichnen (-1 %), während in Liechtenstein kein Anstieg und in Zypern (4 %) und Ungarn (8 %) ein leichter Anstieg zu verzeichnen war.
- Zwischen 2020 und 2024 wurden die Haushaltsmittel für alle bis auf eine Datenschutzbehörde aufgestockt, und in 13 Mitgliedstaaten lag der Anstieg bei über 50 %.
- Die stärkste Aufstockung des Haushalts verzeichnete die Datenschutzbehörde in Zypern (130 %), gefolgt von Österreich (107 %), Bulgarien (100 %) und Estland (97 %).
- Der Haushalt der griechischen Datenschutzbehörde ging um 15 % zurück, während die Haushaltsmittel für die Behörden in Liechtenstein (1 %), der Slowakei (6 %) und Tschechien (8 %) geringfügig aufgestockt wurden.

Zwar lassen diese Statistiken einen allgemeinen Aufwärtstrend bei der Bereitstellung von Ressourcen für die Datenschutzbehörden erkennen, allerdings sind die Behörden selbst der Ansicht, dass ihnen immer noch keine ausreichenden personellen Ressourcen zur Verfügung stehen.[50] Sie betonen, dass sehr spezifisches Fachwissen erforderlich ist, insbesondere in Bezug auf neue und aufkommende Technologien[51], dessen Fehlen sich auf die Quantität und Qualität ihrer Arbeit auswirkt, und dass es schwierig ist, mit dem Privatsektor um Personal zu konkurrieren. Die Datenschutzbehörden nennen unzureichendes juristisches Fachwissen und fehlende Sprachkenntnisse als Faktoren, die ihre Leistung beeinträchtigen. Niedrige Gehälter, die Unfähigkeit zur autonomen Personalauswahl und die hohe Arbeitsbelastung werden als Schlüsselfaktoren hervorgehoben, die die Fähigkeit der Behörden beeinträchtigen, Personal einzustellen und zu halten.[52] Die Datenschutzbehörden weisen ferner darauf hin, dass sie finanzielle Mittel benötigen, um ihre Verfahren zu modernisieren und zu digitalisieren sowie um technische Geräte zu erwerben.[53] Alle Datenschutzbehörden erfüllen Aufgaben, die über die Aufgaben hinausgehen, die ihnen durch die DSGVO[54] übertragen werden, z. B. als Aufsichtsbehörden für die Richtlinie zum Datenschutz bei der Strafverfolgung und die Datenschutzrichtlinie für die elektronische Kommunikation, und viele äußern Bedenken hinsichtlich zusätzlicher Zuständigkeiten im Rahmen neuer digitaler Rechtsvorschriften[55].

(50) Nur fünf Datenschutzbehörden sind der Ansicht, dass sie über angemessene personelle Ressourcen verfügen (Beitrag des Ausschusses, S. 33).
(51) FRA-Bericht, Seite 20. Einige Datenschutzbehörden vergeben bestimmte Aufgaben an externe Auftragnehmer, z. B. Bearbeitung von Beschwerden, rechtliche Analysen und forensische Analysen.
(52) FRA-Bericht, Seite 24.
(53) FRA-Bericht, Seite 22.
(54) Siehe Abschnitt 4.4.5 Beitrag des Ausschusses.
(55) Beitrag des Ausschusses, S. 32.

2.5.2 Schwierigkeiten bei der Bearbeitung einer hohen Zahl von Beschwerden

Mehrere Datenschutzbehörden weisen darauf hin, dass zu viele ihrer Ressourcen für die Bearbeitung einer großen Zahl von Beschwerden, von denen die meisten ihrer Ansicht nach geringfügig und unbegründet sind, aufgewandt werden, da die Bearbeitung jeder Beschwerde eine Verpflichtung nach der DSGVO, die einer gerichtlichen Überprüfung unterliegt, darstellt.[56] Dies bedeutet, dass die Datenschutzbehörden nicht genügend Mittel für andere Tätigkeiten bereitstellen können, wie Untersuchungen auf eigene Initiative, Kampagnen zur Sensibilisierung der Öffentlichkeit und die Zusammenarbeit mit den Verantwortlichen.[57] Als öffentliche Einrichtungen können die Datenschutzbehörden ihre Ressourcen nach eigenem Ermessen zuweisen, um jede ihrer (in Artikel 57 Absatz 1 DSGVO aufgeführten) Aufgaben im öffentlichen Interesse zu erfüllen. Viele Datenschutzbehörden haben Strategien zur Steigerung der Effizienz der Bearbeitung von Beschwerden angenommen, z. B. die Automatisierung[58], die Anwendung von Verfahren zur gütlichen Beilegung[59] und die „Gruppierung“ von Beschwerden, die sich auf ähnliche Themen beziehen[60].

2.5.3 Auslegung der DSGVO durch die nationalen Datenschutzbehörden

Ein zentrales Ziel der DSGVO bestand darin, den fragmentierten Datenschutzansatz, der in der vorherigen Datenschutzrichtlinie (Richtlinie 95/46/EG) bestand, zu beseitigen.[61] Die Datenschutzbehörden legen jedoch die wichtigsten Datenschutzkonzepte weiterhin unterschiedlich aus.[62] Die Interessenträger betrachten dies als Haupthindernis für die einheitliche Anwendung der DSGVO in der EU. Das Fortbestehen unterschiedlicher Auslegungen führt zu Rechtsunsicherheit und erhöht die Kosten für Unternehmen (z. B. durch die Anforderung unterschiedlicher Unterlagen für mehrere Mitgliedstaaten), beeinträchtigt den freien Verkehr personenbezogener Daten in der EU, behindert grenzüberschreitende Geschäfte sowie Forschung und Innovation bei dringenden gesellschaftlichen Herausforderungen.

Zu den spezifischen Fragen, die von den Interessenträgern angesprochen wurden, gehören i) die Tatsache, dass die Datenschutzbehörden in drei Mitgliedstaaten bei der Durchführung einer klinischen Prüfung unterschiedliche Auffassungen über die geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten vertreten; ii) die häufig unterschiedlichen Auffassungen darüber, ob es sich bei einer Einrichtung um einen Verantwortlichen oder einen Auftragsverarbeiter handelt; und (iii) die Fälle, in denen sich die Datenschutzbehörden nicht an die Leitlinien des Ausschusses halten oder auf nationaler Ebene Leitlinien veröffentlichen, die im Widerspruch zu denen des Ausschusses stehen.[63] Diese Probleme werden noch verschärft, wenn mehrere Datenschutzbehörden innerhalb eines Mitgliedstaats unterschiedliche Auslegungen vornehmen.

Einige Interessenträger sind ferner der Ansicht, dass bestimmte Datenschutzbehörden und der Ausschuss Auslegungen annehmen, die vom risikobasierten Ansatz der DSGVO abweichen, was eine Herausforderung für die Entwicklung der digitalen Wirtschaft[64] und

---

([56]) FRA-Bericht, Seite 48.
([57]) FRA-Bericht, Seite 45. Die Datenschutzbehörden halten Untersuchungen von Amts wegen für besonders wichtig, da den Beschwerdeführern viele Verstöße gegen die DSGVO möglicherweise nicht bekannt sind.
([58]) FRA-Bericht, Seite 8.
([59]) FRA-Bericht, Seite 39.
([60]) FRA-Bericht, Seite 41.
([61]) Erwägungsgrund 9 DSGVO.
([62]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
([63]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
([64]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

die Freiheit und Pluralität der Medien darstellt. Als Problembereiche nennen sie i) die Auslegung der Anonymisierung; ii) die Rechtsgrundlage des berechtigten Interesses und der Einwilligung;[65] und iii) die Ausnahmen vom Verbot der automatisierten Entscheidungsfindung im Einzelfall.[66] Es ist anzumerken, dass die Datenschutzbehörden und der Ausschuss die Aufgabe haben, sowohl den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten als auch den freien Verkehr personenbezogener Daten innerhalb der EU sicherzustellen. Wie in der DSGVO[67] festgestellt, muss das Recht auf Schutz der personenbezogenen Daten im Hinblick auf seine gesellschaftliche Funktion betrachtet und unter Wahrung des Grundsatzes der Verhältnismäßigkeit gegen andere Grundrechte abgewogen werden.

2.5.4 Zusammenarbeit mit Verantwortlichen und Auftragsverarbeitern

Die Interessenträger betonen, dass es vorteilhaft ist, die Möglichkeit zu haben, in einen konstruktiven Dialog mit den Datenschutzbehörden einzutreten, um sicherzustellen, dass sie die DSGVO von Anfang an einhalten, insbesondere in Bezug auf neu entstehende Technologien. Die Interessenträger stellen fest, dass einige Datenschutzbehörden aktiv mit den für die Verarbeitung Verantwortlichen zusammenarbeiten, während andere nur langsam reagieren, vage Antworten geben oder überhaupt nicht reagieren.[68]

3 UMSETZUNG DER DSGVO DURCH DIE MITGLIEDSTAATEN

3.1 Fragmentierung der nationalen Anwendung

Zwar ist die DSGVO als Verordnung unmittelbar anwendbar, doch verpflichtet sie die Mitgliedstaaten, in bestimmten Bereichen Rechtsvorschriften zu erlassen, und bietet ihnen die Möglichkeit, ihre Anwendung in einer begrenzten Anzahl von Bereichen[69] näher zu spezifizieren. Wenn die Mitgliedstaaten Rechtsvorschriften auf nationaler Ebene erlassen, müssen sie dies unter den in der DSGVO festgelegten Bedingungen und innerhalb der darin festgelegten Grenzen tun. Wie im Jahr 2020 berichten die Interessenträger über Schwierigkeiten aufgrund der Fragmentierung der nationalen Vorschriften, bei denen die Mitgliedstaaten die Möglichkeit haben, die DSGVO zu präzisieren, insbesondere in Bezug auf

- das Mindestalter für die Einwilligung eines Kindes in Bezug auf das Angebot von Diensten der Informationsgesellschaft für dieses Kind;[70]
- die Einführung weiterer Bedingungen für die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten durch die Mitgliedstaaten;[71]
- die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten[72], die in bestimmten regulierten Sektoren Schwierigkeiten bereitet.

Gleichzeitig berichten viele Interessenträger, dass Probleme der Fragmentierung hauptsächlich auf unterschiedliche Auslegungen der DSGVO durch die Datenschutzbehörden und nicht auf die Verwendung fakultativer Spezifikationsklauseln durch die Mitgliedstaaten zurückzuführen sind.

([65]) Jeweils Artikel 6 Absatz 1 Buchstabe f und Artikel 6 Absatz 1 Buchstabe a DSGVO.
([66]) Artikel 22 Absatz 2 DSGVO.
([67]) Erwägungsgrund 4.
([68]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
([69]) z. B. das Mindestalter für die Einwilligung des Kindes in Bezug auf Dienste der Informationsgesellschaft (Artikel 8 Absatz 1 DSGVO).
([70]) Artikel 8 Absatz 1 DSGVO.
([71]) Eine in Artikel 9 Absatz 4 DSGVO vorgesehene Möglichkeit.
([72]) Artikel 10 DSGVO.

Die Mitgliedstaaten sind der Auffassung, dass ein begrenztes Maß an Fragmentierung unter Umständen zulässig ist und die in der DSGVO vorgesehenen Spezifikationsklauseln weiterhin von Vorteil sind, insbesondere für die Verarbeitung durch Behörden.[73] Gemäß der DSGVO müssen die Mitgliedstaaten ihre nationale Datenschutzbehörde bei der Ausarbeitung von Rechtsvorschriften über die Verarbeitung personenbezogener Daten konsultieren.[74] Im FRA-Bericht wurde festgestellt, dass einige Regierungen für diese Behörden sehr knappe Fristen setzen und sie in einigen Fällen überhaupt nicht konsultieren.[75]

3.2 Überwachung durch die Kommission

Die Kommission überwacht, wie die DSGVO fortlaufend umgesetzt wird. Die Kommission hat Vertragsverletzungsverfahren gegen Mitgliedstaaten eingeleitet, z. B. in Bezug auf die Unabhängigkeit der Datenschutzbehörden (u. a. frei von externer Einflussnahme und die Verfügbarkeit eines Rechtsbehelfs im Falle einer Entlassung)[76] und das Recht betroffener Personen auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die Datenschutzbehörde eine Beschwerde nicht bearbeitet[77]. Im Rahmen ihrer Überwachung fordert die Kommission die Datenschutzbehörden ferner auf, auf streng vertraulicher Basis regelmäßig Informationen[78] über laufende große grenzüberschreitende Fälle bereitzustellen, insbesondere über große Technologieunternehmen.

Die Kommission kommuniziert regelmäßig mit den Mitgliedstaaten über die Umsetzung der DSGVO. Wie im Bericht 2020 dargelegt, nutzte die Kommission weiterhin die Expertengruppe der Mitgliedstaaten zur DSGVO[79], um Diskussionen und den Erfahrungsaustausch über die wirksame Umsetzung der DSGVO zu erleichtern. Die Expertengruppe hat spezifische Diskussionen über folgende Themen geführt: i) die Aufsicht über Gerichte, die im Rahmen ihrer justiziellen Tätigkeit handeln (Artikel 55 DSGVO; Artikel 8 der Charta); ii) die Vereinbarkeit des Rechts auf Datenschutz mit dem Recht auf freie Meinungsäußerung (Artikel 85 DSGVO); und iii) das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde (Artikel 78 DSGVO). Im Anschluss an diese Beratungen hat die Kommission einen Überblick über die bei der Umsetzung dieser Bestimmungen in den Mitgliedstaaten verfolgten Ansätze erstellt.[80] Die Kommission nutzte diese Gruppe auch bei der Ausarbeitung des Vorschlags über Verfahrensregeln für einen Gedankenaustausch mit den Mitgliedstaaten.

Im Rahmen der Schengen-Evaluierungen, die von den Mitgliedstaaten und der Kommission gemeinsam durchgeführt werden, wird auch die Übereinstimmung der nationalen Rechtsvorschriften und Verfahren mit den im EU-Rechtsbestand für den Schengen-Raum festgelegten Datenschutzvorschriften beurteilt. Jährlich werden mindestens fünf Datenschutzbewertungen vor Ort durchgeführt, wobei der Schwerpunkt derzeit auf IT-Großsystemen und dem Schengener Informationssystem, dem Visa-

---

([73]) Standpunkt und Feststellungen des Rates, Rn. 30.
([74]) Artikel 36 DSGVO.
([75]) FRA-Bericht, Seite 11.
([76]) Belgien (2021/4045) und Belgien (2022/2160).
([77]) Finnland (2022/4010) und Schweden (2022/2022).
([78]) Mit Informationen über den Fall, die Art der Untersuchung (auf eigene Initiative oder beschwerdebasiert), eine Zusammenfassung des Untersuchungsumfangs, die betroffenen Datenschutzbehörden, die wichtigsten eingeleiteten Verfahrensschritte und -daten, die Untersuchung oder sonstige ergriffene Maßnahmen und Termine.
([79]) https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=de&do=groupDetail.groupDetail&groupID=3461.
([80]) https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=de&meetingId=31754&fromExpertGroups=3461.

Informationssystem sowie auf der Aufsichtsfunktion der nationalen Datenschutzbehörden im Hinblick auf diese Systeme liegt.

Die Kommission leistet einen aktiven Beitrag zu der großen Zahl von Rechtssachen vor dem Gerichtshof (mit etwa 30 Vorabentscheidungen pro Jahr in den letzten Jahren), die eine zentrale Rolle bei der einheitlichen Auslegung der Schlüsselbegriffe der DSGVO spielen. In einer wachsenden Rechtsprechung des Gerichtshofs wurden mehrere Klarstellungen vorgenommen, z. B. zur Begriffsbestimmung personenbezogener Daten[81], zu besonderen Kategorien personenbezogener Daten[82], zum Verantwortlichen[83], zur Einwilligung[84], zum berechtigten Interesse[85], zum Auskunftsrecht[86], zum Recht auf Löschung[87], zum Recht auf Entschädigung[88], zur automatisierten Entscheidungsfindung im Einzelfall[89], zu Geldbußen[90], zum Datenschutzbeauftragten[91], zur Veröffentlichung personenbezogener Daten in Registern[92] und zur Anwendung der DSGVO auf die Tätigkeiten der Parlamente[93].

4 RECHTE BETROFFENER PERSONEN

Bewusstsein des Einzelnen für die DSGVO und die Datenschutzbehörden (Eurobarometer-Umfrage 549 von 2024 zu Justiz, Rechten und Werten)

- 72 % der Befragten in der gesamten EU gaben an, von der DSGVO gehört zu haben, darunter 40 %, die wissen, worum es sich dabei handelt.
- In 19 Mitgliedstaaten gaben mehr als 70 % der Befragten an, sich der DSGVO bewusst zu sein, wobei unter den Befragten in Schweden (92 %) das Bewusstsein am stärksten ausgeprägt war, gefolgt von den Niederlanden (88 %), Malta und Dänemark (84 %), während die Befragten in Bulgarien (59 %) sich der DSGVO am wenigsten bewusst waren, gefolgt von Litauen (63 %) und Frankreich (64 %).
- 68 % der Befragten in der EU geben an, von einer nationalen Behörde gehört zu haben, die für den Schutz ihrer Datenschutzrechte zuständig ist, wobei 24 % aller Befragten angeben, dass sie auch wissen, welche Behörde zuständig ist.
- In allen Mitgliedstaaten hat mindestens die Hälfte der Befragten von einer solchen nationalen Behörde gehört, wobei die höchsten Werte in den Niederlanden (82 %), Tschechien, Slowenien und Polen (alle 75 %) sowie Portugal (74 %) zu verzeichnen waren. Die Befragten in Österreich (56 %) und Spanien (58 %) sind sich dieser Behörde am wenigsten bewusst.

(81) C-319/22, ECLI:EU:C:2023:837.
(82) Rechtssachen C-184/20, ECLI:EU:C:2022:601; C-252/21, ECLI:EU:C:2023:537.
(83) Rechtssachen C-683/21, ECLI:EU:C:2023:949; C-604/22, ECLI:EU:C:2024:214; C-231/22, ECLI:EU:C:2024:7.
(84) C-61/19, ECLI:EU:C:2020:901.
(85) Rechtssachen C-597/19, ECLI:EU:C:2021:492; C-252/21, ECLI:EU:C:2023:537.
(86) Rechtssachen C-307/22, ECLI:EU:C:2023:811; C-154/21, ECLI:EU:C:2023:3.
(87) C-460/20, ECLI:EU:C:2022:962.
(88) Rechtssache C-300/21, ECLI:EU:C:2023:370; Rechtssache C-687/21, ECLI:EU:C:2024:72; Rechtssache C-667/21, ECLI:EU:C:2023:1022.
(89) Verbundene Rechtssachen C-26/22 und C-64/22, ECLI:EU:C:2023:958.
(90) Rechtssachen C-807/21, ECLI:EU:C:2023:950; C-683/21, ECLI:EU:C:2023:949.
(91) C-453/21, ECLI:EU:C:2023:79.
(92) Rechtssachen C-439/19, ECLI:EU:C:2021:504; C-184/20, ECLI:EU:C:2022:601.
(93) Rechtssachen C-33/22, ECLI:EU:C:2024:46; C-272/19, ECLI:EU:C:2020:535.

Einzelpersonen sind zunehmend mit ihren Rechten gemäß der DSGVO vertraut und üben sie aktiv aus.[94] Die Datenschutzbehörden stellen erhebliche Mittel bereit, um die Öffentlichkeit für die Datenschutzrechte und -pflichten zu sensibilisieren, z. B. durch Social-Media- und Fernsehkampagnen, Hotlines, Newsletter und Präsentationen in Bildungseinrichtungen.[95] Viele dieser Initiativen haben EU-Mittel erhalten.[96] Die Agentur für Grundrechte stellt fest, dass das Bewusstsein der breiten Öffentlichkeit für den Datenschutz zwar zugenommen hat, dass jedoch nach wie vor Wissen über den Datenschutz fehlt, was durch eine große Zahl von geringfügigen oder unbegründeten Beschwerden belegt wird.[97] Es wurden mehrere benutzerfreundliche digitale Instrumente entwickelt, um den betroffenen Personen die Ausübung ihrer Rechte zu erleichtern.[98] Gesetzgebungsakte, insbesondere der Daten-Governance-Rechtsakt[99], sollten dazu führen, dass zusätzliche Möglichkeiten geschaffen werden, damit die betroffenen Personen ihre Rechte künftig wahrnehmen können. Unternehmen weisen darauf hin, dass das Recht auf Löschung zunehmend genutzt wird, während dies beim Recht auf Berichtigung und Widerspruch nur selten der Fall ist.

4.1 Das Auskunftsrecht

Die Verantwortlichen berichten, dass das Auskunftsrecht (Artikel 15 DSGVO) das am häufigsten von den betroffenen Personen geltend gemachte Recht ist. Zwar hat der Ausschuss im Jahr 2022 Leitlinien zu diesem Recht angenommen, jedoch melden die Verantwortlichen weiterhin Herausforderungen, beispielsweise bei der Auslegung des Begriffs „unbegründete oder übermäßige Anträge“[100], bei der Beantwortung einer großen Zahl von Anträgen und bei der Bearbeitung von Anträgen, die zu Zwecken gestellt werden, die nicht mit dem Datenschutz zu tun haben, z. B. bei der Erhebung von Beweismitteln für Gerichtsverfahren[101]. Zivilgesellschaftliche Organisationen weisen darauf hin, dass die Antworten auf Zugangsanträge oft verzögert oder unvollständig sind, während die erhaltenen Daten nicht immer in einem lesbaren Format vorliegen.[102] Behörden verweisen auf Schwierigkeiten bei der Wechselwirkung zwischen dem Recht auf Zugang und den Vorschriften über den Zugang der Öffentlichkeit zu Dokumenten.[103] Es ist daher zu begrüßen, dass der Ausschuss im Februar 2024 eine gemeinsame Maßnahme im Rahmen des koordinierten Durchsetzungsrahmens in Bezug auf das Zugangsrecht eingeleitet hat.[104]

4.2 Das Recht auf Datenübertragbarkeit

Im Bericht 2020 verpflichtete sich die Kommission, im Einklang mit der Datenstrategie praktische Möglichkeiten zu sondieren, die verstärkte Nutzung des Rechts auf Datenübertragbarkeit (Artikel 20 DSGVO) durch Einzelpersonen zu erleichtern. Die Kommission hat seither eine Reihe von Initiativen verabschiedet, die dieses Recht

---

([94]) Standpunkt und Feststellungen des Rates, Rn. 13.
([95]) Beitrag des Ausschusses, Abschnitt 6.
([96]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en.
([97]) FRA-Bericht, Seiten 9 und 48.
([98]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
([99]) Artikel 10 der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) (ABl. L 152 vom 3.6.2022, S. 1).
([100]) Artikel 12 Absatz 5 DSGVO.
([101]) Der Gerichtshof hat jedoch klargestellt, dass die betroffene Person nicht verpflichtet ist, die Gründe für den Antrag auf Auskunft über personenbezogene Daten anzugeben: Rechtssache, C-307/22, ECLI:EU:C:2023:811, Rn. 38.
([102]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
([103]) Standpunkt und Feststellungen des Rates, Rn. 27 und 28.
([104]) https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_de.

ergänzen. Diese Initiativen erleichtern den einfachen Wechsel zwischen Diensten und schaffen so eine größere Auswahl für Einzelpersonen, fördern Wettbewerb und Innovation und ermöglichen es Einzelpersonen, die Vorteile aus der Nutzung ihrer Daten zu ziehen. Die Datenverordnung gewährt den Nutzern intelligenter Geräte ein erweitertes Recht auf Übertragbarkeit von Daten, die durch solche Geräte erzeugt werden, und schreibt vor, dass die Gestaltung des Produkts oder ein Backend-Server des Herstellers oder Dateninhabers eine solche Übertragbarkeit technisch möglich machen müssen. Nach dem Gesetz über digitale Märkte müssen Betreiber zentraler Plattformdienste, die als „Torwächter" eingestuft wurden, die effektive Übertragbarkeit der Daten der Nutzer sicherstellen, einschließlich des kontinuierlichen Echtzeitzugangs zu diesen Daten. Mehrere andere Initiativen der Kommission, über die derzeit verhandelt wird oder über die eine politische Einigung erzielt wurde, sehen verbesserte Rechte auf Übertragbarkeit in bestimmten Bereichen vor, wie die Richtlinie über Plattformarbeit[105], der Europäische Raum für Gesundheitsdaten[106] und der Rahmen für den Zugang zu Finanzdaten[107].

4.3 Das Recht auf Beschwerde

Die große Zahl von Beschwerden zeigt, dass das Recht auf Beschwerde bei einer Datenschutzbehörde weithin bekannt ist. Die Organisationen der Zivilgesellschaft weisen auf ungerechtfertigte Unterschiede in den nationalen Verfahren bei der Bearbeitung von Beschwerden hin; dieses Problem wird im Vorschlag der Kommission zu Verfahrensregeln angegangen. Nur wenige Mitgliedstaaten haben von der in der DSGVO vorgesehenen Möglichkeit Gebrauch gemacht, einer gemeinnützigen Einrichtung das Recht einzuräumen, unabhängig vom Auftrag einer betroffenen Person Maßnahmen zu ergreifen (Artikel 80 Absatz 2). Die im Jahr 2020 angenommene Richtlinie über Verbandsklagen[108] wird jedoch zu einer stärkeren Harmonisierung in dieser Hinsicht führen, indem kollektive Maßnahmen von Einzelpersonen bei Verstößen gegen die DSGVO erleichtert werden. Die nationalen Maßnahmen zur Umsetzung der Richtlinie traten im Juni 2023 in Kraft.

4.4 Schutz personenbezogener Daten von Kindern

Kinder benötigen besonderen Schutz, wenn ihre personenbezogenen Daten verarbeitet werden.[109] Die DSGVO ist Teil eines umfassenden Rechtsrahmens, mit dem sichergestellt wird, dass Kinder sowohl offline als auch online geschützt werden.[110] Angesichts der zunehmenden Präsenz von Kindern im Internet wurden in den letzten Jahren eine Reihe von Maßnahmen auf EU- und nationaler Ebene ergriffen, um den Schutz von Kindern im Internet zu fördern. Die Datenschutzbehörden haben bei der Verarbeitung von Daten von Kindern erhebliche Geldbußen gegen Social-Media-Unternehmen verhängt, weil sie gegen die DSGVO verstoßen haben. Sie arbeiten auch mit anderen Behörden zusammen, um einen besseren Schutz von Kindern im Bereich der Werbung zu fordern. Im Bericht 2020

([105]) Plattformbeschäftigte: Rat bestätigt Einigung über neue Vorschriften zur Verbesserung ihrer Arbeitsbedingungen – Consilium (europa.eu).

([106]) Vorschlag für eine Verordnung über den europäischen Raum für Gesundheitsdaten (COM(2022) 197 final).

([107]) Vorschlag für eine Verordnung über einen Rahmen für den Zugang zu Finanzdaten und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010, (EU) Nr. 1095/2010 und (EU) 2022/2554 (COM(2023) 360 final).

([108]) Richtlinie (EU) 2020/1828 vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG (ABl. L 409 vom 4.12.2020, S. 1).

([109]) Erwägungsgrund 38 DSGVO.

([110]) Empfehlung zur Entwicklung und Stärkung integrierter Kinderschutzsysteme im Interesse des Kindeswohls: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection_de.

forderte die Kommission den Ausschuss auf, Leitlinien für die Verarbeitung von Daten von Kindern anzunehmen. Diese Arbeiten laufen derzeit.[111] Das Gesetz über digitale Dienste enthält spezifische Bestimmungen, um ein hohes Maß an Privatsphäre und Sicherheit für Kinder, die Online-Plattformen nutzen, sicherzustellen.

Einige Interessenträger berichten über Herausforderungen bei der Ausübung der Rechte betroffener Personen, wenn es sich bei den betroffenen Personen um Kinder handelt. Insbesondere berichten sie, dass Kinder ihre Rechte nicht vollständig verstehen, keine digitalen Kompetenzen besitzen und möglicherweise ungebührlicher Einflussnahme ausgesetzt sind.[112] Die Kommission hat mehrere Initiativen auf nationaler Ebene zum Schutz der Daten von Kindern und zur Förderung des Datenschutzbewusstseins von Kindern finanziert.[113] Im Rahmen der Strategie „Besseres Internet für Kinder“ (BIK+) stellt die Kommission Kindern Sensibilisierungsressourcen und Schulungen zu ihren digitalen Rechten, einschließlich des Datenschutzes (z. B. digitale Einwilligung), zur Verfügung.[114] Der Schwerpunkt wird zunehmend auf die Notwendigkeit wirksamer und datenschutzfreundlicher Instrumente zur Altersüberprüfung gelegt. Anfang 2024 richtete die Kommission mit den Mitgliedstaaten, dem Ausschuss und der Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste eine Taskforce zur Altersüberprüfung ein, um die Entwicklung eines EU-weiten Ansatzes für die Altersüberprüfung zu erörtern und zu unterstützen. Diese Arbeit wird nun in der vom Europäischen Gremium für digitale Dienste gebildeten Arbeitsgruppe „Schutz von Minderjährigen“ fortgesetzt. Im Zusammenhang mit der Verordnung über die europäische digitale Identität[115], die im Mai 2024 in Kraft trat, arbeitet die Kommission daran, sicherzustellen, dass die Brieftasche für die europäische digitale Identität im Jahr 2026 allen Bürgern und Einwohnern der EU, auch zur Altersüberprüfung, angeboten wird. Bis das Ökosystem der Brieftasche voll funktionsfähig ist, wird eine kurzfristige Lösung für die Altersüberprüfung entwickelt und in der gesamten EU zur Verfügung gestellt.

5 Chancen und Herausforderungen für Organisationen, insbesondere KMU

Die DSGVO hat für im Binnenmarkt tätige Unternehmen gleiche Wettbewerbsbedingungen geschaffen, und ihr technologieneutraler, innovationsfreundlicher Ansatz ermöglicht es den Unternehmen, Bürokratie abzubauen und von einem größeren Verbrauchervertrauen zu profitieren.[116] Viele Unternehmen haben eine interne Kultur des Datenschutzes entwickelt und sehen den Schutz der Privatsphäre und personenbezogenen Daten als Schlüsselparameter für den Wettbewerb. Unternehmen schätzen den risikobasierten Ansatz der DSGVO als Leitprinzip, das Flexibilität und Skalierbarkeit ihrer Verpflichtungen ermöglicht.[117]

([111]) Siehe auch Standpunkt und Feststellungen des Rates, Rn. 31 Buchstabe a.
([112]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
([113]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en.
([114]) https://digital-strategy.ec.europa.eu/de/policies/strategy-better-internet-kids.
([115]) Verordnung (EU) 2024/1183 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des Rahmens für die europäische digitale Identität (ABl. L 2024/1183 vom 30.4.2024).
([116]) Wie im Bericht der Plattform „Fit for Future“ gewürdigt wird, wurde eine hochrangige Expertengruppe eingesetzt, die die Kommission dabei unterstützt, EU-Rechtsvorschriften zu vereinfachen und den damit verbundenen unnötigen Regelungsaufwand zu verringern: https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f_de. Siehe auch die Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO sowie des Standpunkts und der Feststellungen des Rates, Rn. 12.
([117]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

5.1 Instrumentarium für Unternehmen

Die DSGVO bietet ein Instrumentarium, das es Organisationen ermöglicht, ihre Compliance flexibel zu verwalten und nachzuweisen, darunter Verhaltensregeln, Zertifizierungsmechanismen und Standardvertragsklauseln. Wie im Bericht 2020 angekündigt, nahm die Kommission im Jahr 2021 Standardvertragsklauseln für die Beziehung zwischen Verantwortlichen und Auftragsverarbeitern an.[118] Diese Standardvertragsklauseln bieten ein fertiges und leicht umzusetzendes Instrument zur freiwilligen Compliance, das besonders für KMU oder Organisationen nützlich ist, die unter Umständen nicht über die Ressourcen verfügen, um individuelle Verträge mit ihren Geschäftspartnern auszuhandeln. Unternehmen berichten über gemischte Rückmeldungen zur Verwendung der Standardvertragsklauseln in dem Sinne, dass einige Unternehmen (vor allem KMU) diese ganz oder teilweise nutzen, während andere (meist größere Unternehmen) diese eher nicht verwenden, weil sie lieber eigene Klauseln verwenden.

Unternehmen betonen, dass Verhaltensregeln ein großes Potenzial als sektorspezifisches und kosteneffizientes Instrument zur Einhaltung der Vorschriften haben.[119] Die Entwicklung von Verhaltensregeln war jedoch begrenzt.[120] Den bisher vorliegenden Informationen zufolge wurden nur zwei EU-weite Regeln genehmigt (beide im Cloud-Sektor), während sechs Regeln auf nationaler Ebene genehmigt wurden.[121] Die Interessenträger melden aufwendige Anforderungen (u. a. die Notwendigkeit, eine akkreditierte Überwachungsstelle einzurichten), das mangelnde Engagement der Datenschutzbehörden und ein langwieriges Genehmigungsverfahren als Hauptfaktoren, die die Einführung von Verhaltensregeln einschränken.[122]

Das Verfahren muss transparenter gestaltet werden, und es müssen klare Fristen für die Genehmigung festgelegt werden. Die Datenschutzbehörden und – im Falle EU-weiter Regeln – der Ausschuss sollten die Ausarbeitung von Verhaltensregeln aktiver fördern, indem sie mit den Verbänden zusammenarbeiten, die die Regeln entwickeln. Dies wird dazu beitragen, Auslegungsunterschiede zu beheben und das Genehmigungsverfahren zu beschleunigen. Die Interessenträger bedauern die langen Verzögerungen bei der Annahme von Verhaltensregeln, die dadurch entstanden sind, dass Fragen im Rahmen der Arbeit an den Leitlinien parallel diskutiert wurden. Die Unternehmen berichten ferner, dass die Zertifizierung nicht weitverbreitet ist, da der Entwicklungsprozess langsam und komplex ist. Wie bei den Verhaltensregeln sollten die Datenschutzbehörden klarere Fristen für die Überprüfung und Genehmigung von Zertifizierungen festlegen.

Der Ausschuss hat sich in seiner Strategie 2024–2027 verpflichtet, Compliance-Maßnahmen wie Zertifizierung und Verhaltensregeln weiterhin zu unterstützen, unter anderem durch die Zusammenarbeit mit wichtigen Gruppen von Interessenträgern, um zu erläutern, wie die Instrumente eingesetzt werden können.[123]

([118]) Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 DSGVO und Artikel 29 Absatz 7 DSGVO (C/2021/3701) (ABl. L 199 vom 7.6.2021, S. 18).

([119]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

([120]) Standpunkt und Feststellungen des Rates, Rn. 25.

([121]) https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en?f%5B0%5D=coc_scope%3Anational.

([122]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

([123]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf.

5.2 Besondere Herausforderungen für KMU und kleine Wirtschaftsteilnehmer

Im Bericht 2020 forderte die Kommission, dass die Anstrengungen zur Unterstützung der KMU bei der Einhaltung der DSGVO intensiviert werden. In den letzten Jahren haben die Datenschutzbehörden und der Ausschuss die Entwicklung von Compliance-Instrumenten für KMU fortgesetzt, die teilweise durch Mittel der Kommission unterstützt werden.[124] Im April 2023 veröffentlichte der Ausschuss einen Datenschutzleitfaden für kleine Unternehmen[125], der in einem zugänglichen und leicht verständlichen Format praktische Informationen für KMU enthält.

KMU in vielen Mitgliedstaaten betonen die Vorteile einer maßgeschneiderten Unterstützung durch ihre lokalen Datenschutzbehörden. Die unterschiedlichen Ansätze der Datenschutzbehörden zur Sensibilisierung und Anleitung führen jedoch dazu, dass die KMU in bestimmten Mitgliedstaaten die Einhaltung der Vorschriften als komplex empfinden und die Durchsetzung fürchten.[126]) Die Datenschutzbehörden sollten ihre Anstrengungen zur Bewältigung dieser Herausforderungen verdoppeln, unter anderem indem sie aktiv mit den KMU zusammenarbeiten, um unbegründete Bedenken hinsichtlich der Einhaltung auszuräumen. Die Datenschutzbehörden sollten sich darauf konzentrieren, maßgeschneiderte Unterstützung und praktische Instrumente bereitzustellen, wie Vorlagen (z. B. für die Durchführung von Datenschutz-Folgenabschätzungen), Hotlines, illustrative Beispiele, Checklisten und Anleitungen zu bestimmten Verarbeitungsvorgängen (z. B. Rechnungsstellung oder Newsletter) sowie technischen und organisatorischen Maßnahmen. Da die meisten KMU nicht über internes Datenschutz-Fachwissen verfügen, sollten alle an KMU gerichteten Leitlinien auch für Personen ohne juristische Ausbildung leicht verständlich sein.[127]

Im Einklang mit dem risikobasierten Ansatz der DSGVO tragen KMU, die Verarbeitungstätigkeiten mit geringem Risiko durchführen, keine erhebliche Belastung bei der Compliance. Während die Ausnahmeregelung zur Führung von Aufzeichnungen über Verarbeitungstätigkeiten[128] nur unter bestimmten Umständen[129] gilt, können KMU, die Verarbeitungen mit geringem Risiko durchführen, die Anforderungen erfüllen, indem sie auf der Grundlage der von den Datenschutzbehörden bereitgestellten Vorlagen vereinfachte Aufzeichnungen führen. Darüber hinaus sollten solche Aufzeichnungen als nützliches Instrument für KMU betrachtet werden, um eine Bestandsaufnahme ihrer Verarbeitungstätigkeiten vorzunehmen.

5.3 Datenschutzbeauftragte

Datenschutzbeauftragte spielen eine wichtige Rolle, wenn es darum geht, die Einhaltung der DSGVO in den Organisationen, in denen sie tätig sind, sicherzustellen. Im Allgemeinen verfügen Datenschutzbeauftragte, die in der EU tätig sind, über das erforderliche Wissen und die Fertigkeiten, um ihre Aufgaben im Rahmen der DSGVO

(124) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en.
(125) https://www.edpb.europa.eu/sme-data-protection-guide/home_de.
(126) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
(127) Siehe Standpunkt und Feststellungen des Rates, Rn. 24; Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
(128) Artikel 30 Absatz 5 DSGVO.
(129) Wenn die Organisation weniger als 250 Mitarbeiter beschäftigt , sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 DSGVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 DSGVO einschließt.

wahrzunehmen, und ihre Unabhängigkeit wird gewahrt.[130] Allerdings bestehen nach wie vor mehrere Herausforderungen, darunter: i) Schwierigkeiten bei der Ernennung von Datenschutzbeauftragten, die über das erforderliche Fachwissen verfügen; ii) fehlende EU-weite Standards für die Bildung und Ausbildung; iii) Versäumnis, Datenschutzbeauftragte angemessen in organisatorische Prozesse zu integrieren; iv) Mangel an Ressourcen; v) zusätzliche Aufgaben außerhalb des Datenschutzes; und vi) unzureichendes Dienstalter.[131] Der Ausschuss stellte fest, dass die Datenschutzbehörden ihre Sensibilisierungsmaßnahmen sowie ihre Informations- und Durchsetzungsmaßnahmen intensivieren müssen, um sicherzustellen, dass die Datenschutzbeauftragten ihre Aufgaben im Rahmen der DSGVO wahrnehmen können.[132]

6 DIE DSGVO ALS ECKPFEILER DER EU-POLITIK IM DIGITALEN BEREICH

6.1 Digitalpolitik auf der Grundlage der DSGVO

Im Bericht 2020 verpflichtete sich die Kommission, die einheitliche Anwendung des Datenschutzrahmens in Bezug auf neue Technologien zu unterstützen, um Innovationen und technologische Entwicklungen zu fördern. Seither hat die EU eine Reihe von Initiativen angenommen, von denen einige die DSGVO ergänzen oder festlegen, wie sie in bestimmten Bereichen anzuwenden ist, um bestimmte Ziele zu verfolgen, wie nachstehend dargelegt.

- Das Gesetz über digitale Dienste ([133]), mit dem ein sicheres Online-Umfeld für Einzelpersonen und Unternehmen geschaffen werden soll, verbietet Online-Plattformen, Werbung auf der Grundlage von Profiling unter Verwendung von „besonderen Kategorien personenbezogener Daten“ im Sinne der DSGVO anzuzeigen.
- Um die digitalen Märkte gerechter und bestreitbarer zu machen, untersagt das Gesetz über digitale Märkte ([134]) Betreibern, die als Torwächter benannt wurden, personenbezogene Daten zwischen ihren zentralen Plattformdiensten und anderen Diensten zu „kombinieren“ und „intern zu nutzen“, es sei denn, der Nutzer hat seine Einwilligung im Sinne der DSGVO erteilt.
- Das KI-Gesetz[135] legt die EU-Datenschutzvorschriften in bestimmten Bereichen fest, in denen KI eingesetzt wird, z. B. in biometrischen Fernidentifizierungssystemen, bei der Verarbeitung besonderer Kategorien von Daten zur Erkennung von Verzerrungen und der Weiterverarbeitung personenbezogener Daten in Reallaboren.
- Die Richtlinie über Plattformarbeit[136] ergänzt die DSGVO im Bereich der Beschäftigung, indem sie Vorschriften für automatisierte Überwachungs- und Entscheidungssysteme, die von digitalen Arbeitsplattformen genutzt werden, und insbesondere Beschränkungen für die Verarbeitung personenbezogener Daten, die

([130]) Standpunkt und Feststellungen des Rates, Rn. 26; EDSA 2023 Koordinierte Durchsetzungsmaßnahmen Benennung und Position von Datenschutzbeauftragten: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf.
([131]) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
([132]) Siehe Empfehlungen des EDSA Koordinierte Durchsetzungsmaßnahmen.
([133]) Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27.10.2022, S. 1).
([134]) Verordnung (EU) 2022/1925 (Gesetz über digitale Märkte) (ABl. L 265 vom 12.10.2022, S. 1).
([135]) Verordnung (EU) 2024/1689 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024).
([136]) Plattformbeschäftigte: Rat bestätigt Einigung über neue Vorschriften zur Verbesserung ihrer Arbeitsbedingungen – Consilium (europa.eu).

Transparenz der menschlichen Aufsicht sowie die Überprüfung und Übertragbarkeit festlegt.

- Die Verordnung über politische Werbung[137] verbietet die Verwendung besonderer Kategorien personenbezogener Daten in politischer Werbung und verlangt mehr Transparenz in Bezug auf die eingesetzten Verfahren zum Targeting und Amplifizieren.
- Die Verordnung über die europäische digitale Identität ermöglicht die Schaffung einer universellen, vertrauenswürdigen und sicheren Brieftasche für die Europäische Digitale Identität. Dies wird es Einzelpersonen ermöglichen, persönliche Merkmale wie Alter, Führerscheine, Diplome und Bankkonten unter vollständiger Kontrolle über ihre personenbezogenen Daten und ohne unnötigen Datenaustausch nachzuweisen.

Über den Vorschlag für eine Datenschutzverordnung für elektronische Kommunikation[138], die die derzeitige Datenschutzrichtlinie für elektronische Kommunikation[139] ersetzen und den Rechtsrahmen zum Schutz der Privatsphäre und zum Datenschutz ergänzen soll, wird seit mehreren Jahren verhandelt. Es muss über die nächsten Schritte dieser Initiative, einschließlich ihrer Beziehung zur DSGVO, nachgedacht werden.

Das Gesetz für ein interoperables Europa[140] zielt darauf ab, digitale öffentliche Dienste in der gesamten EU interoperabel zu machen. Es unterstützt die Zusammenarbeit zwischen den Datenschutzbehörden, insbesondere durch Interoperabilitäts-Reallabore.

Mehrere EU-Initiativen bieten eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch private Einrichtungen zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten. Solche Rechtsvorschriften müssen sorgfältig darauf ausgerichtet sein, Eingriffe in das Recht auf Schutz personenbezogener Daten so gering wie möglich zu halten, und in einem angemessenen Verhältnis zu dem verfolgten Ziel stehen.[141] Die Charta, die DSGVO und die Rechtsprechung des Gerichtshofs bieten einen Rahmen, an dem diese Initiativen gemessen werden sollten. Das vorgeschlagene Maßnahmenpaket zur Bekämpfung der Geldwäsche[142] enthält umfassende Garantien für den Schutz personenbezogener Daten, ohne das Ziel zu gefährden, die Risiken von Geldwäsche und Terrorismusfinanzierung zu mindern und kriminelle Versuche, das Finanzsystem der EU zu missbrauchen, wirksam aufzudecken.

In diesem Zusammenhang hat der Rat betont, dass alle neuen EU-Rechtsvorschriften, die Bestimmungen über die Verarbeitung personenbezogener Daten enthalten, mit der DSGVO und der Rechtsprechung des Gerichtshofs im Einklang stehen sollten.

6.2 Ein Rechtsrahmen zur Verbesserung des Datenaustauschs

Die Datenstrategie zielt darauf ab, einen Binnenmarkt für Daten zu schaffen, in dem Daten innerhalb der EU und sektorübergreifend zum Nutzen von Unternehmen, Wissenschaftlern und öffentlichen Verwaltungen ungehindert übertragen werden können. Ein zentrales Ziel

---

([137]) Verordnung (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung (ABl. L 2024/900 vom 20.3.2024).

([138]) Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (COM(2017) 010 final).

([139]) Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

([140]) Verordnung (EU) 2024/903 (Verordnung für ein interoperables Europa) (ABl. L, 2024/903, 22.3.2024).

([141]) Siehe Standpunkt und Feststellungen des Rates, Rn. 31 Buchstabe f.

([142]) https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.

der Datenstrategie ist die Schaffung gemeinsamer europäischer Datenräume, die die Bündelung von Daten, den Zugang zu ihnen und ihre gemeinsame Nutzung erleichtern. In Bezug auf personenbezogene Daten bildet die DSGVO den Rahmen für alle Initiativen, die darauf abzielen, den freien Datenverkehr in der EU zu verbessern, was selbst ein Ziel der DSGVO ist. Soweit personenbezogene Daten betroffen sind, werden die Schutzbestimmungen der DSGVO nicht berührt.

Der Daten-Governance-Rechtsakt[143] und die Datenverordnung[144] sind Säulen der Datenstrategie. Der Daten-Governance-Rechtsakt enthält konkrete Vorschriften im Zusammenhang mit der Weiterverwendung von Daten des öffentlichen Sektors, die personenbezogene Daten umfassen, und schafft einen Rechtsrahmen für Datenvermittlungsdienste, einschließlich Diensten für die Verwaltung personenbezogener Informationen oder Clouds für personenbezogene Daten, die den betroffenen Personen bei der Ausübung ihrer Rechte gemäß der DSGVO zur Verfügung stehen. Außerdem werden die Bedingungen für die Verwendung von Daten für altruistische Zwecke festgelegt. Die Datenverordnung stärkt die Kontrolle der betroffenen Personen über die von ihnen durch die Nutzung intelligenter Objekte, die sie besitzen, mieten oder leasen, erzeugten Daten, indem technische Anforderungen an den Datenzugang und die Datenübertragbarkeit vorgeschrieben werden.

Der europäische Raum für Gesundheitsdaten[145] spiegelt den spezifischen Bedarf im Bereich der Gesundheitsdaten wider und baut gleichzeitig auf der DSGVO auf. Er ermöglicht es Einzelpersonen, problemlos in elektronischer Form auf ihre Gesundheitsdaten zuzugreifen und sie an Angehörige der Gesundheitsberufe, auch in anderen Mitgliedstaaten, weiterzugeben, wodurch die Gesundheitsversorgung verbessert und die Kontrolle der Patienten über ihre Daten erhöht wird. Außerdem wird ein gemeinsamer Rechtsrahmen für die Weiterverwendung von Gesundheitsdaten für Zwecke wie Forschung, Innovation und öffentliche Gesundheit geschaffen, der auf einer Genehmigung beruht, die von einer Zugangsstelle für Gesundheitsdaten erteilt wird. Um für den Schutz personenbezogener Daten zu sorgen, wird der europäische Raum für Gesundheitsdaten ein vertrauenswürdiges Umfeld für den sicheren Zugang zu Gesundheitsdaten und deren Verarbeitung bieten. Die Kommission unterstützt weiterhin die Arbeiten zur Entwicklung gemeinsamer europäischer Datenräume in 14 Sektoren, indem sie den neuen Rechtsrahmen umsetzt und sektorspezifische Initiativen finanziert.

6.3 Governance neuer digitaler Vorschriften

Die Entwicklung digitaler Vorschriften macht eine enge Zusammenarbeit in allen Regulierungsbereichen erforderlich.[146] Eine solche Zusammenarbeit ist umso notwendiger, als sich Datenschutzfragen zunehmend beispielsweise mit Fragen des Wettbewerbsrechts, des Verbraucherrechts, der Vorschriften für digitale Märkte, der Regulierung der elektronischen Kommunikation und der Cybersicherheit überschneiden. Dies ist beispielsweise bei der Beurteilung der Vereinbarkeit von „Zustimmungs- oder Bezahlungsmodellen“ („Pay or Okay“-Modellen) mit dem Unionsrecht der Fall.

In einigen Fällen sind die Datenschutzbehörden mit der Durchsetzung spezifischer Bestimmungen neuer EU-Rechtsvorschriften im digitalen Bereich betraut.[147] Durch neue

(143) Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) (ABl. L 152 vom 3.6.2022, S. 1).
(144) Verordnung (EU) 2023/2854 (Datenverordnung) (ABl. L, 2023/2854, 22.12.2023).
(145) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_DE.html.

(146) Siehe Standpunkt und Feststellungen des Rates, Rn. 40 und 41; Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
(147) Siehe z. B. Artikel 37 Absatz 3 der Datenverordnung.

digitale Vorschriften werden auch maßgeschneiderte Strukturen geschaffen, die die zuständigen Regulierungsbehörden zusammenbringen, um eine kohärente Durchsetzung sicherzustellen, wie die hochrangige Gruppe für das Gesetz über digitale Märkte, der Europäische Dateninnovationsrat (der im Rahmen des Daten-Governance-Rechtsakts eingerichtet wurde) und das Europäische Gremium für digitale Dienste (eingesetzt im Rahmen des Gesetzes über digitale Dienste). Die NI-S2-Richtlinie[148] enthält detailliertere Vorschriften für die Zusammenarbeit zwischen den Regulierungsbehörden und den Datenschutzbehörden beim Umgang mit Sicherheitsvorfällen, die Verletzungen des Schutzes personenbezogener Daten darstellen.

Außerhalb dieser formalen Strukturen unternehmen die Datenschutzbehörden Schritte, um sicherzustellen, dass ihre Maßnahmen mit anderen Regulierungsbereichen komplementär und kohärent sind. Im Juli 2020 richteten Verbraucher- und Datenschutzbehörden eine „Gruppe von Freiwilligen“ ein, um bewährte Verfahren zu ermitteln und Erfahrungen bei der Durchsetzung auszutauschen. Die Datenschutzbehörden nehmen weiterhin an gemeinsamen Workshops mit dem Netzwerk für die Zusammenarbeit im Verbraucherschutz teil. Im Jahr 2023 richtete der Ausschuss eine Taskforce für das Zusammenspiel von Datenschutz, Wettbewerb und Verbraucherschutz ein.

Diese Entwicklungen sind zwar positiv, doch bedarf es strukturierterer und effizienterer Mittel der Zusammenarbeit, insbesondere zur Bewältigung von Situationen, die eine große Zahl von Einzelpersonen in der EU betreffen und an denen mehrere Regulierungsbehörden beteiligt sind.[149] Strukturen dieser Art sollten sicherstellen, dass die Behörden jederzeit für alle Fragen im Zusammenhang mit der Einhaltung der Vorschriften in ihrem Zuständigkeitsbereich verantwortlich bleiben. Die Mitgliedstaaten sollten auch darauf hinwirken, dass auf nationaler Ebene eine angemessene Zusammenarbeit stattfindet.[150]

7 INTERNATIONALE DATENÜBERMITTLUNGEN UND GLOBALE ZUSAMMENARBEIT

7.1 Das Instrumentarium der DSGVO für Datenübermittlungen

Der Datenverkehr ist integraler Bestandteil des digitalen Wandels der Gesellschaft und der Globalisierung der Wirtschaft geworden. Mehr denn je ist die Wahrung der Privatsphäre eine Voraussetzung für stabile, sichere und wettbewerbsfähige Handelsströme und ermöglicht viele Formen der internationalen Zusammenarbeit. Das in Kapitel V der DSGVO vorgesehene Instrumentarium für die Datenübermittlung bietet eine Vielzahl von Instrumenten für unterschiedliche Übermittlungsszenarien und stellt gleichzeitig sicher, dass die Daten beim Verlassen der EU weiterhin ein hohes Schutzniveau genießen.

Seit dem Bericht 2020 wurden die in den EU-Datenschutzvorschriften festgelegten Anforderungen für Datenübermittlungen weiter präzisiert, und das Instrumentarium für die Übermittlung von Daten hat sich ständig weiterentwickelt. Eine wichtige Klarstellung betrifft den Begriff „internationale Übermittlung“, der vom Ausschuss[151] definiert wurde als jede Weitergabe personenbezogener Daten durch einen Verantwortlichen oder Auftragsverarbeiter, dessen Verarbeitung der DSGVO unterliegt, an einen anderen Verantwortlichen oder Auftragsverarbeiter in einem Drittland, unabhängig davon, ob die

(148) Richtlinie (EU) 2022/2555 (NI-S-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).
(149) Siehe Standpunkt und Feststellungen des Rates, Rn. 18, Rn. 40–41 und die Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
(150) Deutschland hat einen „digitalen Cluster“ eingerichtet, dem Regulierungsbehörden aus verschiedenen Bereichen angehören, um ihre Zusammenarbeit in allen Aspekten der Digitalisierung auszuweiten und Wissen und bewährte Verfahren auszutauschen: https://www.dataguidance.com/news/germany-bsi-announces-formation-digital-cluster-bonn.
(151) Leitlinien 05/2021 des EDSA.

Verarbeitung durch diesen der DSGVO unterliegt oder nicht.[152] Diese Leitlinien des Ausschusses waren besonders wichtig, um europäischen Verantwortlichen und Auftragsverarbeitern Rechtssicherheit in Bezug auf die Szenarien zu bieten, in denen ein Übermittlungsinstrument gemäß Kapitel V DSGVO benötigt wird.

Weitere Klarstellungen hat der Gerichtshof in seinem Urteil in der Rechtssache *Schrems II*[153] zu dem Schutz gemacht, der durch verschiedene Übermittlungsinstrumente gewährleistet werden muss, um sicherzustellen, dass das durch die DSGVO garantierte Schutzniveau nicht untergraben wird.[154] Diese Instrumente müssen insbesondere sicherstellen, dass Personen, deren Daten außerhalb der EU übermittelt werden, ein Schutzniveau genießen, das dem innerhalb der EU garantierten Niveau im Wesentlichen gleichwertig ist.[155] Es liegt in der Verantwortung des EU-Datenexporteurs, zu beurteilen, ob dies der Fall ist, wobei die besonderen Umstände seiner Übermittlungen zu berücksichtigen sind.[156]

Bei der Beurteilung des Schutzniveaus müssen Datenexporteure sowohl die Datenschutzgarantien berücksichtigen, die in dem mit einem Datenimporteur aus Drittländern geschlossenen Übermittlungsinstrument (z. B. einem Vertrag) festgelegt sind, als auch maßgebliche Aspekte des Rechtssystems des Landes, in dem der Datenimporteur ansässig ist, insbesondere im Hinblick auf den möglichen Zugang der Behörden zu den Daten in diesem Land.[157] Letzteres muss anhand der in Artikel 45 DSGVO festgelegten Kriterien für die Beurteilung der Angemessenheit geprüft werden. Der Gerichtshof hat diese Kriterien zudem weiter ausgeführt, insbesondere in Bezug auf die Vorschriften über den Zugang von Behörden zu personenbezogenen Daten für Zwecke der Strafverfolgung und der nationalen Sicherheit.

Diese Auslegung schlägt sich auch in den Leitlinien des Ausschusses nieder, der seine „Referenzgrundlage für Angemessenheit“[158] aktualisiert hat (die Leitlinien zu den Elementen lieferte, die die Kommission bei der Durchführung einer Angemessenheitsbeurteilung zu berücksichtigen hat). Der Ausschuss nahm ferner neue Leitlinien an, die weitere Klarstellungen zu folgenden Punkten enthalten: i) die Elemente, die von den einzelnen Datenexporteuren bei der Beurteilung des Schutzniveaus zu berücksichtigen sind; ii) Überblick über mögliche Quellen, die genutzt werden können; und iii) Beispiele für mögliche ergänzende Maßnahmen (z. B. vertragliche und technische Schutzmaßnahmen).[159] In den Leitlinien wird ausdrücklich darauf hingewiesen, dass jede von Datenexporteuren durchgeführte Beurteilung einzigartig ist und dass sie daher die Besonderheiten jeder Übermittlung berücksichtigen müssen, die sich je nach Zweck der Datenübermittlung, Art der beteiligten Einrichtungen, Sektor, in dem die Übermittlung erfolgt, Kategorien der übermittelten personenbezogenen Daten usw. unterscheiden können. [160]

Unter Berücksichtigung dieser unterschiedlichen Klarstellungen zu den Anforderungen an internationale Datenübermittlungen wurden in den letzten Jahren wichtige Schritte unternommen, um das Instrumentarium der DSGVO für die Übermittlung von Daten weiterzuentwickeln und umzusetzen.

([152]) Abschnitt 2 der Leitlinien 05/2021 des EDSA.
([153]) Rechtssache C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).
([154]) *Schrems II*, Rn. 93.
([155]) *Schrems II*, Rn. 96 und 105.
([156]) *Schrems II*, Rn. 131.
([157]) *Schrems II*, Rn. 105.
([158]) Empfehlungen 02/2020 des EDSA und Referenzgrundlage für Angemessenheit, WP 254 rev. 01.
([159]) Empfehlungen 01/2020 des EDSA, ergänzt durch die Empfehlungen 02/2020.
([160]) Siehe z. B. Rn. 8–13, 32–33 der Empfehlungen 01/2020 des EDSA.

7.1.1 Angemessenheitsbeschlüsse

Wie auch in den Rückmeldungen der Interessenträger zum Ausdruck kommt, spielen Angemessenheitsbeschlüsse weiterhin eine Schlüsselrolle im Instrumentarium der DSGVO für die Übermittlung von Daten[161], da sie eine einfache und umfassende Lösung für Datenübermittlungen bieten, ohne dass der Datenexporteur weitere Garantien bieten oder eine Genehmigung einholen muss. Die Angemessenheitsbeschlüsse haben den freien Verkehr personenbezogener Daten ermöglicht, was zur Öffnung des Handelsverkehrs für die Wirtschaftsbeteiligten in der EU (unter anderem durch die Ergänzung und Verstärkung der Vorteile von Handelsabkommen) und zur Erleichterung der Zusammenarbeit mit ausländischen Partnern in einem breiten Spektrum von Bereichen, von der Zusammenarbeit in Regulierungsfragen bis zur Forschung, geführt hat.

Seit dem Bericht 2020 hat die Zahl der Länder, die moderne Datenschutzgesetze erlassen haben, die unter anderem wichtige Datenschutzgrundsätze, individuelle Rechte und eine wirksame Durchsetzung durch unabhängige Regulierungsbehörden vorsehen, weiter zugenommen. Dieser Trend[162] hat es der Kommission auch ermöglicht, ihre Tätigkeit im Bereich Angemessenheit zu intensivieren. Dazu gehört auch die Annahme eines Angemessenheitsbeschlusses für das Vereinigte Königreich[163], der für das ordnungsgemäße Funktionieren der verschiedenen Abkommen, die nach dem Brexit mit dem Vereinigten Königreich geschlossen wurden, von zentraler Bedeutung ist. Um sicherzustellen, dass der Angemessenheitsbeschluss zukunftssicher bleibt, enthält er eine „Auslaufklausel“, die 2025 enden soll; danach kann sie verlängert werden, wenn das Schutzniveau weiterhin angemessen ist. Die Kommission hat ferner einen Angemessenheitsbeschluss für die Republik Korea[164] angenommen, der das Freihandelsabkommen zwischen der EU und Korea über den Austausch personenbezogener Daten ergänzt und die Zusammenarbeit in Regulierungsfragen erleichtert. Eine erste Überprüfung des Angemessenheitsbeschlusses ist für Ende 2024 geplant.

Darüber hinaus nahm die Kommission nach der Außerkraftsetzung des Angemessenheitsbeschlusses für den EU-US-Datenschutzschild Gespräche mit der Regierung der Vereinigten Staaten auf, um eine Nachfolgevereinbarung zu entwickeln, die den vom Gerichtshof erläuterten Anforderungen entspricht.[165] Der US-Präsident verabschiedete ein neues US-Dekret über die „Verbesserung der Sicherheitsvorkehrungen für nachrichtendienstliche Tätigkeiten der Vereinigten Staaten“, mit der neue verbindliche und durchsetzbare Schutzmaßnahmen eingeführt wurden, um zu sicherzustellen, dass der Zugriff auf Daten zu Zwecken der nationalen Sicherheit nur in dem Maße möglich ist, wie es notwendig und verhältnismäßig ist, und dass die Europäer wirksame Rechtsmittel einlegen können. Auf dieser Grundlage nahm die Kommission ihren Angemessenheitsbeschluss zum Datenschutzrahmen[166] EU-USA an, der den freien Verkehr personenbezogener Daten aus der EU an US-amerikanische Unternehmen, die dem Datenschutzrahmen beitreten, ermöglicht. Da die von der US-Regierung im Bereich der nationalen Sicherheit eingeführten Garantien unabhängig von dem verwendeten Mechanismus der DSGVO für alle Datenübermittlungen an Unternehmen in den USA

([161]) Siehe z. B. Beitrag des Ausschusses, S. 7; Standpunkt und Feststellungen des Rates, Rn. 36; Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

([162]) Umsetzung der Mitteilung der Kommission über den Austausch und Schutz personenbezogener Daten in einer globalisierten Welt, 10.1.2017 COM(2017) 7 final.

([163]) Durchführungsbeschluss (EU) 2021/1772 der Kommission (ABl. L 360 vom 11.10.2021, S. 1).

([164]) Durchführungsbeschluss (EU) 2022/254 der Kommission (ABl. L 44 vom 24.2.2022, S. 1).

([165]) https://commission.europa.eu/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-2020-08-10_en.

([166]) Durchführungsbeschluss (EU) 2023/1795 der Kommission (ABl. L 231 vom 20.9.2023, S. 118).

gelten, wurde der Einsatz anderer Instrumente, wie Standardvertragsklauseln und verbindlicher unternehmensinterner Vorschriften, erheblich erleichtert. Eine erste Überprüfung der Funktionsweise des Datenschutzrahmens wird im Sommer 2024 stattfinden, um zu ermitteln, ob alle einschlägigen Elemente vollständig im US-Rechtsrahmen umgesetzt wurden und in der Praxis wirksam funktionieren.

Derzeit laufen Angemessenheitsverhandlungen mit Brasilien und Kenia sowie zum ersten Mal mit mehreren internationalen Organisationen (beispielsweise befinden sich die Angemessenheitsgespräche mit der Europäischen Patentorganisation in einem fortgeschrittenen Stadium).[167] Entsprechend den Forderungen verschiedener Interessenträger[168] hat sich die Kommission aktiv an Sondierungsgesprächen mit Ländern in verschiedenen Regionen der Welt beteiligt.

Ferner überwacht die Kommission kontinuierlich die Entwicklungen in den Ländern, die bereits von Angemessenheitsfeststellungen profitieren, und überprüft regelmäßig bestehende Beschlüsse im Einklang mit ihren entsprechenden Verpflichtungen im Rahmen der DSGVO.[169] Im April 2023 nahm die Kommission ihren Bericht über die erste regelmäßige Überprüfung des Angemessenheitsbeschlusses für Japan[170] an, in dem sie zu dem Schluss kam, dass Japan weiterhin für ein angemessenes Schutzniveau sorgt.[171] Die Überprüfung ergab, dass sich die Datenschutzrahmen der EU und Japans seit der Annahme der gegenseitigen Angemessenheitsbeschlüsse weiter annähern.

Darüber hinaus wurde gemäß Artikel 97 DSGVO die erste Überprüfung der elf Angemessenheitsbeschlüsse[172], die im Rahmen des früheren EU-Datenschutzrahmens (Datenschutzrichtlinie) erlassen wurden, im Rahmen der Bewertung der Anwendung und Funktionsweise der DSGVO im Jahr 2020 eingeleitet. Die Schlussfolgerung zu diesem Aspekt der Überprüfung wurde verschoben, um insbesondere dem Urteil des Gerichtshofs in der Rechtssache *Schrems II* und der anschließenden Auslegung durch den Ausschuss Rechnung zu tragen. Die genannten Klarstellungen des Rechnungshofs zu Schlüsselelementen des Angemessenheitsstandards führten zu einem ausführlichen Austausch mit den betreffenden Ländern und Gebieten über maßgebliche Aspekte ihres Rechtsrahmens sowie über Aufsichts- und Durchsetzungsmechanismen.

Am 15. Januar 2024 veröffentlichte die Kommission ihren Bericht über diese elf Beschlüsse zusammen mit detaillierten Länderberichten, in denen die Entwicklungen in den einzelnen Ländern und Gebieten seit der Annahme der Angemessenheitsbeschlüsse sowie die Vorschriften für den Zugang von Behörden zu Daten, insbesondere für Zwecke der Strafverfolgung und der nationalen Sicherheit, beschrieben werden.[173] In dem Bericht

---

([167]) Die Europäische Patentorganisation ist eine zwischenstaatliche Organisation, die auf der Grundlage des Europäischen Patentübereinkommens gegründet wurde. Ihre Hauptaufgabe besteht in der Erteilung europäischer Patente. In diesem Zusammenhang arbeitet sie eng mit Unternehmen und Behörden in den EU-Mitgliedstaaten sowie mit verschiedenen Organen und Einrichtungen der EU zusammen.

([168]) Beitrag des Ausschusses, S. 7.

([169]) Artikel 45 Absätze 4 und 5 DSGVO. Siehe auch *Schrems I*, Rn. 76.

([170]) Durchführungsbeschluss (EU) 2019/419 der Kommission (ABl. L 76 vom 19.3.2019, S. 1). Siehe auch https://ec.europa.eu/commission/presscorner/detail/de/IP_19_421. Dieser Beschluss stellte den ersten Angemessenheitsbeschluss, der im Rahmen der DSGVO angenommen wurde, und die erste gegenseitige Angemessenheitsvereinbarung dar.

([171]) Bericht der Kommission über die erste Überprüfung der Funktionsweise des Angemessenheitsbeschlusses in Bezug auf Japan, 3.4.2023, COM(2023) 275 final (und SWD(2023) 75 final).

([172]) Andorra, Argentinien, Kanada (für Wirtschaftsbeteiligte), Färöer, Guernsey, Isle of Man, Israel, Jersey, Neuseeland, Schweiz und Uruguay.

([173]) Bericht der Kommission über die erste Überprüfung der Wirkungsweise der Angemessenheitsfeststellungen gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG, 15.1.2024, COM(2024) 7 final (und SWD(2024) 3 final).

wird der Schluss gezogen, dass alle elf Länder und Gebiete weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten bieten. Er spiegelt wider, dass alle betroffenen Länder und Gebiete ihren Rechtsrahmen zum Schutz der Privatsphäre auf unterschiedliche Weise modernisiert und gestärkt haben. Wenn dies zur Sicherstellung der Kontinuität der Angemessenheitsfeststellung erforderlich war, wurden darüber hinaus mit einigen davon zusätzliche Garantien für aus Europa übermittelte personenbezogene Daten ausgehandelt und vereinbart, um maßgebliche Unterschiede bezüglich des Schutzniveaus anzugehen.

Diese Überprüfungen zeigen auch, dass die Angemessenheitsbeschlüsse die Grundlage für eine engere Zusammenarbeit und eine weitere Angleichung der Rechtsvorschriften zwischen der EU und diesen gleichgesinnten Partnern geschaffen haben und nicht etwa ein „Endpunkt" waren. So wird beispielsweise in dem Bericht über die erste Überprüfung des Angemessenheitsbeschlusses für Japan anerkannt, dass die weitere Stärkung des japanischen Datenschutzrahmens den Weg dafür ebnen kann, den Angemessenheitsbeschluss über den Handelsaustausch hinaus auf Übermittlungen auszuweiten, die derzeit von seinem Anwendungsbereich ausgenommen sind, z. B. im Bereich der Regulierungszusammenarbeit und der Forschung. Derzeit werden Gespräche geführt, um eine solche mögliche Verlängerung zu prüfen. Im Allgemeinen sind Angemessenheitsbeschlüsse zu einer strategischen Komponente der allgemeinen Beziehungen der EU zu diesen ausländischen Partnern geworden und werden als wichtiger Faktor für die Vertiefung der Zusammenarbeit in einer Vielzahl von Bereichen anerkannt.

Das wachsende Netz von Ländern und Gebieten, für die die EU einen Angemessenheitsbeschluss angenommen hat, bietet nicht nur eine solide Grundlage für eine verstärkte bilaterale Zusammenarbeit, sondern auch neue Möglichkeiten, um die Vorteile eines sicheren und freien Datenverkehrs zu maximieren und bei der Durchsetzung der Datenschutzvorschriften enger zwischen gleichgesinnten Partnern zusammenzuarbeiten. Im März 2024 veranstaltete die Kommission daher das erste Expertentreffen über den sicheren Datenverkehr, bei dem die zuständigen Minister und Leiter der Datenschutzbehörden von 15 Ländern und Gebieten, für die die EU einen Angemessenheitsbeschluss angenommen hat, sowie der Vorsitz des Europäischen Datenschutzausschusses zusammenkamen.[174] Auf der Sitzung wurden mehrere konkrete Aktionspunkte ermittelt, zu denen in dieser Gruppe Folgemaßnahmen laufen.

Generell werden durch die Kommission erlassene Angemessenheitsbeschlüsse aufgrund ihres „Netzwerkeffekts" auch über die EU hinaus immer wichtiger, da sie nicht nur den freien Datenverkehr mit den 30 Volkswirtschaften des EWR ermöglichen, sondern auch mit vielen anderen Ländern und Gebieten auf der ganzen Welt, die in ihren eigenen Datenschutzvorschriften Länder als sichere Zielländer anerkennen, deren Schutzniveau von der EU als angemessen eingestuft wurde.[175]

7.1.2 Instrumente, die geeignete Garantien bieten

Seit dem Bericht 2020 wurden zusätzliche Instrumente entwickelt, die geeignete Garantien bieten, und praktische Leitlinien herausgegeben, um deren Nutzung zu erleichtern.

Wie im Bericht 2020 angekündigt, hat die Kommission modernisierte Standardvertragsklauseln[176] angenommen, deren Entwicklung sich weitgehend auf Rückmeldungen verschiedener Interessenträger stützte.[177] Die neuen

(174) https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307#11.
(175) Dazu gehören beispielsweise Argentinien, Kolumbien, Israel, Marokko, die Schweiz und Uruguay.
(176) Durchführungsbeschluss (EU) 2021/914 der Kommission (ABl. L 199 vom 7.6.2021, S. 31).
(177) Dazu gehörte beispielsweise die gemeinsame Stellungnahme 2/2021 des EDSA und des EDSB im Rahmen des Verfahrens zur Annahme der Standardvertragsklauseln.

Standardvertragsklauseln haben die drei Standardvertragsklauseln ersetzt, die im Rahmen der Datenschutzrichtlinie angenommen wurden. Zu den wichtigsten Neuerungen gehören: i) aktualisierte Garantien im Einklang mit der DSGVO; ii) ein modularer Ansatz, der einen zentralen Einstiegspunkt für eine breite Palette von Übertragungsszenarien bietet; iii) größere Flexibilität bei der Verwendung von Standardvertragsklauseln durch mehrere Parteien; und iv) ein praktisches Instrumentarium zur Umsetzung des Urteils *Schrems II*.

Die modernisierten Standardvertragsklauseln wurden von den Interessenträgern begrüßt, und die eingegangenen Rückmeldungen bestätigen, dass Standardvertragsklauseln nach wie vor das bei Weitem am häufigsten verwendete Instrument für die Übermittlung von Daten durch EU-Datenexporteure sind.[178] Um die Datenexporteure bei ihren Bemühungen um Einhaltung der Vorschriften zu unterstützen, hat die Kommission eine Webseite mit Fragen und Antworten erstellt, die weitere Leitlinien für die Anwendung der Klauseln enthält[179] und bei neuen Fragen, auch im Lichte der im Rahmen dieser Bewertung eingegangenen weiteren Rückmeldungen, weiter aktualisiert wird.

Viele Datenexporteure berichten von Schwierigkeiten bei der Durchführung der im Urteil in der Rechtssache *Schrems II* geforderten „Datentransfer-Folgenabschätzungen", wobei sie insbesondere auf deren Komplexität sowie auf die Kosten und den Zeitaufwand für ihre Durchführung verweisen.[180] Sie begrüßen die Leitlinien des Ausschusses und der Standardvertragsklauseln, fordern jedoch zusätzliche Leitlinien (z. B. in Bezug auf die Zuständigkeiten der beteiligten Parteien und den bei Folgenabschätzungen für Datenübermittlungen erforderlichen Detaillierungsgrad) und zusätzliche Instrumente zur Unterstützung der Durchführung solcher Beurteilungen (z. B. Vorlagen, allgemeine Länderbeurteilungen, Risikokataloge). Die Interessenträger haben zwar hauptsächlich Rückmeldungen zu den Standardvertragsklauseln gegeben, dieselben Beurteilungen sind jedoch auch für andere Übermittlungsinstrumente (z. B. verbindliche unternehmensinterne Vorschriften) erforderlich. Daher ist es wichtig, dass der Ausschuss – aufbauend auf den Erfahrungen mit der Anwendung der sich aus der Rechtssache *Schrems II* ergebenden Anforderungen in den vergangenen Jahren, auch im Rahmen der Durchsetzungsmaßnahmen der nationalen Datenschutzbehörden – prüft, wie Datenexporteure in diesem Zusammenhang weiter unterstützt werden können.

Zur Ergänzung der bestehenden Standardvertragsklauseln entwickelt die Kommission zusätzliche Klauseln, um den EU-Datenexporteuren ein umfassendes und kohärentes Paket zur Verfügung zu stellen. Dazu gehören Standardvertragsklauseln gemäß der Verordnung (EU) 2018/1725 für Datenübermittlungen durch Organe, Einrichtungen und sonstigen Stellen der EU an Wirtschaftsbeteiligte in Drittländern[181] und Standardvertragsklauseln für Datenübermittlungen an Datenimporteure aus Drittländern, deren Verarbeitungsvorgänge unmittelbar unter die DSGVO fallen. Letzteres entspricht der Forderung der Interessenträger, insbesondere Szenarien abzudecken, in denen der Datenimporteur in den räumlichen Anwendungsbereich der DSGVO fällt (z. B. weil die betreffende Verarbeitung gemäß Artikel 3 Absatz 2 DSGVO auf den EU-Markt abzielt).[182] Wie der Ausschuss klargestellt hat, ist auch in diesem Fall ein Übermittlungsinstrument nach Kapitel V DSGVO erforderlich, da die Risiken für personenbezogene Daten, die außerhalb der EU

([178]) Standpunkt und Feststellungen des Rates, Rn. 37, Beitrag des Ausschusses, Seite 9, Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

([179]) https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en.

([180]) Siehe z. B. Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

([181]) Gemäß Artikel 48 Absatz 2 Buchstabe b der Verordnung (EU) 2018/1725.

([182]) Standpunkt und Feststellungen des Rates, Rn. 37, Beitrag des Ausschusses, S. 9, Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.

verarbeitet werden, z. B. aufgrund möglicherweise entgegenstehender nationaler Rechtsvorschriften oder eines unverhältnismäßigen staatlichen Zugriffs in dem Drittland, erhöht werden.[183] Die neuen Standardvertragsklauseln, die derzeit von der Kommission entwickelt werden, werden sich speziell mit diesem Szenario befassen und den Anforderungen, die im Rahmen der DSGVO bereits unmittelbar für diese Verantwortlichen und Auftragsverarbeiter gelten, in vollem Umfang Rechnung tragen.[184]

Wie auch von verschiedenen Arten von Interessenträgern[185] anerkannt wird, spielen Musterklauseln eine zunehmend zentrale Rolle bei der Erleichterung des Datenverkehrs in der ganzen Welt. Mehrere Länder und Gebiete haben die Standardvertragsklauseln der EU als Übermittlungsmechanismus im Rahmen ihrer eigenen Datenschutzgesetze mit begrenzten formellen Anpassungen ihrer innerstaatlichen Rechtsordnung gebilligt.[186] Einige andere Länder haben ihre eigenen Musterklauseln eingeführt, die wichtige gemeinsame Merkmale mit den Standardvertragsklauseln der EU aufweisen.[187] Ein besonders wichtiges Beispiel ist die Schaffung von Musterklauseln durch andere internationale/regionale Organisationen oder Netze wie den Beratenden Ausschuss des Europarats nach dem Übereinkommen Nr. 108, das Iberoamerikanische Datenschutznetzwerk und der Verband südostasiatischer Nationen (ASEAN).[188] Dies eröffnet neue Möglichkeiten, den Datenverkehr zwischen verschiedenen Regionen der Welt auf der Grundlage von Musterklauseln zu erleichtern. Ein konkretes Beispiel hierfür ist der EU-ASEAN Leitfaden zu den Standardvertragsklauseln der EU und den ASEAN-Musterklauseln, der sie auf der Grundlage von Beiträgen von Unternehmen bei ihren Bemühungen um die Einhaltung beider Klauseln unterstützt.[189]

Zusätzlich zu den Standardvertragsklauseln werden für den Datenverkehr zwischen Mitgliedern von Unternehmensgruppen oder zwischen Unternehmen, die eine gemeinsame wirtschaftliche Tätigkeit ausüben, weiterhin häufig verbindliche unternehmensinterne Vorschriften (BCR) verwendet. Da die DSGVO Anwendung findet, nahm der Ausschuss 80 positive Stellungnahmen zu nationalen Beschlüssen zur Genehmigung von verbindlichen unternehmensinternen Vorschriften an.[190] Der Ausschuss gab auch Leitlinien zu den Elementen heraus, die in die verbindlichen unternehmensinternen Vorschriften für Verantwortliche aufzunehmen sind (und zu den im Rahmen ihrer Anwendung bereitzustellenden Informationen). Diese Leitlinien wurden aktualisiert, um den Anforderungen der DSGVO und dem Urteil in der Rechtssache *Schrems II* zu tragen.[191] Außerdem werden aktualisierte Leitlinien zu verbindlichen

---

([183]) Leitlinien 05/2021 des EDSA, S. 3.
([184]) Wie auch in Abschnitt 4 der Leitlinien 05/2021 des EDSA dargelegt.
([185]) Beitrag des Ausschusses, S. 9, Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
([186]) Z. B. Vereinigtes Königreich (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) und Schweiz (https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html).
([187]) Z. B. Neuseeland (https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/) und Argentinien (https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm).
([188]) Siehe https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4; https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf und https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
([189]) https://commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062_en?filename=%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf.
([190]) Beitrag des Ausschusses, S. 9.
([191]) EDSA-Empfehlungen 1/2022.

unternehmensinternen Vorschriften für Auftragsverarbeiter ausgearbeitet.[192] Da verbindliche unternehmensinterne Vorschriften darauf abzielen, verbindliche Datenschutzstrategien/-programme in Unternehmen einzuführen, halten viele Interessenträger sie für ein besonders nützliches Instrument zur Einhaltung der Vorschriften und für ein vertrauenswürdiges Übermittlungsinstrument.[193] Gleichzeitig berichten die Interessenträger nach wie vor, dass die Länge und Komplexität des Genehmigungsverfahrens der nationalen Datenschutzbehörden eine breitere Einführung der verbindlichen internen Datenschutzvorschriften verhindert. Daher ist es wichtig, dass die Behörden weiter an der Straffung und Verkürzung des Genehmigungsverfahrens arbeiten.

Seit dem Bericht 2020 wurden auch Schritte unternommen, um die Verwendung von Zertifizierungen und Verhaltensregeln als Instrumente für Übermittlungen zu erleichtern, z. B. durch die Annahme spezieller Leitlinien für beide Instrumente durch den Ausschuss.[194] Gleichzeitig berichten die Interessenträger über dieselben Probleme in Bezug auf den Zeitplan und die Komplexität des Genehmigungsverfahrens wie die genannten in Bezug auf Zertifizierung und Verhaltensregeln als Instrumente der Rechenschaftspflicht.

Schließlich sieht die DSGVO auch spezifische Instrumente – internationale Abkommen und Verwaltungsvereinbarungen, die von den Datenschutzbehörden genehmigt werden – vor, die von Behörden genutzt werden sollen, um personenbezogene Daten an ihre Partner in Drittländern oder an internationale Organisationen zu übermitteln. Der Ausschuss hat Leitlinien zu den Garantien angenommen, die in solche Instrumente[195] aufgenommen werden sollten. Leitlinien dieser Art können die Aushandlung solcher Abkommen und Vereinbarungen unterstützen.

7.1.3 Sicherstellung der Komplementarität mit anderen Politikbereichen

Da der Datenverkehr für so zahlreiche Tätigkeiten unerlässlich geworden ist, muss unbedingt sichergestellt werden, dass die Datenschutzpolitik und andere Politikbereiche einander ergänzen. Die Aufnahme von Datenschutzgarantien in internationale Instrumente ist nicht nur häufig eine Voraussetzung für den Datenverkehr, sondern auch eine wichtige Voraussetzung für eine stabile und vertrauenswürdige Zusammenarbeit.

So sind beispielsweise internationale Abkommen, die die erforderlichen Datenschutzgarantien vorsehen, unter anderem durch die Sicherstellung der Kontinuität des Schutzes seitens der ersuchenden Behörde, von entscheidender Bedeutung, um für entgegenkommendes Verhalten zu sorgen und den grenzüberschreitenden Zugang der Strafverfolgungsbehörden zu elektronischen Beweismitteln, die sich im Besitz von Unternehmen befinden, zu erleichtern und auf diese Weise eine wirksamere Kriminalitätsbekämpfung zu ermöglichen. Dieser Ansatz schlägt sich im Zweiten Zusatzprotokoll zum Übereinkommen über Computerkriminalität[196] nieder, das die bestehenden Vorschriften für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln bei strafrechtlichen Ermittlungen verbessert und gleichzeitig angemessene Datenschutzgarantien sicherstellt. Das Protokoll wurde inzwischen von mehreren EU-Mitgliedstaaten unterzeichnet. Auch die bilateralen Verhandlungen zwischen der EU und

(192) Beitrag des Ausschusses, S. 9.
(193) Zusammenfassung der Rückmeldungen der Multi-Stakeholder-Expertengruppe zur DSGVO.
(194) Leitlinien 07/2022 und Leitlinien 04/2021 des EDSA.
(195) EDSA-Leitlinien 2/2020.
(196) Zweites Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Verstärkung der Zusammenarbeit und der Weitergabe von elektronischem Beweismaterial (SEV Nr. 224).

den USA über ein Abkommen über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die Zusammenarbeit in Strafsachen kommen voran.[197]

Der Austausch von Fluggastdatensätzen (PNR-Daten) ist ein weiterer Bereich der EU-Sicherheitspolitik, der von der Entwicklung strenger Datenschutzgarantien profitiert hat. Im Jahr 2023 schlossen die EU und Kanada im Einklang mit den Anforderungen, die der Gerichtshof in seiner Stellungnahme 1/15 dargelegt hatte, ihre Verhandlungen über ein neues PNR-Abkommen ab.[198] Ähnliche Garantien wurden in das PNR-Kapitel des Handels- und Kooperationsabkommens zwischen der EU und dem Vereinigten Königreich aufgenommen. Die Aufnahme eines verstärkten Schutzes der Privatsphäre in diese Abkommen, die als Muster für künftige Abkommen mit anderen Partnern dienen können, schafft Rechtssicherheit für die Luftfahrtunternehmen und sorgt gleichzeitig für die Stabilität eines wichtigen Informationsaustauschs zur Bekämpfung des Terrorismus und anderer schwerer grenzüberschreitender Kriminalität.

Die Kommission setzt sich ferner für strenge Bestimmungen zum Schutz der Privatsphäre und zur Förderung des digitalen Handels in der Welthandelsorganisation in den laufenden Verhandlungen über die Initiative für eine gemeinsamen Erklärung zum elektronischen Geschäftsverkehr ein. Ähnliche Bestimmungen zur Bekämpfung ungerechtfertigter Hindernisse für den digitalen Handel bei gleichzeitigem Schutz des erforderlichen politischen Spielraums der Vertragsparteien im Bereich des Datenschutzes wurden konsequent in die Freihandelsabkommen aufgenommen, die die EU nach Inkrafttreten der DSGVO geschlossen hat, insbesondere in das Handels- und Kooperationsabkommen zwischen der EU und dem Vereinigten Königreich und in die Abkommen mit Chile, Japan und Neuseeland. Bestimmungen über den Schutz der Privatsphäre und den Datenverkehr werden auch in den laufenden Verhandlungen über den digitalen Handel mit Singapur und Südkorea erörtert.

7.2 Internationale Zusammenarbeit im Bereich des Datenschutzes

7.2.1 Die bilaterale Dimension

Die Kommission hat den Dialog mit Ländern und internationalen Organisationen über die Entwicklung, Reform und Umsetzung von Datenschutzvorschriften fortgesetzt, unter anderem durch Beiträge zu öffentlichen Konsultationen über Gesetzesentwürfe oder Regulierungsmaßnahmen im Bereich des Datenschutzes[199], durch Anhörungen vor den zuständigen parlamentarischen Gremien[200] und durch die Teilnahme an speziellen Treffen mit Regierungsvertretern, parlamentarischen Delegationen und Regulierungsbehörden aus vielen Regionen der Welt[201]. Eine Reihe dieser Maßnahmen wurde im Rahmen des von der EU finanzierten Projekts „Verbesserter Datenschutz und Datenverkehr“ durchgeführt, mit dem Länder unterstützt werden, die moderne Datenschutzrahmen entwickeln oder die Kapazitäten ihrer Regulierungsbehörden stärken wollen, und zwar durch Schulungen, Wissensaustausch, Kapazitätsaufbau und den Austausch bewährter Verfahren. Die

(197) https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en.

(198) Vorschlag der Kommission für einen Beschluss des Rates über die Unterzeichnung – im Namen der Europäischen Union – eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (PNR-Daten), COM(2024) 94 final.

(199) Dies betraf beispielsweise von Australien, China, Ruanda, Argentinien, Brasilien, Äthiopien, Indonesien, Peru, Malaysia und Thailand organisierte Konsultationen.

(200) Beispielsweise vor den parlamentarischen Gremien Chiles, Ecuadors und Paraguays.

(201) Dazu gehörte auch die Organisation von Seminaren und Studienbesuchen, z. B. in Kenia, Indonesien und Singapur.

Kommission leistete zudem einen Beitrag zu anderen Initiativen wie der Digitalallianz EU-CELAC.

Ferner wird der Datenschutz weiterhin eine Schlüsselrolle bei der Arbeit der Kommission im Zusammenhang mit der Erweiterung spielen. Die EU-Datenschutzvorschriften sind ein wichtiger Bestandteil der Gesamtbemühungen der Erweiterungsländer um die Angleichung ihres Rechtsrahmens an den der EU (zumal die Verarbeitung und der Austausch personenbezogener Daten im Mittelpunkt zahlreicher politischer Maßnahmen stehen). Darüber hinaus sind die Unabhängigkeit und das ordnungsgemäße Funktionieren einer Datenschutzbehörde ein Schlüsselelement der allgemeinen Gewaltenteilung und der Rechtsstaatlichkeit und werden mit der schrittweisen Integration der Erweiterungsländer in den Binnenmarkt durch die EU (was in Initiativen wie dem Wachstumsplan für die westlichen Balkanländer vorgesehen ist) zunehmend an Bedeutung gewinnen.

Ein zunehmend wichtiger Aspekt des Dialogs der EU mit Drittländern besteht im Austausch zwischen den Regulierungsbehörden. Wie im Bericht 2020 angekündigt, hat die Kommission eine „Datenschutzakademie“ eingerichtet, um den Austausch zwischen Datenschutzbehörden der EU und Drittländern zu fördern und auf diese Weise zum Kapazitätsaufbau beizutragen und die Zusammenarbeit „vor Ort“ zu verbessern. Die Akademie bietet auf Ersuchen der Behörden von Drittländern maßgeschneiderte Schulungen an und bringt das Fachwissen von Vertretern der mit der Durchsetzung befassten Kreise, der Wissenschaft, des Privatsektors und der europäischen Einrichtungen zusammen. Der Mehrwert der Schulungen liegt in der Anpassung der verschiedenen Komponenten an die Interessen und Bedürfnisse der ersuchenden Behörde. Darüber hinaus ermöglichen diese Schulungen den Datenschutzbehörden der EU und von Drittländern, Kontakte zu knüpfen, Wissen zu teilen, Erfahrungen und bewährte Verfahren auszutauschen und potenzielle Bereiche für eine Zusammenarbeit zu ermitteln. Die Akademie hat bislang Schulungen für die Datenschutzbehörden Indonesiens, Brasiliens, Kenias, Nigerias und Ruandas angeboten und bereitet derzeit Schulungen für mehrere andere Länder vor.

Neben der Notwendigkeit, den Dialog zwischen den Regulierungsbehörden aufrechtzuerhalten, besteht – wie auch in den Rückmeldungen des Rates und des Ausschusses[202] festgestellt wird – immer mehr Bedarf daran, geeignete Rechtsinstrumente für eine engere Zusammenarbeit und gegenseitige Unterstützung zu entwickeln, unter anderem durch die Ermöglichung des erforderlichen Informationsaustauschs im Rahmen von Untersuchungen. Da Datenschutzverletzungen zunehmend grenzüberschreitende Auswirkungen haben, können sie häufig nur im Rahmen der Zusammenarbeit zwischen den Regulierungsbehörden der EU und von Drittländern wirksam untersucht und bekämpft werden. Die Kommission wird daher die Genehmigung zur Aufnahme von Verhandlungen zum Abschluss von Vereinbarungen über die Zusammenarbeit bei der Rechtsdurchsetzung mit den betreffenden Drittländern einholen (wie auch in Artikel 50 DSGVO vorgesehen). In diesem Zusammenhang nimmt die Kommission das Ersuchen des Ausschusses zur Kenntnis, speziell die Länder mit den meisten Wirtschaftsbeteiligten, die unmittelbar der DSGVO unterliegen, als potenzielle Partner in Betracht zu ziehen, insbesondere die G7-Länder und/oder Länder, die von Angemessenheitsbeschlüssen profitieren.[203]

Solche Kooperations- und Amtshilfeabkommen würden auch dazu beitragen, die Einhaltung und wirksame Durchsetzung durch ausländische Marktteilnehmer, die der DSGVO unterliegen, sicherzustellen, z. B. weil sie mit ihrem Angebot von Waren oder Dienstleistungen speziell auf den EU-Markt ausgerichtet sind. Der Rat stellt fest, dass es

([202]) Beitrag des Ausschusses, S. 8; Standpunkt und Feststellungen des Rates, Rn. 38.
([203]) Beitrag des Ausschusses, S. 8.

wichtig ist, die Einhaltung der DSGVO in solchen Fällen durchzusetzen, und äußert Bedenken hinsichtlich der gleichen Wettbewerbsbedingungen mit Einrichtungen in der EU sowie hinsichtlich des wirksamen Schutzes der Rechte des Einzelnen.[204] Die Kommission schließt sich der Forderung des Rates an, verschiedene Möglichkeiten zur Erleichterung der Durchsetzung in diesem Szenario zu prüfen. Zwar könnten formalere Arten der Zusammenarbeit mit den Regulierungsbehörden von Drittländern sicherlich eine wichtige Rolle spielen, doch sollten auch andere – bereits bestehende – Wege entschlossener genutzt werden. Dazu gehört die umfassende Nutzung des Instrumentariums für die Durchsetzung von Artikel 58 DSGVO und die Einbeziehung von Vertretern ausländischer Unternehmen in der EU (Benennung gemäß Artikel 27 DSGVO).

7.2.2 Die multilaterale Dimension

Die Kommission beteiligt sich auch weiterhin aktiv an einer Reihe internationaler Foren, um gemeinsame Werte zu fördern und auf regionaler und globaler Ebene Konvergenz zu schaffen.

Dazu gehört zum Beispiel ein aktiver Beitrag zur Arbeit des Beratenden Ausschusses zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108), dem einzigen rechtsverbindlichen multilateralen Instrument im Bereich des Schutzes personenbezogener Daten. Bislang haben 31 Staaten das Änderungsprotokoll zur Modernisierung des Übereinkommens 108[205] ratifiziert, darunter viele EU-Mitgliedstaaten sowie einige Nichtmitglieder des Europarats (Argentinien, Mauritius und Uruguay). Unter den EU-Mitgliedstaaten steht nur die Unterzeichnung durch einen Mitgliedstaat[206] noch aus, während acht Mitgliedstaaten[207] das modernisierte Übereinkommen bisher unterzeichnet, aber nicht ratifiziert haben. Die Kommission appelliert an den einen verbleibenden Mitgliedstaat, das modernisierte Übereinkommen zu unterzeichnen, und fordert die anderen nachdrücklich auf, die Ratifizierung zügig voranzutreiben, damit das Übereinkommen in naher Zukunft in Kraft treten kann. Darüber hinaus fördert die Kommission weiterhin aktiv den Beitritt von Drittländern.

Auf der Ebene der G20 und der G7 konzentrierten sich die Diskussionen über den Datenschutz und den Datenverkehr auf die Umsetzung des ursprünglich von Japan vorgeschlagenen Konzepts des vertrauensvollen, freien Datenverkehrs, das dem Umstand Rechnung trägt, dass Datenschutz und Sicherheit zum Vertrauen in die digitale Wirtschaft beitragen und den Datenverkehr erleichtern können.[208] Die OECD spielt in diesem Zusammenhang eine besonders wichtige Rolle, indem sie ein Forum für eine Expertengemeinschaft zum vertrauensvollen, freien Datenverkehr bietet, in der ein breites Spektrum von Interessenträgern (Regierungen, Regulierungsbehörden, Industrie, Zivilgesellschaft, Wissenschaft) zusammenkommen, um Beiträge zu spezifischen Projekten und Fragen im Zusammenhang mit dem vertrauensvollen, freien Datenverkehr zu leisten. Darüber hinaus ist ein wichtiges Ergebnis der Initiative zum vertrauensvollen, freien Datenverkehr, zu der die Kommission erheblich beigetragen hat, die Annahme einer Erklärung der OECD über den Zugang der Regierung zu personenbezogenen Daten, die von Unternehmen des privaten Sektors erhoben werden. Diese Erklärung ist das erste

---

([204]) Standpunkt und Feststellungen des Rates, Rn. 39.
([205]) Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 223).
([206]) Dänemark.
([207]) Belgien, Tschechien, Griechenland, Irland, Lettland, Luxemburg, Niederlande und Schweden.
([208]) Siehe z. B. https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communique-data.pdf?download=1.

internationale Instrument in diesem Bereich. Sie enthält eine Reihe gemeinsamer Anforderungen zum Schutz der Privatsphäre beim Zugriff auf personenbezogene Daten für die Zwecke der nationalen Sicherheit und der Strafverfolgung. Vor dem Hintergrund der zunehmenden weltweiten Erkenntnis, dass das Vertrauen in Datenübermittlungen durch einen unverhältnismäßigen staatlichen Zugang beeinträchtigt wird, ist diese Erklärung ein wichtiger Beitrag zur Erleichterung eines vertrauenswürdigen Datenverkehrs. Die Kommission wird die Länder weiterhin ermutigen, der Erklärung beizutreten, die auch Nicht-OECD-Mitgliedern offensteht.

Die Kommission arbeitet ferner mit verschiedenen regionalen Organisationen und Netzwerken zusammen, die gemeinsame Datenschutzgarantien gestalten. Dies gilt beispielsweise für den ASEAN, die Afrikanische Union, das Forum der asiatisch-pazifischen Datenschutzbehörden, das Iberoamerikanische Datenschutznetzwerk und das Netzwerk afrikanischer Datenschutzbehörden (NADPA – RADPD). Die Entwicklung des genannten EU-ASEAN-Leitfadens zu den Musterklauseln ist ein konkretes Beispiel für eine solche fruchtbare Zusammenarbeit.

Schließlich unterhält die Kommission einen Dialog mit verschiedenen internationalen Organisationen, unter anderem um zu prüfen, wie der Datenverkehr zwischen der EU und diesen Organisationen weiter erleichtert werden kann. Da viele Organisationen ihre Datenschutzrahmen in den letzten Jahren modernisiert haben oder dabei sind, ergeben sich auch neue Möglichkeiten für den Austausch von Erfahrungen und bewährten Verfahren. In diesem Zusammenhang haben sich die vom Europäischen Datenschutzbeauftragten organisierten jährlichen Workshops mit internationalen Organisationen und einer speziellen Taskforce für internationale Datenübermittlungen als besonders nützliche Foren erwiesen, um konkrete Instrumente für die Zusammenarbeit, einschließlich personenbezogener Daten, auszutauschen und auszuloten.[209]

8 SCHLUSSBEMERKUNG

In den sechs Jahren seit dem Geltungsbeginn der DSGVO hat diese Verordnung den Menschen die Möglichkeit gegeben, echte Kontrolle über ihre Daten auszuüben. Ebenso hat sie dazu beigetragen, gleiche Wettbewerbsbedingungen für Unternehmen zu schaffen, und einen Eckpfeiler für die zahlreichen Initiativen gebildet, die den digitalen Wandel in der EU vorantreiben.

Damit die beiden Ziele der DSGVO – ein starker Schutz des Einzelnen bei gleichzeitiger Sicherstellung des freien Verkehrs personenbezogener Daten innerhalb der EU und eines sicheren Datenverkehrs außerhalb der EU – vollständig erreicht werden, muss der Fokus auf folgende Elemente gerichtet werden:

- solide Durchsetzung der DSGVO, beginnend mit der raschen Annahme des Vorschlags der Kommission über Verfahrensregeln, um in Fällen, die Einzelpersonen in der gesamten EU betreffen, schnelle Rechtsbehelfe und Rechtssicherheit zu schaffen;
- aktive Unterstützung von Interessenträgern, insbesondere KMU und kleinen Marktteilnehmern, durch die Datenschutzbehörden bei ihren Bemühungen um Einhaltung der Vorschriften;
- einheitliche Auslegung und Anwendung der DSGVO in der gesamten EU;

(209) https://www.edps.europa.eu/protection-des-donnees/notre-travail/cepd-dans-le-monde/protection-des-donnees-et-organisations_de.

- wirksame Zusammenarbeit zwischen den Regulierungsbehörden sowohl auf nationaler als auch auf EU-Ebene, um die einheitliche und kohärente Anwendung des wachsenden Regelwerks der EU im digitalen Bereich sicherzustellen;
- weitere Förderung der internationalen Datenschutzstrategie der Kommission.

Um die wirksame Anwendung der DSGVO zu unterstützen und in weitere Überlegungen zum Datenschutz einfließen zu können, sind mehrere hier genannte Maßnahmen erforderlich. Die Kommission wird die Umsetzung dieser Maßnahmen auch im Hinblick auf den im Jahr 2028 anstehenden Bericht unterstützen und überwachen.

Entwicklung wirksamer Strukturen für die Zusammenarbeit

Das Europäische Parlament und der Rat werden ersucht, den Vorschlag über die Verfahrensregeln der DSGVO rasch anzunehmen.

Der Ausschuss und die Datenschutzbehörden werden ersucht,

- in Fragen, die sich auf den Datenschutz auswirken, eine regelmäßige Zusammenarbeit mit anderen sektoralen Regulierungsbehörden aufzunehmen, insbesondere mit den Behörden, die im Rahmen der neuen Rechtsvorschriften der EU im digitalen Bereich eingerichtet wurden, und sich aktiv an den Strukturen auf EU-Ebene zu beteiligen, die die Zusammenarbeit zwischen den Regulierungsbehörden erleichtern sollen;
- die in der DSGVO vorgesehenen Instrumente für die Zusammenarbeit umfassender zu nutzen, damit die Streitbeilegung nur als letztes Mittel genutzt wird;
- effizientere und gezieltere Arbeitsvereinbarungen für Leitlinien, Stellungnahmen und Beschlüsse umzusetzen und Schlüsselthemen zu priorisieren, um den Aufwand für die Datenschutzbehörden zu verringern und schneller auf Marktentwicklungen zu reagieren.

Die Mitgliedstaaten müssen

- die wirksame und vollständige Unabhängigkeit der nationalen Datenschutzbehörden sicherstellen;
- den Datenschutzbehörden ausreichende Ressourcen zur Verfügung stellen, damit sie ihre Aufgaben erfüllen können, insbesondere indem ihnen die technischen Ressourcen und das Fachwissen zur Verfügung gestellt werden, die für den Umgang mit neuen Technologien und die Wahrnehmung neuer Aufgaben im Rahmen der Rechtsvorschriften im digitalen Bereich erforderlich sind;
- die Datenschutzbehörden mit den Ermittlungsinstrumenten ausstatten, die sie benötigen, damit sie die in der DSGVO vorgesehenen Durchsetzungsbefugnisse wirksam nutzen können;
- den Dialog zwischen den Datenschutzbehörden und anderen nationalen Regulierungsbehörden unterstützen, insbesondere denjenigen, die im Rahmen der neuen digitalen Rechtsvorschriften eingerichtet wurden.

Die Kommission wird

- die rasche Annahme des Vorschlags über die Verfahrensregeln der DSGVO durch die beiden gesetzgebenden Organe aktiv unterstützen;
- die wirksame und vollständige Unabhängigkeit der nationalen Datenschutzbehörden weiterhin genau überwachen;
- auf der Grundlage von Erfahrungen Synergien und Kohärenz zwischen der DSGVO und allen Rechtsvorschriften, die die Verarbeitung personenbezogener Daten betreffen,

schaffen und erforderlichenfalls geeignete Maßnahmen ergreifen, um Rechtssicherheit zu schaffen;

- prüfen, wie der Notwendigkeit einer strukturierten und effizienten Zusammenarbeit zwischen den Regulierungsbehörden besser entsprochen werden kann, um die wirksame, konsequente und kohärente Anwendung der Digitalvorschriften der EU sicherzustellen, wobei die Zuständigkeit der Datenschutzbehörden für alle Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten zu achten ist.

Umsetzung und Ergänzung des Rechtsrahmens

Die Mitgliedstaaten müssen

- sicherstellen, dass die Datenschutzbehörden rechtzeitig konsultiert werden, bevor Rechtsvorschriften über die Verarbeitung personenbezogener Daten erlassen werden.

Die Kommission wird

- weiterhin alle ihr zur Verfügung stehenden Instrumente, einschließlich Vertragsverletzungsverfahren, nutzen, um sicherzustellen, dass die Mitgliedstaaten die DSGVO einhalten;
- weiterhin den Austausch von Meinungen und nationalen Verfahren zwischen den Mitgliedstaaten unterstützen, unter anderem im Rahmen der Sachverständigengruppe der Mitgliedstaaten zur DSGVO;
- Maßnahmen ergreifen, um sicherzustellen, dass Kinder im Internet geschützt, gestärkt und geachtet werden;
- über die möglichen nächsten Schritte in Bezug auf den Vorschlag für eine Verordnung über den Datenschutz in der elektronischen Kommunikation nachdenken, einschließlich ihrer Beziehung zur DSGVO.

Unterstützung der Interessenträger

Der Ausschuss und die Datenschutzbehörden werden ersucht,

- mit Verantwortlichen und Auftragsverarbeitern in einen konstruktiven Dialog über die Einhaltung der DSGVO einzutreten;
- weitere Anstrengungen zu unternehmen, um die Einhaltung der Vorschriften durch KMU zu unterstützen, indem maßgeschneiderte Leitlinien und Instrumente bereitgestellt, unbegründete Bedenken von KMU, deren Kerngeschäft nicht die Verarbeitung personenbezogener Daten ist, ausgeräumt und sie bei ihren Bemühungen zur Einhaltung der Vorschriften begleitet werden;
- die Umsetzung wirksamer Compliance-Maßnahmen durch Unternehmen, wie z. B. die Zertifizierung und Verhaltensregeln (auch als Instrumente für Übermittlungen), zu unterstützen, indem während des Genehmigungsverfahrens mit Interessenträgern zusammengearbeitet wird, klare Zeitpläne für Genehmigungen bereitgestellt werden und – wie in der Strategie 2024–2027 des Ausschusses zugesagt – den wichtigsten Gruppen von Interessenträgern erklärt wird, wie diese Instrumente genutzt werden können;
- sicherzustellen, dass die nationalen Leitlinien und die Anwendung der DSGVO auf nationaler Ebene mit den Leitlinien des Ausschusses und der Rechtsprechung des Gerichtshofs im Einklang stehen;
- unterschiedliche Auslegungen der DSGVO zwischen den Datenschutzbehörden zu beheben, auch zwischen Behörden innerhalb desselben Mitgliedstaats;

- präzise, praktische und für das jeweilige Publikum zugängliche Leitlinien bereitzustellen, wie in der Strategie 2024–2027 des Ausschusses zugesagt;
- eine frühzeitigere und aussagekräftigere Konsultation zu Leitlinien und Stellungnahmen sicherzustellen, um die Marktdynamik und geschäftlichen Gepflogenheiten besser zu verstehen, die eingegangenen Rückmeldungen angemessen zu berücksichtigen und die konkrete Anwendung der angenommenen Auslegungen einzubeziehen;
- die laufenden Arbeiten an den Leitlinien zu den Daten von Kindern, wissenschaftlicher Forschung, Anonymisierung, Pseudonymisierung und den berechtigten Interessen vorrangig abzuschließen;
- die Sensibilisierungs-, Informations- und Durchsetzungsmaßnahmen zu verstärken, um sicherzustellen, dass die Datenschutzbeauftragten ihre Aufgaben im Rahmen der DSGVO wahrnehmen können.

Die Kommission wird

- weiterhin finanzielle Unterstützung für Tätigkeiten der Datenschutzbehörden bereitstellen, die die Umsetzung der Verpflichtungen aus der DSGVO durch KMU erleichtern;
- alle verfügbaren Mittel nutzen, um zweckdienliche Klarstellungen zu Fragen zu liefern, die für die Interessenträger, einschließlich KMU, von Bedeutung sind, insbesondere indem der Ausschuss um Stellungnahmen ersucht wird.

Weiterentwicklung des Instrumentariums für Datenübermittlungen und internationale Zusammenarbeit

Der Ausschuss und die Datenschutzbehörden werden ersucht,

- die Arbeiten zur Straffung und Verkürzung des Genehmigungsverfahrens für verbindliche unternehmensinterne Vorschriften sowie zur Aktualisierung der Leitlinien zu den Aspekten, die in verbindlichen unternehmensinternen Vorschriften zu finden sind, abzuschließen;
- Möglichkeiten/Instrumente auszuloten, um Datenexporteure bei ihren Bemühungen um die Einhaltung der Schrems-II-Anforderungen weiter zu unterstützen;
- weitere Möglichkeiten zu prüfen, wie eine wirksame Durchsetzung gegen in Drittländern niedergelassene Betreiber, die in den räumlichen Anwendungsbereich der DSGVO fallen, sichergestellt werden kann.

Die Mitgliedstaaten müssen

- sicherstellen, dass das modernisierte Übereinkommen 108+ des Europarats so bald wie möglich unterzeichnet und ratifiziert wird, damit es in Kraft treten kann.

Die Kommission wird

- weitere Fortschritte bei den laufenden Angemessenheitsgesprächen erzielen, die Weiterentwicklung bestehender Angemessenheitsfeststellungen prüfen und neue Angemessenheitsdialoge mit interessierten Partnern führen;
- eine verstärkte Zusammenarbeit zwischen dem Netz von Ländern, die von Angemessenheitsbeschlüssen profitieren, unterstützen;
- die Arbeit an zusätzlichen Standardvertragsklauseln abschließen, insbesondere für Datenübermittlungen an Datenimporteure, deren Verarbeitung unmittelbar der

DSGVO unterliegt, und für Übermittlungen gemäß der Verordnung (EU) 2018/1725 für Datenübermittlungen durch Organe und Einrichtungen der EU;

- gemeinsam mit internationalen Partnern an der Erleichterung des Datenverkehrs auf der Grundlage von Mustervertragsklauseln arbeiten;
- laufende Reformprozesse in Drittländern zu neuen oder modernisierten Datenschutzvorschriften durch den Austausch von Erfahrungen und bewährten Verfahren unterstützen;
- mit internationalen und regionalen Organisationen wie der OECD und der G7 zusammenarbeiten, um einen auf hohen Datenschutzstandards basierenden, vertrauenswürdigen Datenverkehr zu fördern, auch im Rahmen des Ansatzes des „vertrauensvollen, freien Datenverkehrs“;
- den Austausch zwischen europäischen und internationalen Regulierungsbehörden erleichtern und unterstützen, unter anderem über ihre Datenschutzakademie;
- dazu beitragen, bei der Durchsetzung die internationale Zusammenarbeit zwischen den Aufsichtsbehörden zu erleichtern, unter anderem durch die Aushandlung von Kooperations- und Amtshilfeabkommen.