EUROPÄISCHE
KOMMISSION

Brüssel, den 24.6.2020
SWD(2020) 115 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

[…]

Begleitunterlage zur

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung

{COM(2020) 264 final}

Inhalt

1 HINTERGRUND

Die Datenschutz-Grundverordnung[1] (im Folgenden „DSGVO“) ist das Ergebnis von acht Jahren Vorbereitung, Ausarbeitung und interinstitutionellen Verhandlungen; sie gilt nach einem zweijährigen Übergangszeitraum (von Mai 2016 bis Mai 2018) ab dem 25. Mai 2018. Nach Artikel 97 der DSGVO ist die Kommission verpflichtet, über die Bewertung und Überprüfung der Verordnung Bericht zu erstatten, beginnend mit einem ersten Bericht nach zwei Jahren der Anwendung und danach alle vier Jahre.

Die Bewertung ist außerdem Teil eines vielschichtigen Ansatzes, den die Kommission bereits vor Beginn der Anwendung der DSGVO verfolgt hat und der seitdem weiterhin aktiv fortgeführt wird. Im Rahmen dieses Ansatzes führte die Kommission fortlaufend bilaterale Dialoge mit den Mitgliedstaaten über die Vereinbarkeit der nationalen Rechtsvorschriften mit der DSGVO, leistete einen aktiven Beitrag zur Arbeit des Europäischen Datenschutzausschusses (EDSA, im Folgenden „Ausschuss“), indem sie ihre Erfahrung und ihr Fachwissen zur Verfügung stellte, unterstützte die Datenschutzbehörden und unterhielt enge Kontakte mit einem breiten Spektrum von Interessenträgern im Hinblick auf die praktische Anwendung der Verordnung.

Die Bewertung stützt sich auf die Bestandsaufnahme, die die Kommission für das erste Anwendungsjahr der DSGVO durchgeführt hatte und die in der Mitteilung vom Juli 2019[2] zusammengefasst ist. Sie befasst sich außerdem mit der Nachverfolgung der Feststellungen in der Mitteilung über die Anwendbarkeit der DSGVO vom Januar 2018[3]. Des Weiteren veröffentlichte die Kommission im September 2018 einen Leitfaden zur Verwendung personenbezogener Daten im Zusammenhang mit Wahlen sowie im April 2020 Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie.

Obgleich der Schwerpunkt dieser Bewertung auf den beiden in Artikel 97 Absatz 2 der DSGVO genannten Themenbereichen liegt, nämlich auf internationalen Datenübermittlungen und den Verfahren der Zusammenarbeit und Kohärenz, wird hierbei ein umfassenderer Ansatz verfolgt, um Fragen zu behandeln, die in den letzten beiden Jahren von verschiedenen Akteuren angesprochen wurden.

Bei der Vorbereitung der Bewertung berücksichtigte die Kommission

- Beiträge des Rates,[4]

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

[2] Mitteilung der Kommission an das Europäische Parlament und den Rat: Datenschutzvorschriften als Voraussetzung für Vertrauen in die EU und darüber hinaus – eine Bilanz (COM(2019) 374 final, 24.7.2019).

[3] Mitteilung der Kommission an das Europäische Parlament und den Rat: Besserer Schutz und neue Chancen – Leitfaden der Kommission zur unmittelbaren Anwendbarkeit der Datenschutz–Grundverordnung ab 25. Mai 2018 (COM(2018) 043 final).

[4] Standpunkt und Feststellungen des Rates zur Anwendung der Datenschutz-Grundverordnung (DSGVO), 14994/2/19 REV 2, 15.1.2020: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/de/pdf.

- Beiträge des Europäischen Parlaments (Ausschuss für bürgerliche Freiheiten, Justiz und Inneres),[5]
- Beiträge des Europäischen Datenschutzausschusses[6] und einzelner Datenschutzbehörden[7] auf der Grundlage eines von der Kommission übermittelten Fragebogens,
- Rückmeldungen der Mitglieder der Multi-Stakeholder-Expertengruppe zur Unterstützung der Anwendung der DSGVO[8], ebenfalls auf der Grundlage eines von der Kommission übermittelten Fragebogens
- und Ad-hoc-Beiträge, die von Interessenträgern eingingen.

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

Mit der DSGVO wurde ein innovatives Verwaltungssystem eingeführt und die Grundlage für eine echte europäische Datenschutzkultur geschaffen, die nicht nur eine harmonisierte Auslegung von Datenschutzvorschriften, sondern auch ihre harmonisierte Anwendung und Durchsetzung gewährleisten soll. Die entsprechenden Säulen sind die unabhängigen nationalen Datenschutzbehörden und der neu eingerichtet Europäische Datenschutzausschuss.

Da die Datenschutzbehörden für das Funktionieren des gesamten Datenschutzsystems der Union von entscheidender Bedeutung sind, beobachtet die Kommission aufmerksam deren tatsächliche Unabhängigkeit, auch in Bezug auf angemessene finanzielle, personelle und technische Ressourcen.

Angesichts des bisherigen kurzen Erfahrungszeitraums ist es noch zu früh, um die Funktionsweise der Verfahren der Zusammenarbeit und Kohärenz umfassend zu bewerten.[9] Darüber hinaus haben die Datenschutzbehörden noch nicht alle in der DSGVO vorgesehenen Instrumente genutzt, um ihre Zusammenarbeit weiter zu verstärken.

2.1 Nutzung der verstärkten Befugnisse der Datenschutzbehörden

Mit der DSGVO werden unabhängige Datenschutzbehörden eingerichtet und mit harmonisierten und verstärkten Durchsetzungsbefugnissen ausgestattet. Seit der

---

[5] Schreiben des LIBE-Ausschusses des Europäischen Parlaments vom 21. Februar 2020 an Kommissionsmitglied Reynders, Az.: IPOL-COM-LIBE D (2020)6525.

[6] Beitrag des Ausschusses zur Bewertung der DSGVO nach Artikel 97, angenommen am 18. Februar 2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en.

[7] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

[8] Die von der Kommission für die DSGVO eingesetzte Multi-Stakeholder-Expertengruppe besteht aus Vertreterinnen und Vertretern der Zivilgesellschaft, Wirtschaft, Wissenschaft und Praxis: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=DE.
Der Bericht der Multi-Stakeholder-Expertengruppe ist abrufbar unter: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356.

[9] Diese Tatsache wird insbesondere auch vom Rat in seinem Standpunkt und seinen Feststellungen zur Anwendung der DSGVO sowie vom Ausschuss in seinem Beitrag zur Bewertung betont.

Anwendung der DSGVO haben die Datenschutzbehörden von einer Vielzahl der darin vorgesehenen Abhilfebefugnisse Gebrauch gemacht, z. B. Geldbußen (22 EU-/EWR-Behörden)[10], Warnungen und Verwarnungen (23), Anordnungen, den Anträgen betroffener Personen zu entsprechen (26), Anordnungen, Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen (27), und Anordnungen zur Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten (17). Rund die Hälfte der Datenschutzbehörden (13) haben eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, verhängt. Dies belegt eine bewusste Anwendung aller in der DSGVO vorgesehenen Abhilfemaßnahmen; die Datenschutzbehörden sind nicht davor zurückgeschreckt, zusätzlich zu anderen Abhilfemaßnahmen oder an deren Stelle je nach Umständen des Einzelfalls Geldbußen zu verhängen.

Geldbußen:

Zwischen dem 25. Mai 2018 und dem 30. November 2019 verhängten 22 EU-/EWR-Datenschutzbehörden Geldbußen in rund 785 Fällen. Nur wenige Behörden haben bisher noch keine Geldbußen verhängt, obwohl derzeit laufende Verfahren zu solchen Geldbußen führen könnten. Die meisten Geldbußen wurden wegen Verstößen gegen den Grundsatz der Rechtmäßigkeit, gegen die Einholung einer gültigen Einwilligung, gegen den Schutz sensibler Daten, gegen die Pflicht zur Transparenz und gegen die Rechte der betroffenen Personen sowie aufgrund der Verletzung des Schutzes personenbezogener Daten verhängt.

Beispiele von Geldbußen, die von den Datenschutzbehörden verhängt wurden, umfassen:[11]

- 200 000 EUR wegen des Verstoßes gegen das Recht, Widerspruch gegen Direktwerbung einzulegen, in Griechenland;
- 220 000 EUR gegen ein Datenvermittlungsunternehmen in Polen wegen unterlassener Unterrichtung der betroffenen Personen über die Verarbeitung ihrer Daten;
- 250 000 EUR gegen die spanische Fußballliga LaLiga wegen fehlender Transparenz bei der Gestaltung ihrer Smartphone-App;
- 14,5 Mio. EUR wegen Verletzung der Datenschutzgrundsätze, insbesondere der rechtswidrigen Speicherung, durch ein deutsches Immobilienunternehmen;
- 18 Mio. EUR wegen der rechtswidrigen Verarbeitung besonderer Kategorien von Daten in großem Umfang durch österreichische Postdienste;
- 50 Mio. EUR gegen Google in Frankreich im Zusammenhang mit den Bedingungen für die Einholung der Einwilligung von Nutzern.

[10] Die Zahlen in Klammern geben die Zahl der Datenschutzbehörden in der Europäischen Union und im Europäischen Wirtschaftsraum an, die zwischen Mai 2018 und Ende November 2019 von der aufgeführten Befugnis Gebrauch gemacht haben. Siehe Beitrag des Ausschusses auf den Seiten 32 und 33.

[11] Mehrere Beschlüsse über die Verhängung von Geldbußen unterliegen noch einer gerichtlichen Überprüfung.

Der Erfolg der DSGVO sollte nicht an der Zahl der verhängten Geldbußen gemessen werden, da die Verordnung eine breitere Palette von Abhilfebefugnissen vorsieht. Je nach Umständen kann beispielsweise die abschreckende Wirkung eines Verbots der Verarbeitung von Daten oder der Aussetzung der Übermittlung von Daten viel stärker sein.

Für den öffentlichen Sektor relevante spezifische Aspekte

Laut der DSGVO können die Mitgliedstaaten festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen Geldbußen verhängt werden können. Sofern Mitgliedstaaten von dieser Möglichkeit Gebrauch machen, hindert das die Datenschutzbehörden nicht daran, alle anderen Abhilfebefugnisse gegenüber Behörden und öffentlichen Stellen auszuüben.[12]

Ein weiterer spezifischer Aspekt ist die Aufsicht über die Gerichte. Die DSGVO gilt zwar auch für die Tätigkeiten der Gerichte, jedoch sind diese von der Aufsicht durch die Datenschutzbehörden ausgenommen, wenn sie im Rahmen ihrer justiziellen Tätigkeit handeln. Gemäß der Charta der Grundrechte der Europäischen Union und dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) sind die Mitgliedstaaten verpflichtet, eine unabhängige Stelle innerhalb ihres Justizsystems mit der Aufsicht über solche Verarbeitungsvorgänge zu betrauen.[13]

Zusammenarbeit mit anderen Regulierungsbehörden

Wie in ihrer Mitteilung vom Juli 2019 angekündigt, unterstützt die Kommission das Zusammenspiel mit anderen Regulierungsbehörden unter voller Achtung ihrer jeweiligen Zuständigkeiten. Vielversprechende Bereiche für die Zusammenarbeit sind unter anderem der Verbraucherschutz und der Wettbewerb. Der Ausschuss bekundete seine Bereitschaft, mit anderen Regulierungsbehörden zusammenzuarbeiten, insbesondere in Bezug auf die Marktkonzentration auf den digitalen Märkten.[14] Die Kommission erkannte die Bedeutung des Schutzes der Privatsphäre und des Datenschutzes als qualitativer Parameter für den Wettbewerb an.[15] Die Ausschussmitglieder nahmen an gemeinsamen Workshops mit dem Netzwerk für die Zusammenarbeit im Verbraucherschutz zum Thema Zusammenarbeit für eine bessere Durchsetzung von Rechtsvorschriften im Bereich Verbraucher- und Datenschutz in der EU teil. Dieser Ansatz wird verfolgt, um ein gemeinsames Verständnis zu fördern und praktische Wege zur Lösung konkreter Probleme zu entwickeln, mit denen Verbraucher insbesondere in der digitalen Wirtschaft konfrontiert sind.

Zur Gewährleistung eines kohärenten Ansatzes für den Schutz der Privatsphäre und den Datenschutz ist bis zur Annahme der e-Datenschutz-Verordnung eine enge Zusammenarbeit mit den Behörden unerlässlich, die für die Durchsetzung der e-Datenschutz-Richtlinie[16] – die Lex specialis im Bereich der elektronischen

---

12 Artikel 83 Absatz 7 der DSGVO.

13 Artikel 8 Absatz 3 der Charta; Artikel 16 Absatz 2 AEUV; Erwägungsgrund 20 der DSGVO.

14 Vgl. Erklärung des Europäischen Datenschutzausschusses (EDPB) zu den datenschutzbezogenen Auswirkungen von Unternehmenszusammenschlüssen (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_de.pdf).

15 Siehe Rechtssache COMP/M.8124, Microsoft/LinkedIn.

16 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen

Kommunikation – zuständig sind. Eine engere Zusammenarbeit mit den nach der NIS-Richtlinie[17] zuständigen Behörden und der NIS-Kooperationsgruppe wäre sowohl für die betreffenden Behörden als auch für die Datenschutzbehörden von gegenseitigem Vorteil.

2.2 Verfahren der Zusammenarbeit und Kohärenz

Mit der DSGVO wurden das Verfahren der Zusammenarbeit (ein zentrales System für Wirtschaftsteilnehmer, gemeinsame Maßnahmen und Amtshilfe zwischen den Datenschutzbehörden) und das Kohärenzverfahren geschaffen. Ziel war die Förderung der einheitlichen Anwendung der Datenschutzvorschriften, indem eine kohärente Auslegung und die Beilegung etwaiger Meinungsverschiedenheiten zwischen den Behörden durch den Ausschuss gewährleistet werden.

Der Ausschuss, dem alle Datenschutzbehörden angehören, wurde als Einrichtung der Union mit eigener Rechtspersönlichkeit geschaffen, ist voll funktionsfähig und wird durch ein Sekretariat[18] unterstützt. Er ist für das Funktionieren der beiden oben genannten Verfahren von entscheidender Bedeutung. Bis Ende 2019 hatte der Ausschuss 67 Dokumente angenommen, darunter 10 neue Leitlinien[19] und 43 Stellungnahmen[2021].

Die wichtige Rolle des Ausschusses wurde deutlich, als die Notwendigkeit bestand, schnell für eine einheitliche Auslegung der DSGVO zu sorgen und nach sofort anwendbaren Lösungen auf EU-Ebene zu suchen. Beispielsweise nahm der Ausschuss im Zusammenhang mit dem Ausbruch der COVID-19-Pandemie im März 2020 eine Stellungnahme in Bezug auf die Verarbeitung personenbezogener Daten[22] an, die sich unter anderem mit der Rechtmäßigkeit der Verarbeitung und der diesbezüglichen Nutzung mobiler Standortdaten befasste. Im April 2020 nahm der Ausschuss zwei weitere Leitlinien an, zum einen Leitlinien für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch[23] sowie Leitlinien für die Verwendung von Standortdaten und Tools zur

---

Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

17 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

18 Einzelheiten zu den Aufgaben des Sekretariats sind dem Beitrag des Ausschusses zu entnehmen, S. 24-26.

19 Ergänzend zu den zehn Leitlinien, die von der Artikel-29-Datenschutzgruppe im Vorfeld der Anwendung der DSGVO angenommen und vom Ausschuss gebilligt wurden. Darüber hinaus hat der Ausschuss zwischen Januar und Ende Mai 2020 vier weitere Leitlinien angenommen und ein bestehendes Leitliniendokument aktualisiert.

20 42 dieser Stellungnahmen wurden nach Artikel 64 der DSGVO und eine nach Artikel 70 Absatz 1 Buchstabe s der DSGVO angenommen und betrafen den Angemessenheitsbeschluss in Bezug auf Japan.

21 Ein vollständiger Überblick über die Tätigkeiten des Ausschusses ist im Beitrag des Ausschusses auf den Seiten 18-23 zu finden.

22 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

23 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_de.pdf

Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19[24]. Darüber hinaus leistete der Ausschuss einen wichtigen Beitrag zur Gestaltung des von der Kommission und den Mitgliedstaaten erarbeiteten EU-Ansatzes für Tracing-Apps.

Die tägliche Zusammenarbeit zwischen den Datenschutzbehörden erfolgt auf der Grundlage des Informationsaustauschs und der Meldungen über von den Behörden eingeleitete Fälle, unabhängig davon, ob die Behörden in eigener Funktion oder als Mitglieder des Ausschusses handeln. Um die Kommunikation zwischen den Behörden zu erleichtern, hat die Kommission erhebliche Unterstützung durch die Bereitstellung eines Systems für den Informationsaustausch[25] geleistet. Die meisten Behörden sind der Auffassung, dass dieses System den Erfordernissen der Verfahren der Zusammenarbeit und Kohärenz entspricht, auch wenn eine weitere Feinabstimmung vorgenommen werden könnte, um es z. B. benutzerfreundlicher zu gestalten.

Obwohl der Prozess noch am Anfang steht, lassen sich bereits einige Erfolge und Herausforderungen ermitteln, die nachstehend dargelegt werden. Sie zeigen, dass die Datenschutzbehörden die Instrumente der Zusammenarbeit bisher wirksam genutzt haben, jedoch flexiblere Lösungen bevorzugen würden.

Ein zentrales Verfahren

Generell kann die Datenschutzbehörde eines Mitgliedstaats in grenzüberschreitenden Fällen entweder als i) federführende Behörde beteiligt sein, wenn sich die Hauptniederlassung des Wirtschaftsteilnehmers in diesem Mitgliedstaat befindet, oder ii) als betroffene Behörde, wenn der Wirtschaftsteilnehmer eine Niederlassung im Hoheitsgebiet dieses Mitgliedstaats hat, wenn die Verarbeitung erhebliche Auswirkungen auf Personen in diesem Mitgliedstaat hat oder wenn bei diesen Behörden eine Beschwerde eingereicht wurde.

Diese enge Zusammenarbeit ist inzwischen tägliche Praxis der Behörden: Seit Geltungsbeginn der DSGVO wurden Datenschutzbehörden in allen Mitgliedstaaten in grenzüberschreitenden Fällen zu irgendeinem Zeitpunkt entweder als federführende Behörde oder als betroffene Behörde festgelegt, wenn auch in unterschiedlichem Umfang.

Von Mai 2018 bis Ende 2019 fungierte die Datenschutzbehörde in Irland bei den meisten grenzüberschreitenden Fällen als federführende Behörde (127), gefolgt von Deutschland (92), Luxemburg (87), Frankreich (64) und den Niederlanden (45). Diese Rangfolge spiegelt vor allem die besondere Situation in Irland und Luxemburg wider, in denen mehrere große multinationale Technologieunternehmen ansässig sind.

Was die Beteiligung einer Datenschutzbehörde als betroffene Behörde anbelangt, ist die Rangfolge eine andere, wobei die Behörden in Deutschland an den meisten Fällen beteiligt sind (435), gefolgt von Spanien (337), Dänemark (327), Frankreich (332) und Italien (306).[26]

---

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf

[25] Binnenmarkt-Informationssystem („IMI“).

[26] Siehe Beitrag des Ausschusses, S. 8.

Zwischen dem 25. Mai 2018 und dem 31. Dezember 2019 wurden 141 Beschlussentwürfe im Wege des Verfahrens der Zusammenarbeit und Kohärenz vorgelegt, von denen 79 in endgültigen Beschlüssen mündeten. Zum Zeitpunkt der Veröffentlichung dieses Berichts standen mehrere wichtige Beschlüsse mit grenzüberschreitender Dimension, die dem Verfahren der Zusammenarbeit und Kohärenz unterliegen, noch aus. Einige dieser Beschlüsse betreffen große multinationale Technologieunternehmen.[27] Es wird erwartet, dass diese Beschlüsse Klarheit bringen und zu einer stärkeren Harmonisierung bei der Auslegung der DSGVO beitragen werden.

Gegenseitige Amtshilfe

Das Amtshilfeinstrument wurde von den Datenschutzbehörden umfassend genutzt.

Bis Ende 2019 gab es 115 Amtshilfeverfahren[28], insbesondere zur Durchführung von Untersuchungen, wobei in der Mehrheit der Fälle Amtshilfe ausgehend von den Datenschutzbehörden Spaniens (26), Deutschlands (20), Dänemarks (13), Polens (12) und der Tschechischen Republik (10) ersucht wurde. Andererseits gingen in Irland (19), Frankreich (11), Österreich (10), Deutschland (10) und Luxemburg (9) die meisten Amtshilfeersuchen ein.[29]

Die große Mehrheit der Behörden erachtet die Amtshilfe als ein sehr nützliches Instrument der Zusammenarbeit und hat keine besonderen Hindernisse bei der Anwendung des Amtshilfeverfahrens erfahren. Der freiwillige Austausch im Rahmen der Amtshilfe, für den weder eine gesetzliche Frist noch eine strikte Antwortpflicht besteht, wurde häufiger genutzt, in 2427 Verfahren. Die Datenschutzbehörde Irlands übermittelte und erhielt die meisten Amtshilfeersuchen (527 übermittelte und 359 eingegangene), gefolgt von den deutschen Behörden (260 übermittelte und 356 eingegangene).

Andererseits wurden bisher noch keine gemeinsamen Maßnahmen[30] durchgeführt, die Datenschutzbehörden mehrerer Mitgliedstaaten bei grenzüberschreitenden Fällen bereits in der Untersuchungsphase eine Beteiligung ermöglichen würden. Der Ausschuss stellt weiterhin Überlegungen hinsichtlich der praktischen Umsetzung dieses Instruments sowie der Förderung seiner Anwendung an.

Kohärenzverfahren

Bisher wurde nur der erste Teil des Kohärenzverfahrens genutzt, und zwar die Annahme von Stellungnahmen des Ausschusses.[31] Dagegen wurden bisher weder eine Streitbeilegung durch den Ausschuss[32] noch Dringlichkeitsverfahren[33] eingeleitet.

---

27 Beispielsweise hat die irische Datenschutzbehörde am 22. Mai 2020 anderen betroffenen Behörden gemäß Artikel 60 der DSGVO einen Beschlussentwurf über eine Untersuchung gegen Twitter International Company aufgrund der Meldung einer Datenschutzverletzung vorgelegt. An demselben Tag gab die irische Datenschutzbehörde ebenfalls bekannt, dass ein Beschlussentwurf bezüglich WhatsApp Ireland Limited zur Vorlage nach Artikel 60 in Vorbereitung sei, der die Transparenz betreffe, darunter auch die Transparenz bezüglich der Frage, welche Informationen mit Facebook geteilt werden.

28 Artikel 61 der DSGVO.

29 Siehe Beitrag des Ausschusses, S. 12-14.

30 Artikel 62 der DSGVO.

31 Auf der Grundlage von Artikel 64 der DSGVO.

Zwischen dem 25. Mai 2018 und dem 31. Dezember 2019 gab der Ausschuss im Zusammenhang mit dem Erlass von Maßnahmen durch eines seiner Mitglieder 36 Stellungnahmen ab.[34] Die meisten von ihnen (31) betrafen die Annahme nationaler Listen von Verarbeitungsvorgängen, die eine Datenschutz-Folgenabschätzung erfordern. Zwei Stellungnahmen betrafen verbindliche interne Datenschutzvorschriften, zwei weitere bezogen sich auf Entwürfe von Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln und eine betraf Standardvertragsklauseln[35].

Des Weiteren nahm der Ausschuss auf Antrag sechs Stellungnahmen an.[36] Drei dieser Stellungnahmen betrafen nationale Listen, in denen Verarbeitungsvorgänge aufgeführt sind, die keine Datenschutz-Folgenabschätzung erfordern. Die anderen befassten sich mit einer Verwaltungsvereinbarung für die Übermittlung personenbezogener Daten zwischen Finanzaufsichtsbehörden innerhalb des Europäischen Wirtschaftsraums (EWR) und Finanzaufsichtsbehörden außerhalb des EWR, dem Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO bzw. der Zuständigkeit einer Aufsichtsbehörde im Falle einer Veränderung von Umständen, die die Hauptniederlassung oder die einzige Niederlassung betrifft.[37]

Anstehende Herausforderungen

Obwohl die Datenschutzbehörden im Ausschuss äußerst aktiv zusammengearbeitet haben und die Amtshilfe als Instrument der Zusammenarbeit bereits intensiv nutzen, ist der Aufbau einer echten gemeinsamen Datenschutzkultur weiterhin ein fortlaufender Prozess.

Vor allem die Bearbeitung grenzüberschreitender Fälle erfordert einen effizienteren und stärker harmonisierten Ansatz sowie die wirksame Nutzung aller in der DSGVO vorgesehenen Instrumente der Zusammenarbeit. In diesem Punkt besteht ein sehr breiter Konsens, da dieses Problem vom Europäischen Parlament, vom Rat, vom Europäischen Datenschutzbeauftragten, von Interessenträgern (innerhalb und außerhalb der Multi-Stakeholder-Gruppe) und von den Datenschutzbehörden auf unterschiedliche Weise angesprochen wurde.

Zu den wichtigsten Fragen, die diesbezüglich angegangen werden müssen, gehören Unterschiede in folgenden Bereichen:

- nationale Verwaltungsverfahren, insbesondere in Bezug auf Beschwerdeverfahren, Zulässigkeitskriterien für Beschwerden, Verfahrensdauer aufgrund unterschiedlicher oder fehlender Fristen, Zeitpunkt im Verfahren, zu dem der Anspruch auf rechtliches Gehör gewährt wird, Unterrichtung und Einbeziehung von Beschwerdeführern während des Verfahrens,
- Auslegungen von Begriffen im Zusammenhang mit dem Verfahren der Zusammenarbeit, wie zweckdienliche Informationen, der Begriff „unverzüglich“,

---

[32] Artikel 65 der DSGVO.
[33] Artikel 66 der DSGVO.
[34] Nach Artikel 64 Absatz 1 der DSGVO.
[35] Artikel 28 Absatz 8 der DSGVO.
[36] Nach Artikel 64 Absatz 2 DSGVO.
[37] Siehe Beitrag des Ausschusses, S. 15.

„Beschwerde“, das als „Beschlussentwurf“ der federführenden Datenschutzbehörde definierte Dokument, gütliche Einigung (insbesondere das Verfahren, das zu einer gütlichen Einigung führt, und die Rechtsform des Vergleichs) und

- die Vorgehensweise dahingehend, wann das Verfahren der Zusammenarbeit einzuleiten, die betroffenen Datenschutzbehörden einzubeziehen und Informationen an diese Behörden zu übermitteln sind. Mehrere Mitglieder der Multi-Stakeholder-Gruppe betonten, dass es den Beschwerdeführern auch an Klarheit dahingehend mangele, wie ihre Fälle in grenzüberschreitenden Situationen behandelt werden. Darüber hinaus weisen Unternehmen darauf hin, dass die nationalen Datenschutzbehörden in bestimmten Situationen keine Fälle an die federführende Datenschutzbehörde verwiesen, sondern sie als lokale Fälle behandelt haben.

Die Kommission begrüßt die Ankündigung des Ausschusses, Überlegungen dahingehend anzustellen, wie diese Bedenken ausgeräumt werden können. Insbesondere gab der Ausschuss an, dass er die Verfahrensschritte bei der Zusammenarbeit zwischen der federführenden Datenschutzbehörde und den betroffenen Datenschutzbehörden klären, die nationalen Verwaltungsverfahrensgesetze analysieren, auf eine gemeinsame Auslegung der Schlüsselbegriffe hinarbeiten und die Kommunikation und Zusammenarbeit (einschließlich gemeinsamer Maßnahmen) verstärken werde. Die Überlegungen und Analysen des Ausschusses sollten zur Entwicklung effizienterer Arbeitsvereinbarungen in grenzüberschreitenden Fällen[38] führen, unter anderem durch die Nutzung des Fachwissens seiner Mitglieder und durch eine stärkere Einbeziehung des Sekretariats. Darüber hinaus sei darauf hingewiesen, dass die Verantwortung des Ausschusses, eine einheitliche Auslegung der DSGVO sicherzustellen, nicht lediglich dadurch erfüllt werden kann, dass der niedrigste gemeinsame Nenner gefunden wird.

Schließlich muss der Ausschuss als Einrichtung der Union auch das Unionsverwaltungsrecht anwenden und für Transparenz im Entscheidungsprozess sorgen.

2.3 Beratung und Leitlinien

Verstärkte Sensibilisierung und Beratung durch die Datenschutzbehörden

Mehrere Datenschutzbehörden haben neue Instrumente geschaffen, z. B. Leitfäden für Einzelpersonen und Unternehmen und Instrumentarien für Unternehmen.[39] Viele Wirtschaftsteilnehmer begrüßen die pragmatische Vorgehensweise, die diese Behörden bei der Unterstützung zur Anwendung der DSGVO gezeigt haben. Insbesondere haben mehrere von ihnen aktiv und eng mit den Datenschutzbeauftragten zusammengearbeitet und mit ihnen kommuniziert, wobei diese Zusammenarbeit zum Teil auch über die Verbände von Datenschutzbeauftragten lief. Um die Datenschutzbeauftragten bei ihrer täglichen Arbeit zu unterstützen, haben viele Behörden auch Leitlinien herausgegeben, in denen die Funktion und die

[38] Wie auch im Standpunkt und in den Feststellungen des Rates dargelegt.
[39] Nähere Einzelheiten dazu siehe Abschnitt 7.

Pflichten der Datenschutzbeauftragten behandelt werden, und speziell für sie konzipierte Seminare veranstaltet. Dies ist jedoch nicht bei allen Datenschutzbehörden der Fall.

Die Rückmeldungen von Interessenträgern deuten auch auf eine Reihe von Problemen in Bezug auf Orientierungshilfe und Beratung hin:

- das Fehlen eines kohärenten Ansatzes und einheitlicher Leitlinien zwischen den nationalen Datenschutzbehörden zu bestimmten Fragen (z. B. zu Cookies[40], zur Anwendung berechtigter Interessen, zur Meldung von Datenschutzverletzungen oder zu Datenschutz-Folgenabschätzungen) oder selbst zwischen den Datenschutzbehörden in demselben Mitgliedstaat (z. B. in Deutschland in Bezug auf die Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“);
- eine mangelnde Übereinstimmung der auf nationale Ebene angenommenen Leitlinien mit den vom Ausschuss angenommenen Leitlinien;
- das Fehlen öffentlicher Konsultationen zu bestimmten auf nationaler Ebene angenommenen Leitlinien;
- unterschiedliche Ebenen der Einbeziehung von Interessenträgern bei den Datenschutzbehörden;
- Verzögerungen bei der Antwort auf Auskunftsersuchen;
- Schwierigkeiten bei der Einholung praktischer und wertvoller Ratschläge von Datenschutzbehörden;
- die Notwendigkeit, das branchenspezifische Fachwissen in einigen Datenschutzbehörden zu verbessern (z. B. in den Bereichen Gesundheit und Pharmazie).

Einige dieser Probleme hängen auch damit zusammen, dass in mehreren Datenschutzbehörden keine ausreichenden Ressourcen vorhanden sind (siehe unten).

Unterschiedliche Praktiken bei der Meldung von Datenschutzverletzungen[41]

Der Rat hebt zwar die Belastung hervor, die durch solche Meldungen entsteht, jedoch gibt es zwischen den Mitgliedstaaten erhebliche Diskrepanzen bei den Meldungen: Während die Gesamtzahl der Meldungen von Datenschutzverletzungen im Zeitraum von Mai 2018 bis Ende November 2019 in den meisten Mitgliedstaaten unter 2000 und in sieben Mitgliedstaaten zwischen 2000 und 10 000 lag, gaben die niederländischen und die deutschen Datenschutzbehörden 37 400 bzw. 45 600 Meldungen an.[42]

---

[40] Bis zum Erlass der e-Datenschutz-Verordnung ist eine enge Zusammenarbeit mit den für die Durchsetzung der e-Datenschutz-Richtlinie zuständigen Behörden in den Mitgliedstaaten erforderlich. Gemäß dieser Richtlinie sind in einigen Mitgliedstaaten die für die Durchsetzung von Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie (in dem die Bedingungen festgelegt sind, unter denen „Cookies“ im Endgerät eines Nutzers gespeichert und darauf zugegriffen werden kann) zuständigen Behörden nicht dieselben wie die Aufsichtsbehörden nach der DSGVO.

[41] Artikel 33 der DSGVO.

[42] Siehe Beitrag des Ausschusses S. 35.

Dies deutet unter Umständen auf eine mangelnde einheitliche Auslegung und Umsetzung hin, obwohl auf EU-Ebene Leitlinien über die Meldung von Datenschutzverletzungen vorhanden sind.

Leitlinien des Europäischen Datenschutzausschusses

Bisher hat der Ausschuss mehr als 20 Leitlinien zu zentralen Aspekten der DSGVO angenommen.[43] Die Leitlinien sind ein wesentliches Instrument für die einheitliche Anwendung der DSGVO und wurden daher von den Interessenträgern weitgehend begrüßt. Von den Interessenträgern wurde die systematische öffentliche Konsultation (6 bis 8 Wochen) gewürdigt. Allerdings fordern sie einen intensiveren Dialog mit dem Ausschuss. In diesem Zusammenhang sollte die Praxis, vor der Ausarbeitung von Leitlinien Workshops zu gezielten Themen zu veranstalten, fortgesetzt und ausgebaut werden, um die Transparenz, die Einbindung und die Relevanz der Arbeit des Ausschusses zu gewährleisten. Die Interessenträger fordern ferner, die Auslegung der strittigsten Fragen nicht in den Stellungnahmen gemäß Artikel 64 Absatz 2 der DSGVO, sondern in den Leitlinien zu behandeln, da diese Gegenstand einer öffentlichen Konsultation sind. Einige Interessenträger wünschen sich auch stärker praxisorientierte Leitlinien, in denen die Anwendung der Begriffe und Bestimmungen der DSGVO im Einzelnen dargelegt werden.[44] Die Mitglieder der Multi-Stakeholder-Gruppe heben hervor, dass konkretere Beispiele benötigt würden, um den Spielraum für unterschiedliche Auslegungen zwischen den Datenschutzbehörden so weit wie möglich zu verringern. Gleichzeitig sollten die Forderungen nach Klärung der Frage, wie die DSGVO anzuwenden und Rechtssicherheit zu schaffen ist, nicht zu zusätzlichen Anforderungen führen oder die Vorteile des risikobasierten Ansatzes und des Grundsatzes der Rechenschaftspflicht schmälern.

Die Themen, zu denen die Interessenträger zusätzliche Leitlinien des Ausschusses wünschen, sind unter anderem folgende: Umfang der Rechte der betroffenen Personen (auch im Beschäftigungskontext), Aktualisierung der Stellungnahme zur Verarbeitung auf der Grundlage eines berechtigten Interesses, die Begriffe „Verantwortlicher“, „gemeinsam für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ sowie die erforderlichen Vereinbarungen zwischen den Parteien,[45] Anwendung der DSGVO auf neue Technologien (wie Blockchain und künstliche Intelligenz), Verarbeitung im Rahmen der wissenschaftlichen Forschung (auch im Hinblick auf die internationale Zusammenarbeit), Verarbeitung der Daten von Kindern, Pseudonymisierung und Anonymisierung sowie die Verarbeitung von Gesundheitsdaten.

Der Ausschuss hat bereits darauf hingewiesen, dass er Leitlinien zu vielen dieser Themen herausgeben wird, wobei die Arbeit zu einigen davon bereits aufgenommen wurde (z. B. über die Anwendung des berechtigten Interesses als Rechtsgrundlage für die Verarbeitung).

---

[43] Die Arbeit an Leitlinien begann bereits vor der Anwendung der DSGVO am 25. Mai 2018 im Rahmen der Artikel-29-Datenschutzgruppe. Siehe eine vollständige Liste der Leitlinien unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de.

[44] Dies wurde auch vom Europäischen Parlament und vom Rat betont.

[45] Derzeit werden Leitlinien des Ausschusses zum Thema Verantwortliche und Auftragsverarbeiter erarbeitet.

Die Interessenträger fordern den Ausschuss auf, ggf. bestehende Leitlinien zu aktualisieren und zu überarbeiten und dabei die seit ihrer Veröffentlichung gesammelten Erfahrungen zu berücksichtigen sowie die Gelegenheit zu nutzen, bei Bedarf mehr ins Detail zu gehen.

2.4 Ressourcen der Datenschutzbehörden

Die Ausstattung jeder Datenschutzbehörde mit den erforderlichen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ist eine Voraussetzung dafür, dass sie ihre Aufgaben und Befugnisse effektiv wahrnehmen kann, und bildet somit die Grundlage für ihre Unabhängigkeit.[46]

Seit Inkrafttreten der DSGVO im Jahr 2016[47] haben die meisten Datenschutzbehörden von einer Aufstockung des Personals und der Ressourcen profitiert. Allerdings berichten viele von ihnen immer noch, dass sie nicht über ausreichende Ressourcen verfügen.[48]

Zahl der Mitarbeiter in den nationalen Datenschutzbehörden

Die Gesamtzahl der Mitarbeiter in den Datenschutzbehörden im EWR ist zwischen 2016 und 2019 insgesamt um 42 % gestiegen (um 62 % bei Betrachtung der Prognose für 2020).

Die meisten Behörden verzeichneten in diesem Zeitraum eine Zunahme ihrer Mitarbeiterzahl, wobei der prozentuale Anstieg bei den Behörden in Irland (+169 %), in den Niederlanden (+ 145 %), in Island (+143 %), in Luxemburg (+126 %) und in Finnland (+ 114 %) am größten war. Andererseits ging die Zahl der Mitarbeiter in mehreren Datenschutzbehörden zurück, wobei die stärksten Rückgänge in Griechenland (-15 %), Bulgarien (-14 %), Estland (-11 %), Lettland (-10 %) und Litauen (-8 %) zu beobachten waren. In einigen Behörden ist der Personalrückgang auch auf die Abwanderung von Datenschutzexperten in die Privatwirtschaft zurückzuführen, wo attraktivere Beschäftigungsbedingungen geboten werden.

Generell sieht die Prognose für 2020 einen Personalzuwachs im Vergleich zu 2019 vor, mit Ausnahme bei den Behörden in Bulgarien, Italien, Österreich, Schweden und Island (wo die Personalstärke voraussichtlich stabil bleiben wird) sowie in Dänemark und Zypern (wo eine Verringerung der Mitarbeiterzahlen erwartet wird).

Die deutschen Datenschutzbehörden[49] haben zusammengenommen die höchste Mitarbeiterzahl (888 im Jahr 2019/1002 in der Prognose für 2020), gefolgt von den Datenschutzbehörden in Polen (238/260), Frankreich (215/225), Spanien (170/220), den Niederlanden (179/188), Italien (170/170) und Irland (140/176).

Am niedrigsten sind die Mitarbeiterzahlen in den Datenschutzbehörden in Zypern (24/22), Lettland (19/31), Island (17/17), Estland (16/18) und Malta (13/15).

---

[46] Siehe Artikel 52 Absatz 4 der DSGVO.

[47] Die Verordnung trat im Mai 2016 in Kraft und gilt nach einem Übergangszeitraum von zwei Jahren ab Mai 2018.

[48] Siehe Beitrag des Ausschusses, S. 26-30.

[49] In Deutschland gibt es 18 Behörden, eine Behörde auf Bundesebene und 17 Behörden in den Bundesländern (davon zwei in Bayern).

Budget der nationalen Datenschutzbehörden

Das Gesamtbudget der Datenschutzbehörden im EWR ist zwischen 2016 und 2019 insgesamt um 49 % gestiegen (um 64 % bei Betrachtung der Prognose für 2020).

Bei den meisten Behörden erhöhte sich in diesem Zeitraum das Budget, wobei der prozentuale Anstieg bei den Behörden in Irland (+223 %), in Island (+167 %), in Luxemburg (+165 %), in den Niederlanden (+130 %) und in Zypern (+114 %) am größten war. Demgegenüber verzeichneten einige Behörden nur eine geringe Mittelaufstockung, die bei den Datenschutzbehörden in Estland (7 %), in Lettland (4 %), in Rumänien (3 %) und in Belgien (1 %) am niedrigsten war, während bei den Behörden in Frankreich die Mittel gekürzt wurden (-2 %).

Generell sieht die Prognose für 2020 eine Erhöhung des Budgets gegenüber 2019 vor, mit Ausnahme der Behörden in Bulgarien, Estland, Österreich und den Niederlanden (deren Mittelausstattung voraussichtlich stabil bleiben wird).

Zu den Datenschutzbehörden mit dem größten Budget zählen diejenigen in Deutschland (76,6 Mio. EUR 2019/85,8 Mio. EUR in der Prognose für 2020), in Italien (29,1 Mio. EUR/30,1 Mio. EUR), in den Niederlanden (18,6 Mio. EUR/18,6 Mio. EUR), in Frankreich (18,5 Mio. EUR/20,1 Mio. EUR) und in Irland (15,2 Mio. EUR/16,9 Mio. EUR).

Über das geringste Budget verfügen die Behörden Kroatiens (1,2 Mio. EUR 2019/1,4 Mio. EUR in der Prognose für 2020), Rumäniens (1,1 Mio. EUR/1,3 Mio. EUR), Lettlands (0,6 Mio. EUR/1,2 Mio. EUR), Zyperns (0,5 Mio. EUR/0,5 Mio. EUR) und Maltas (0,5 Mio. EUR/0,6 Mio. EUR).

Die Tabelle in Anhang II gibt einen Überblick über die personellen und finanziellen Ressourcen der nationalen Datenschutzbehörden.

Der Mangel an Ressourcen wirkt sich nicht nur auf die Fähigkeit der Datenschutzbehörden aus, Vorschriften auf nationaler Ebene durchzusetzen, sondern schränkt auch ihre Kapazität ein, an den Verfahren der Zusammenarbeit und Kohärenz und an der Arbeit im Ausschuss mitzuwirken und entsprechende Beiträge zu leisten. Wie der Ausschuss betonte, hängt der Erfolg der Verfahren der Zusammenarbeit und Kohärenz davon ab, wie viel Zeit und Aufwand die Datenschutzbehörden der Bearbeitung der einzelnen grenzüberschreitenden Fälle sowie der diesbezüglichen Zusammenarbeit widmen können. Die Ressourcenproblematik wird durch die zunehmend wichtige Rolle, die den Behörden bei der Überwachung gegenwärtig entwickelter IT-Großsysteme zukommt, noch verschärft. Darüber hinaus haben die Datenschutzbehörden in Irland und Luxemburg aufgrund ihrer Rolle als federführende Behörden bei der Durchsetzung der DSGVO gegenüber großen Technologieunternehmen, die überwiegend in diesen Mitgliedstaaten ansässig sind, einen besonderen Ressourcenbedarf.

Während der Rat auf die Auswirkungen des Verfahrens der Zusammenarbeit und der betreffenden Fristen auf die Arbeit der Datenschutzbehörden[50] hinweist, sind die

[50] Artikel 60 der DSGVO.

Mitgliedstaaten nach der DSGVO verpflichtet, ihre nationalen Datenschutzbehörden mit angemessenen personellen, finanziellen und technischen Ressourcen auszustatten[51].

Das Sekretariat des Ausschusses, das vom Europäischen Datenschutzbeauftragten bereitgestellt wird[52], besteht derzeit aus 20 Personen, darunter Rechts-, IT- und Kommunikationsexperten. Es ist zu prüfen, ob diese Zahl künftig erhöht werden muss, damit das Sekretariat seine Aufgabe, die in der analytischen, administrativen und logistischen Unterstützung des Ausschusses und seiner Untergruppen besteht, unter anderem auch durch die Verwaltung des Informationsaustauschsystems, wirksam erfüllen kann.

3 HARMONISIERTE REGELUNGEN TROTZ GEWISSER FRAGMENTIERUNG UND UNTERSCHIEDLICHER KONZEPTE

Die DSGVO sieht einen einheitlichen Ansatz für die Datenschutzvorschriften in der gesamten EU vor, der die verschiedenen nationalen Regelungen ersetzt, die im Rahmen der Datenschutzrichtlinie von 1995 bestanden.

3.1 Umsetzung der DSGVO durch die Mitgliedstaaten

Die DSGVO ist seit dem 25. Mai 2018 in allen Mitgliedstaaten unmittelbar anwendbar. Sie verpflichtet die Mitgliedstaaten, Rechtsvorschriften zu erlassen und insbesondere nationale Datenschutzbehörden einzurichten und allgemeine Bedingungen für ihre Mitglieder festzulegen, damit sichergestellt ist, dass jede Behörde bei der Wahrnehmung ihrer Aufgaben und Befugnisse gemäß der DSGVO völlig unabhängig handelt. Rechtliche Verpflichtungen und öffentliche Aufgaben können nur dann eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen, wenn sie in (Unions- oder) nationalem Recht verankert sind. Darüber hinaus müssen die Mitgliedstaaten insbesondere für Verstöße, die nicht mit Geldbußen geahndet werden, Regelungen für Sanktionen festlegen und das Recht auf Schutz personenbezogener Daten mit dem Recht auf Meinungs- und Informationsfreiheit in Einklang bringen. Außerdem kann im nationalen Recht eine Rechtsgrundlage für die Ausnahme vom generellen Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten vorgesehen werden, beispielsweise aus Gründen eines erheblichen öffentlichen Interesses im Bereich der öffentlichen Gesundheit, einschließlich des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren. Des Weiteren müssen die Mitgliedstaaten die Akkreditierung von Zertifizierungsstellen sicherstellen.

Die Kommission überwacht, wie die DSGVO in der nationalen Gesetzgebung umgesetzt wird. Zum Zeitpunkt der Erstellung dieses Berichts hatten alle Mitgliedstaaten mit Ausnahme Sloweniens neue Datenschutzvorschriften erlassen oder ihre Rechtsvorschriften in diesem Bereich angepasst. Die Kommission forderte

[51] Artikel 52 Absatz 4 der DSGVO.
[52] Artikel 75 der DSGVO.

Slowenien daher auf, die bisher erzielten Fortschritte zu erläutern, und drängte das Land, diesen Prozess abzuschließen.[53]

Darüber hinaus wird die Vereinbarkeit der nationalen Rechtsvorschriften mit den Datenschutzvorschriften bezüglich des Schengen-Besitzstands auch im Rahmen des von der Kommission koordinierten Schengen-Evaluierungsmechanismus bewertet. Die Kommission und die Mitgliedstaaten bewerten gemeinsam, wie die Länder den Schengen-Besitzstand in einer Reihe von Bereichen umsetzen und anwenden; im Bereich Datenschutz betrifft dies IT-Großsysteme wie das Schengener Informationssystem und das Visa-Informationssystem und schließt die Rolle der Datenschutzbehörden bei der Überwachung der Verarbeitung personenbezogener Daten innerhalb dieser Systeme ein.

Die Anpassung sektorspezifischer Vorschriften auf nationaler Ebene ist noch im Gange. Nach ihrer Aufnahme in das Abkommen über den Europäischen Wirtschaftsraum wurde die Anwendung der DSGVO auf Norwegen, Island und Liechtenstein ausgeweitet. Auch diese Länder haben nationalen Datenschutzvorschriften erlassen.

Die Kommission wird alle ihr zur Verfügung stehenden Instrumente, einschließlich Vertragsverletzungsverfahren, nutzen, um sicherzustellen, dass die Mitgliedstaaten die DSGVO einhalten.

Die wichtigsten Fragen im Zusammenhang mit der Umsetzung auf nationaler Ebene

Zu den wichtigsten Fragen, die bisher im Rahmen der laufenden Bewertung der nationalen Rechtsvorschriften und des bilateralen Austauschs mit den Mitgliedstaaten ermittelt wurden, zählen:

- Beschränkungen der Anwendung der DSGVO: beispielsweise schließen einige Mitgliedstaaten die Tätigkeiten des nationalen Parlaments vollständig aus.
- Unterschiede in der Anwendbarkeit der nationalen präzisierenden Vorschriften. Einige Mitgliedstaaten verknüpfen die Anwendbarkeit ihrer nationalen Rechtsvorschriften mit dem Ort, an dem die Waren oder Dienstleistungen angeboten werden, andere mit dem Ort der Niederlassung des Verantwortlichen oder des Auftragsverarbeiters. Dies läuft dem mit der DSGVO verfolgten Ziel der Harmonisierung zuwider.
- Nationale Rechtsvorschriften, die Fragen zur Verhältnismäßigkeit des Eingriffs in das Recht auf Datenschutz aufwerfen. So hat die Kommission beispielsweise ein Vertragsverletzungsverfahren gegen einen Mitgliedstaat eingeleitet, der Rechtsvorschriften erlassen hat, nach denen Richter bestimmte Informationen über ihre nicht beruflichen Tätigkeiten offenlegen müssen, was mit dem Recht auf Achtung des Privatlebens und dem Recht auf Schutz personenbezogener Daten unvereinbar ist.[54]

---

[53] Es gilt festzustellen, dass die nationale Datenschutzbehörde Sloweniens auf der Grundlage des aktuellen nationalen Datenschutzrechts eingerichtet wurde und die Anwendung der DSGVO in diesem Mitgliedstaat überwacht.

[54] Dieses Vertragsverletzungsverfahren betrifft das polnische Justizgesetz vom 20. Dezember 2019, das die Unabhängigkeit der Richter beeinträchtigt und unter anderem die Offenlegung ihrer nicht beruflichen Tätigkeiten betrifft:

- Fehlen einer unabhängigen Stelle für die Überwachung der Datenverarbeitung durch Gerichte, die im Rahmen ihrer justiziellen Tätigkeit handeln.[55]
- Rechtsvorschriften in Bereichen, die vollständig in der DSGVO geregelt sind, jenseits des Spielraums für Spezifizierungen oder Beschränkungen. Dies ist insbesondere dann der Fall, wenn nationale Vorschriften Bedingungen für die Verarbeitung auf der Grundlage eines berechtigten Interesses festlegen, indem sie eine Abwägung der jeweiligen Interessen des Verantwortlichen und der betroffenen Personen vorsehen, während die DSGVO jeden Verantwortlichen verpflichtet, eine solche Abwägung einzeln vorzunehmen und sich auf diese Rechtsgrundlage zu stützen.
- Spezifizierungen und zusätzliche Anforderungen, die über die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder einer öffentlichen Aufgabe hinausgehen (z. B. für eine Videoüberwachung im privaten Sektor oder für die Direktwerbung), und für in der DSGVO verwendete Begriffe (z. B. „umfangreich" oder „Löschung").

Einige dieser Fragen werden unter Umständen vom Gerichtshof der Europäischen Union in noch anhängigen Rechtssachen geklärt.[56]

Vereinbarkeit des Rechts auf Schutz personenbezogener Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit

Eine spezifische Frage betrifft die Umsetzung der Pflicht der Mitgliedstaaten, das Recht auf Schutz personenbezogener Daten per Rechtsvorschrift mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.[57] Diese Frage ist sehr komplex, da bei einer Abwägung zwischen diesen Grundrechten auch die Bestimmungen und Garantien in den Presse- und Mediengesetzen berücksichtigt werden müssen.

Bei der Bewertung der Rechtsvorschriften der Mitgliedstaaten zeigen sich unterschiedliche Ansätze bezüglich der Vereinbarkeit des Rechts auf Schutz personenbezogener Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit:

- Einige Mitgliedstaaten legen den Grundsatz fest, dass der freien Meinungsäußerung Vorrang eingeräumt wird, oder befreien grundsätzlich die Anwendung ganzer in Artikel 85 Absatz 2 der DSGVO genannter Kapitel, wenn die Verarbeitung für journalistische Zwecke und für akademische, künstlerische und literarische Zwecke gefährdet ist. In gewissem Umfang sehen Mediengesetze einige Garantien in Bezug auf die Rechte betroffener Personen vor.
- In einigen Mitgliedstaaten wird dem Schutz personenbezogener Daten Vorrang eingeräumt und die Anwendung von Datenschutzvorschriften nur in bestimmten

https://ec.europa.eu/commission/presscorner/detail/de/ip_20_772.

55 Siehe Artikel 8 Absatz 3 der Charta; Artikel 16 AEUV; Erwägungsgrund 20 der DSGVO.

56 Beispielsweise ist die Ausnahme eines parlamentarischen Petitionsausschusses von der Anwendung der DSGVO Gegenstand eines vor dem Gerichtshof anhängigen Verfahrens über ein Vorabentscheidungsersuchen (C-272/19).

57 Artikel 85 der DSGVO.

Situationen ausgeschlossen, beispielsweise wenn eine Person mit öffentlichem Status betroffen ist.

- Andere Mitgliedstaaten sehen wiederum eine bestimmte Abwägung durch den Gesetzgeber und/oder eine Einzelfallbewertung hinsichtlich der Abweichung von bestimmten Bestimmungen der DSGVO vor.

Die Kommission setzt ihre Bewertung der nationalen Rechtsvorschriften auf der Grundlage der Anforderungen der Charta fort. Die Vereinbarkeit muss gesetzlich vorgesehen sein, den Wesensgehalt dieser Grundrechte achten sowie verhältnismäßig und erforderlich sein (Artikel 52 Absatz 1 der Charta). Die Datenschutzvorschriften sollten die Ausübung des Rechts auf Freiheit der Meinungsäußerung und Informationsfreiheit nicht beeinträchtigen, insbesondere nicht dadurch, dass sie eine abschreckende Wirkung entfalten oder als Möglichkeit ausgelegt werden, Druck auf Journalisten auszuüben, ihre Quellen offenzulegen.

3.2 Fakultative Spezifikationsklauseln und ihre Grenzen

Die DSGVO gibt den Mitgliedstaaten die Möglichkeit, ihre Anwendung in einer begrenzten Zahl von Bereichen zu präzisieren. Dieser Spielraum für nationale Rechtsvorschriften ist von der oben erwähnten Verpflichtung zur Umsetzung bestimmter anderer Bestimmungen der DSGVO zu unterscheiden. Die Klauseln für fakultative Spezifikationen sind in Anhang I aufgeführt.

Die Spielräume für Rechtsvorschriften der Mitgliedstaaten unterliegen den in der DSGVO festgelegten Bedingungen und Beschränkungen und erlauben keine parallele nationale Datenschutzregelung.[58] Die Mitgliedstaaten sind verpflichtet, die nationalen Datenschutzvorschriften, einschließlich sektorspezifischer Rechtsvorschriften mit Datenschutzaspekten, zu ändern oder aufzuheben.

Des Weiteren dürfen die einschlägigen Rechtsvorschriften der Mitgliedstaaten keine Bestimmungen enthalten, die zu Verwirrung hinsichtlich der unmittelbaren Anwendung der DSGVO führen könnten. Daher können die Mitgliedstaaten in den Fällen, in denen die DSGVO eine Präzisierung oder Einschränkung ihrer Vorschriften durch das Recht der Mitgliedstaaten vorsieht, Teile der DSGVO in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.[59]

Die Interessenträger sind der Auffassung, dass die Mitgliedstaaten fakultative Spezifikationsklauseln nur in geringem Maße vorsehen oder ganz darauf verzichten sollten, da sie nicht zur Harmonisierung beitragen. Die nationalen Unterschiede bei der Umsetzung der Rechtsvorschriften und ihrer Auslegung durch die Datenschutzbehörden erhöhen die Kosten für die Einhaltung der Rechtsvorschriften in der EU erheblich.

Fragmentierung im Zusammenhang mit der Verwendung fakultativer Spezifikationsklauseln

- Altersgrenze für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

Einige Mitgliedstaaten haben von der Möglichkeit Gebrauch gemacht, für die Einwilligung in Bezug auf Dienste der Informationsgesellschaft ein niedrigeres Alter als 16 Jahre vorzusehen (Artikel 8 Absatz 1 der DSGVO). Während neun Mitgliedstaaten die Altersgrenze von 16 Jahren anwenden, haben sich acht Mitgliedstaaten für eine Altersgrenze von 13 Jahren, sechs Mitgliedstaaten für eine Altersgrenze von 14 Jahren und drei Mitgliedstaaten für eine Altersgrenze von 15 Jahren entschieden.[60]

---

[58] Der weitverbreitete Begriff „Öffnungsklauseln“ im Sinne von Spezifikationsklauseln ist irreführend, da er den Eindruck erwecken könnte, dass die Mitgliedstaaten über einen Handlungsspielraum verfügen, der über die Bestimmungen der Verordnung hinausgeht.

[59] Erwägungsgrund 8 der DSGVO.

[60] In Belgien, Dänemark, Estland, Finnland, Lettland, Malta, Portugal und Schweden gilt eine Altersgrenze von 13 Jahren. In Bulgarien, Italien, Litauen, Österreich, Spanien und Zypern gilt eine Altersgrenze von 14 Jahren. In Frankreich, Griechenland und der Tschechischen Republik gilt eine

Demzufolge muss ein Unternehmen, das in der gesamten EU Dienste der Informationsgesellschaft für Minderjährige anbietet, nach dem Alter der potenziellen Nutzer abhängig davon unterscheiden, in welchem Mitgliedstaat sie ansässig sind. Dies steht im Widerspruch zu dem Hauptziel der DSGVO, ein gleiches Schutzniveau für Personen und gleiche Geschäftsmöglichkeiten in allen Mitgliedstaaten zu gewährleisten.

Solche Unterschiede führen dazu, dass der Mitgliedstaat, in dem der Verantwortliche niedergelassen ist, eine andere Altersgrenze vorsieht als die Mitgliedstaaten, in denen die betroffenen Personen ihren Wohnsitz haben.

Altersgrenze von 15 Jahren. In Deutschland, Irland, Kroatien, Luxemburg, den Niederlanden, Polen, Rumänien, der Slowakei und Ungarn gilt eine Altersgrenze von 16 Jahren.

- Gesundheit und Forschung

Bei der Umsetzung von Ausnahmen vom allgemeinen Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten[61] folgen die Rechtsvorschriften der Mitgliedstaaten beim Grad der Präzisierungen und Garantien, einschließlich zu gesundheitlichen und Forschungszwecken, unterschiedlichen Ansätzen. Die meisten Mitgliedstaaten haben weitere Bedingungen in Bezug auf die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten eingeführt oder beibehalten. Dies gilt auch für Ausnahmen, die sich auf die Rechte betroffener Personen hinsichtlich der Verarbeitung personenbezogener Daten zu Forschungszwecken[62] beziehen, und zwar sowohl in Bezug auf den Umfang der Ausnahmen als auch auf die damit verbundenen Garantien.

Die künftigen Leitlinien des Ausschusses zur Verwendung personenbezogener Daten auf dem Gebiet der wissenschaftlichen Forschung werden zu einem harmonisierten Ansatz in diesem Bereich beitragen. Die Kommission wird dem Ausschuss insbesondere in Bezug auf die Forschung im Gesundheitsbereich zuarbeiten, unter anderem in Form konkreter Fragen und der Analyse konkreter Szenarien aus der Forschungsgemeinschaft. Eine Annahme dieser Leitlinien vor dem Start des Rahmenprogramms „Horizont Europa“ wäre hilfreich, um Datenschutzpraktiken zu harmonisieren und die gemeinsame Nutzung von Daten für Fortschritte in der Forschung zu erleichtern. Leitlinien des Ausschusses in Bezug auf die Verarbeitung personenbezogener Daten im Gesundheitsbereich könnten ebenfalls von Nutzen sein.

Die DSGVO bietet einen soliden Rahmen für nationale Rechtsvorschriften im Bereich der öffentlichen Gesundheit und umfasst ausdrücklich grenzüberschreitende Gesundheitsgefahren sowie die Überwachung von Epidemien und deren Ausbreitung[63], was im Zusammenhang mit der Bekämpfung der COVID-19-Pandemie von Bedeutung war.

Auf EU-Ebene verabschiedete die Kommission am 8. April 2020 eine Empfehlung für ein Instrumentarium für den Einsatz von Technik und Daten zur Bekämpfung und Überwindung der COVID-19-Krise, insbesondere im Hinblick auf Mobil-Apps und die Verwendung anonymisierter Mobilitätsdaten[64] sowie am 16. April 2020 Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie[65]. Der Ausschuss veröffentlichte am 19. März 2020 eine Erklärung zur Verarbeitung personenbezogener Daten im Zusammenhang mit COVID-19[66], gefolgt von Leitlinien für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19[67], die am 21. April 2020 angenommen wurden. In diesen Empfehlungen und Leitlinien wird erläutert, wie die Grundsätze und Vorschriften für den Schutz personenbezogener Daten im Zusammenhang mit der Bekämpfung der Pandemie anzuwenden sind.

---

61 Artikel 9 der DSGVO.
62 Artikel 89 Absatz 2 der DSGVO.
63 Siehe Artikel 9 Absatz 2 Buchstabe i und Erwägungsgrund 46 der DSGVO.
64 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf
65 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=DE
66 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_art_23gdpr_20200602_de_1.pdf
67 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf

- Umfangreiche Beschränkungen der Rechte betroffener Personen

In den meisten nationalen Datenschutzvorschriften, welche die Rechte betroffener Personen beschränken, werden die Ziele des allgemeinen öffentlichen Interesses, die durch diese Beschränkungen sichergestellt werden, nicht angegeben und/oder die Bedingungen und Garantien gemäß Artikel 23 Absatz 2 der DSGVO nicht ausreichend erfüllt.[68] Mehrere Mitgliedstaaten räumen keinen Spielraum für die Verhältnismäßigkeitsprüfung ein oder erweitern die Beschränkungen sogar über den Anwendungsbereich von Artikel 23 Absatz 1 der DSGVO hinaus. So wird beispielsweise in einigen nationalen Rechtsvorschriften das Auskunftsrecht bezüglich personenbezogener Daten, die aufgrund einer Speicherverpflichtung oder im Zusammenhang mit der Erfüllung öffentlicher Aufgaben gespeichert werden, aus Gründen eines unverhältnismäßigen Aufwands seitens des Verantwortlichen verweigert, ohne dass eine solche Beschränkung auf Ziele des allgemeinen öffentlichen Interesses begrenzt wird.

- Zusätzliche Anforderungen für Unternehmen

Auch wenn die obligatorische Benennung eines Datenschutzbeauftragten risikobasiert ist[69], dehnte ein Mitgliedstaat[70] diese Anforderung auf ein quantitatives Kriterium aus und verpflichtete Unternehmen, in denen mindestens 20 Mitarbeiter dauerhaft in die automatisierte Verarbeitung personenbezogener Daten einbezogen sind, zur Benennung eines Datenschutzbeauftragten unabhängig von den mit der Verarbeitung verbundenen Risiken[71]. Dies hat zu zusätzlichem Aufwand geführt.

4 BEFÄHIGUNG JEDES EINZELNEN ZUR KONTROLLE SEINER DATEN

Mit der DSGVO werden die Grundrechte wirksam, insbesondere das Recht auf Schutz personenbezogener Daten, aber auch die anderen in der Charta festgeschriebenen Grundrechte, darunter Achtung des Privat- und Familienlebens, Freiheit der Meinungsäußerung und Informationsfreiheit, Nichtdiskriminierung, Gedanken-, Gewissens- und Religionsfreiheit, unternehmerische Freiheit und Recht auf einen wirksamen Rechtsbehelf. Diese Rechte müssen unter Wahrung des Grundsatzes der Verhältnismäßigkeit gegeneinander abgewogen werden.[72]

Die DSGVO gewährt Personen durchsetzbare Rechte wie das Recht auf Auskunft, Berichtigung, Löschung, Widerspruch, Datenübertragbarkeit und erhöhte Transparenz. Sie gewährt Personen außerdem das Recht, Beschwerde bei einer Datenschutzbehörde einzureichen, unter anderem in Form von Verbandsklagen, sowie das Recht auf gerichtliche Rechtsbehelfe.

Wie die Ergebnisse der Eurobarometer-Umfrage[73] vom Juli 2019 und die Umfrage der Agentur der Europäischen Union für Grundrechte[74] zeigen, sind sich die Bürgerinnen und Bürger ihrer Rechte zunehmend bewusst.

---

68 Da sie zum Beispiel lediglich den Wortlaut von Artikel 23 Absatz 1 der DSGVO wiederholen.
69 Artikel 37 Absatz 1 der DSGVO.
70 Deutschland.
71 Durch Anwendung der Spezifikationsklausel in Artikel 37 Absatz 4 der DSGVO.
72 Vgl. Erwägungsgrund 4 der DSGVO.
73 https://ec.europa.eu/commission/presscorner/detail/de/IP_19_2956

Laut der von der Agentur der Europäischen Union für Grundrechte durchgeführten Umfrage zu den Grundrechten

- haben 69 % der über 16-Jährigen in der EU von der DSGVO gehört;
- haben 71 % der Befragten in der EU von ihrer nationalen Datenschutzbehörde gehört; diese Zahl reicht von 90 % in der Tschechischen Republik bis 44 % in Belgien;
- sind sich 60 % der Befragten in der EU eines Gesetzes bewusst, das ihnen Auskunft über ihre im Besitz der öffentlichen Verwaltung befindlichen personenbezogenen Daten ermöglicht; dieser Wert sinkt jedoch bei Privatunternehmen auf 51 %;
- möchte mehr als einer von fünf Befragten (23 %) in der EU personenbezogene Daten (z. B. Anschrift, Staatsangehörigkeit oder Geburtsdatum) nicht an die öffentliche Verwaltung weitergeben, und 41 % möchten diese Daten nicht an private Unternehmen weitergeben.

Personen machen zunehmend von ihrem Recht Gebrauch, Beschwerden bei Datenschutzbehörden einzureichen, sei es einzeln oder in Form von Verbandsklagen.[75] Nur wenige Mitgliedstaaten haben nichtstaatlichen Organisationen gestattet, im Einklang mit der in der DSGVO vorgesehenen Möglichkeit Maßnahmen ohne Auftrag einzuleiten. Nach dem Erlass der vorgeschlagenen Richtlinie über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher[76] dürfte der Rahmen für Verbandsklagen auch im Bereich des Datenschutzes gestärkt werden.

Beschwerden

Nach Angaben des Ausschusses wurden zwischen Mai 2018 und Ende November 2019 insgesamt rund 275 000 Beschwerden eingereicht.[77] Diese Zahl sollte jedoch mit großer Vorsicht betrachtet werden, da eine Beschwerde bei den Behörden unterschiedlich definiert wird. Die absolute Zahl der bei den Datenschutzbehörden eingegangenen Beschwerden[78] ist von Mitgliedstaat zu Mitgliedstaat sehr unterschiedlich. Die meisten Beschwerden wurden in Deutschland (67 000), den Niederlanden (37 000), Spanien und Frankreich (jeweils 18 000), Italien (14 000), Polen und Irland (jeweils 12 000) verzeichnet. Zwei Drittel der Behörden gaben eine Beschwerdezahl zwischen 8000 und 600 an. In Estland und Belgien (jeweils rund 500) sowie in Malta und Island (jeweils weniger als 200) war die Zahl der Beschwerden am niedrigsten.

Die Zahl der Beschwerden korreliert nicht unbedingt mit der Bevölkerungszahl oder dem BIP, beispielsweise gab es in Deutschland fast doppelt so viele Beschwerden wie in den Niederlanden und viermal so viele Beschwerden wie in Spanien und Frankreich.

---

74 Agentur der Europäischen Union für Grundrechte (FRA) (2020): Umfrage zu den Grundrechten 2019. Datenschutz und Technologie: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

75 Artikel 80 der DSGVO.

76 COM/2018/0184 final – 2018/089 (COD)

77 Sowohl nach Artikel 77 als auch nach Artikel 80 der DSGVO.

78 Siehe Beitrag des Ausschusses, S. 31-32.

Aus den Rückmeldungen der Multi-Stakeholder-Gruppe geht hervor, dass die Unternehmen eine Vielzahl von Maßnahmen ergriffen haben, um die Ausübung der Rechte der betroffenen Personen zu erleichtern, darunter die Umsetzung von Prozessen, die eine individuelle Überprüfung von Anträgen und eine Antwort des Verantwortlichen gewährleisten, die Nutzung mehrerer Kanäle (Postweg, spezifische E-Mail-Adresse, Website usw.), aktualisierte interne Verfahren und Strategien für die zeitnahe interne Bearbeitung von Anträgen sowie Schulung des Personals. Einige Unternehmen haben digitale Portale eingerichtet, die über die Website des Unternehmens (oder das unternehmenseigene Intranet für die Mitarbeiter) zugänglich sind, um den betroffenen Personen die Ausübung ihrer Rechte zu erleichtern.

Folgende Punkte erfordern jedoch weitere Fortschritte:

- Nicht alle Verantwortlichen kommen ihrer Verpflichtung nach, den betroffenen Personen die Ausübung ihrer Rechte zu erleichtern.[79] Die Verantwortlichen müssen sicherstellen, dass den betroffenen Personen eine wirksame Anlaufstelle mitgeteilt wird, an die sie sich wenden und ihre Probleme erläutern können. Hierbei kann es sich um den Datenschutzbeauftragten handeln, dessen Kontaktdaten der betroffenen Person mitgeteilt werden müssen.[80] Die Art der Kontaktaufnahme darf sich nicht auf E-Mails beschränken, sondern es muss der betroffenen Person auch ermöglicht werden, sich auf anderem Wege an den Verantwortlichen zu wenden.

- Personen haben nach wie vor Schwierigkeiten, wenn sie Auskunft über ihre Daten beantragen, beispielsweise bei Plattformen, Datenvermittlern und AdTech-Unternehmen.

- Das Recht auf Datenübertragbarkeit wird nicht in vollem Umfang genutzt. In der von der Kommission am 19. Februar 2020 angenommenen Europäischen Datenstrategie (im Folgenden „Datenstrategie“)[81] wurde betont, dass alle Nutzungsmöglichkeiten dieses Rechts erleichtert werden müssen (z. B. indem technische Schnittstellen und maschinenlesbare Formate vorgeschrieben werden, die die Übertragbarkeit von Daten in Echtzeit oder nahezu Echtzeit ermöglichen). Die Wirtschaftsteilnehmer weisen darauf hin, dass es bisweilen schwierig sei, die Daten (aufgrund fehlender Standards) in einem strukturierten und gängigen maschinenlesbaren Format bereitzustellen. Nur in bestimmten Sektoren – z. B. im Banken- und Telekommunikationssektor sowie im Bereich der Wasser- und Heizungsablesung – tätige Unternehmen berichten, dass sie die erforderlichen Schnittstellen eingerichtet haben.[82] Um dem Einzelnen die Ausübung seiner Rechte im Rahmen der DSGVO zu erleichtern, und zwar nicht nur auf die Datenübertragbarkeit beschränkt, wurden neue technologische Instrumente entwickelt (z. B. persönliche Datenräume und Dienste für die Verwaltung personenbezogener Informationen).

- Rechte von Kindern: Mehrere Mitglieder der Multi-Stakeholder-Gruppe betonen die Notwendigkeit, Kinder zu informieren, sowie die Tatsache, dass viele Unternehmen außer Acht lassen, dass Kinder von der Verarbeitung ihrer Daten

---

79 Artikel 12 Absatz 2 der DSGVO.
80 Artikel 13 Absatz 1 Buchstabe b und Artikel 14 Absatz 1 Buchstabe b der DSGVO.
81 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_de.pdf
82 Siehe Bericht der Multi-Stakeholder-Gruppe.

betroffen sein können. Der Ausschuss weist darauf hin, dass bei der Entwicklung von Verhaltensregeln dem Schutz von Kindern besondere Aufmerksamkeit gewidmet werden könnte. Der Schutz von Kindern ist auch ein Schwerpunkt der Datenschutzbehörden.[83]

- Recht auf Information: Einige Unternehmen verfolgen einen äußerst legalistischen Ansatz, indem sie Datenschutzhinweise als Rechtshandlung betrachten, wobei die Informationen recht komplex, schwer verständlich oder unvollständig sind, wohingegen die DSGVO vorschreibt, dass alle Informationen präzise und in einer klaren und einfachen Sprache abgefasst sein müssen[84]. Es scheint, dass einige Unternehmen den Empfehlungen des Ausschusses nicht folgen, beispielsweise was die Auflistung der Namen der Einrichtungen betrifft, mit denen sie Daten austauschen.
- Mehrere Mitgliedstaaten haben die Rechte der betroffenen Personen durch nationales Recht stark eingeschränkt, einige sogar über den in Artikel 23 der DSGVO genannten Rahmen hinaus.
- Die Ausübung der Rechte des Einzelnen wird bisweilen durch die Praktiken einiger wichtiger digitaler Akteure behindert, die es erschweren, Einstellungen zu wählen, mit denen eine Person ihre Privatsphäre am besten schützen kann (Verstoß gegen die Anforderung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[85]).[86]

Die Leitlinien des Ausschusses zu den Rechten der betroffenen Personen werden von den Interessenträgern gespannt erwartet.

5 MÖGLICHKEITEN UND HERAUSFORDERUNGEN FÜR ORGANISATIONEN, INSBESONDERE FÜR KLEINE UND MITTLERE UNTERNEHMEN

Chancen für Unternehmen

---

[83] Siehe Ergebnisse einer von der irischen Datenschutzbehörde durchgeführten öffentlichen Konsultation zu den Datenschutzrechten von Kindern: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf. Auch die französische Datenschutzbehörde leitete im April 2020 eine öffentliche Konsultation ein: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique.

[84] Artikel 12 Absatz 1 der DSGVO.

[85] Artikel 25 der DSGVO.

[86] Siehe Bericht des Norwegischen Verbraucherrats „Deceived by design“, in dem die „Dark Patterns“, Voreinstellungen und anderen Merkmale und Techniken dargelegt werden, die Unternehmen verwenden, um Nutzer zur Auswahl von Optionen zu bringen, die in ihre Privatsphäre eindringen: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/.
Siehe auch die im Dezember 2019 veröffentlichte Studie des Transatlantischen Verbraucherdialogs und der Heinrich-Böll-Stiftung Europäische Union in Brüssel, in der die Praktiken dreier großer globaler Plattformen analysiert wurden: https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms.

Die DSGVO fördert Wettbewerb und Innovation. Zusammen mit der Verordnung über den freien Verkehr nicht-personenbezogener Daten[87] gewährleistet sie den freien Verkehr von Daten innerhalb der EU und schafft gleiche Wettbewerbsbedingungen für Unternehmen mit Sitz außerhalb der EU. Durch die Schaffung eines harmonisierten Rahmens für den Schutz personenbezogener Daten stellt die DSGVO sicher, dass alle Akteure im Binnenmarkt an dieselben Vorschriften gebunden sind und von den gleichen Chancen profitieren, unabhängig davon, wo sie niedergelassen sind und wo die Verarbeitung stattfindet. Die Technologieneutralität der DSGVO bildet den Datenschutzrahmen für neue technologische Entwicklungen. Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen bieten Anreize für innovative Lösungen, in die von Beginn an Datenschutzaspekte integriert werden, wodurch sich die Kosten für die Einhaltung der Datenschutzvorschriften senken lassen.

Außerdem wird Datenschutz zu einem wichtigen Wettbewerbsparameter, der bei der Auswahl von Dienstleistungen immer häufiger berücksichtigt wird. Personen, die besser informiert und stärker für Datenschutzfragen sensibilisiert sind, suchen nach Produkten und Dienstleistungen, die einen wirksamen Schutz personenbezogener Daten gewährleisten. Die Umsetzung des Rechts auf Datenübertragbarkeit birgt das Potenzial, dass Schranken für den Marktzutritt von Unternehmen abgebaut werden, die innovative und datenschutzfreundliche Dienstleistungen anbieten. Die Auswirkungen einer potenziell breiteren Inanspruchnahme dieses Rechts in verschiedenen Marktsektoren sollten beobachtet werden. Durch die Einhaltung der Datenschutzvorschriften und ihre transparente Anwendung wird Vertrauen in die Verwendung personenbezogener Daten geschaffen, wodurch sich Unternehmen neue Chancen bieten.

Wie bei allen Regelungen entstehen den Unternehmen auch durch Datenschutzvorschriften inhärente Kosten für deren Einhaltung. Diese Kosten werden jedoch durch die Chancen und Vorteile eines gestärkten Vertrauens in die digitale Innovation sowie den Nutzen, der sich aus der Achtung eines Grundrechts für die Gesellschaft ergibt, wettgemacht. Indem gleiche Wettbewerbsbedingungen gewährleistet und Datenschutzbehörden mit Instrumenten für eine wirksame Durchsetzung der Vorschriften ausgestattet werden, verhindert die DSGVO, dass Unternehmen, welche die Vorschriften nicht einhalten, auf der Welle des Vertrauens mitreiten, das von den vorschriftenkonformen Unternehmen aufgebaut wurde.

Besondere Herausforderungen für kleine und mittlere Unternehmen (KMU)

Nach allgemeiner Wahrnehmung der Interessenträger, aber auch des Europäischen Parlaments, des Rates und der Datenschutzbehörden, stellt die Anwendung der DSGVO eine besondere Herausforderung für Kleinstunternehmen sowie kleine und mittlere Unternehmen sowie kleine Freiwilligen- und Wohltätigkeitsorganisationen dar.

Aus dem risikobasierten Ansatz geht hervor, dass Ausnahmen auf der Grundlage der Größe des Wirtschaftsteilnehmers ungeeignet wären, da die Größe allein keine Aussage über die möglichen Risiken für Verbraucher zulässt, die sich aus der von

[87] Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (Abl. L 303 vom 28.11.2018, S. 59).

dem Unternehmen durchgeführten Verarbeitung personenbezogener Daten ergeben. Der risikobasierte Ansatz vereint Flexibilität und wirksamen Schutz. Hierbei werden die Erfordernisse von KMU berücksichtigt, deren Kerngeschäft nicht die Verarbeitung von Daten ist, und ihre Pflichten entsprechend angepasst, insbesondere auf der Grundlage der Eintrittswahrscheinlichkeit und der Schwere der Risiken[88] in Verbindung mit der von ihnen durchgeführten Verarbeitung.

Unabhängig von der Größe des Unternehmens, das die Verarbeitung vornimmt, sollte die Verarbeitung von Daten in kleinerem Umfang und mit geringem Risiko nicht auf dieselbe Weise behandelt werden wie die häufige und mit hohem Risiko verbundene Verarbeitung. Daher sollte, wie der Ausschuss feststellte, „in jedem Fall der vom Gesetzgeber im Text propagierte risikobasierte Ansatz beibehalten werden, da die Risiken für die betroffenen Personen nicht von der Größe der Verantwortlichen abhängen“.[89] Die Datenschutzbehörden sollten diesen Grundsatz bei der Durchsetzung der DSGVO in vollem Umfang berücksichtigen, vorzugsweise im Rahmen eines gemeinsamen europäischen Ansatzes, um keine Hindernisse für den Binnenmarkt zu schaffen.

Die Datenschutzbehörden haben diverse Instrumente entwickelt und ihre Absicht bekundet, diese weiter zu verbessern. Einige Behörden haben Sensibilisierungskampagnen in die Wege geleitet und werden sogar kostenlose „DSGVO-Schulungen“ für KMU veranstalten.

Beispiele für Leitlinien und Instrumente, die von den Datenschutzbehörden speziell für KMU bereitgestellt werden

- Veröffentlichung von gezielt an KMU gerichtete Informationen;
- Seminare für Datenschutzbeauftragte und Veranstaltungen für KMU, die keinen Datenschutzbeauftragten benennen müssen;
- interaktive Leitfäden zur Unterstützung von KMU;
- Hotlines für Konsultationen;
- Vorlagen für Verarbeitungsverträge und Aufzeichnungen über Verarbeitungstätigkeiten.

Der Beitrag des Ausschusses enthält eine Beschreibung der diesbezüglichen Aktivitäten der Datenschutzbehörden.[90]

Mehrere Maßnahmen, mit denen speziell KMU unterstützt werden, wurden mithilfe von Unionsmitteln finanziert. Die Kommission stellte in drei Finanzierungsrunden Zuschüsse in Höhe von insgesamt 5 Mio. EUR zur Verfügung, wobei die letzten beiden Runden konkret dazu dienten, die nationalen Datenschutzbehörden bei ihren Bemühungen zu unterstützen, Einzelpersonen und KMU zu erreichen. Infolgedessen wurden 2018 neun Datenschutzbehörden (Belgien, Bulgarien, Dänemark, Litauen, Lettland, Niederlande, Slowenien, Ungarn und Island) Mittel in Höhe von

[88] Artikel 24 Absatz 1 der DSGVO.
[89] Siehe Beitrag des Ausschusses, S. 35.
[90] Siehe Beitrag des Ausschusses, S. 35-45.

2 Mio. EUR für Aktivitäten im Zeitraum 2018–2019 zugewiesen[91], und 2019 erhielten vier Datenschutzbehörden (Belgien, Malta, Slowenien und Kroatien in Partnerschaft mit Irland) 1 Mio. EUR für Aktivitäten im Jahr 2020 92. 2020 werden nochmals Mittel in Höhe von 1 Mio. EUR zugewiesen.

Trotz dieser Initiativen berichten KMU und Start-ups häufig, dass sie mit der Umsetzung des in der DSGVO verankerten Grundsatzes der Rechenschaftspflicht zu kämpfen hätten.[93] Im Einzelnen führen sie an, dass sie nicht immer genügend Orientierungshilfen und praktische Ratschläge von den nationalen Datenschutzbehörden erhielten oder dass dies zu lange dauerte. Es gab auch Fälle, in denen die Behörden sich nur ungern zu Rechtsfragen äußern wollten. In solchen Situationen wenden KMU sich häufig an externe Berater und Anwälte, wenn es um die Umsetzung des Grundsatzes der Rechenschaftspflicht und des risikobasierten Ansatzes (einschließlich Transparenzforderung, Verzeichnis von Verarbeitungstätigkeiten und Meldungen von Datenschutzverletzungen) geht. Dadurch können ihnen zusätzliche Kosten entstehen.

Ein spezifisches Problem ist die Erfassung der Verarbeitungstätigkeiten, die von KMU und kleinen Vereinigungen als umständlicher Verwaltungsaufwand angesehen wird. Die Befreiung von dieser Pflicht in Artikel 30 Absatz 5 der DSGVO ist tatsächlich sehr eng gefasst. Allerdings sollten die mit der Erfüllung dieser Pflicht verbundenen Anstrengungen auch nicht überbewertet werden. Wenn das Kerngeschäft der KMU nicht in der Verarbeitung personenbezogener Daten besteht, ist die Erfassung der Verarbeitungstätigkeiten unter Umständen einfach und nicht sehr aufwendig. Gleiches gilt für Freiwilligenorganisationen und andere Vereinigungen. Die Führung solcher vereinfachten Verzeichnisse wird durch Vorlagen erleichtert, wie dies bereits bei einigen Datenschutzbehörden gängige Praxis ist. In jedem Fall sollte jeder, der personenbezogene Daten verarbeitet, als grundlegende Voraussetzung zur Erfüllung des Grundsatzes der Rechenschaftspflicht eine Übersicht über seine Datenverarbeitung führen.

Wenn der Ausschuss praktische Instrumente, z. B. einheitliche Formulare für Datenschutzverletzungen und vereinfachte Verzeichnisse von Verarbeitungstätigkeiten, auf EU-Ebene entwickelt, kann dies KMU und kleine Vereinigungen[94], deren Haupttätigkeit nicht in der Verarbeitung personenbezogener Daten besteht, dabei unterstützen, ihrer diesbezüglichen Pflicht nachzukommen.

Verschiedene Branchenverbände haben Anstrengungen unternommen, um ihre Mitglieder zu sensibilisieren und zu informieren, beispielsweise durch Konferenzen und Seminare, indem sie Unternehmen über verfügbare Orientierungshilfen unterrichten oder einen Unterstützungsdienst zum Schutz der Privatsphäre entwickeln, den ihre Mitglieder nutzen können. Außerdem wird von einer zunehmenden Zahl von Seminaren, Treffen und Veranstaltungen berichtet, die von Denkfabriken und KMU-Verbänden zu Themen im Zusammenhang mit der DSGVO organisiert werden.

---

91 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai- ag-2017

92 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

93 Siehe Bericht der Multi-Stakeholder-Gruppe.

94 Siehe Beitrag des Ausschusses.

Um den freien Verkehr aller Daten innerhalb der EU zu verbessern und eine kohärente Anwendung der DSGVO und der Verordnung über den freien Verkehr nicht-personenbezogener Daten zu erreichen, hat die Kommission außerdem praktische Leitlinien zu den Vorschriften für die Verarbeitung gemischter Datensätze, die sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten bestehen, herausgegeben, welche sich insbesondere an KMU richten.[95]

Instrumentarium für Unternehmen

Die DSGVO sieht Instrumente vor, die dabei helfen, ihre Einhaltung nachzuweisen, wie Verhaltensregeln, Zertifizierungsverfahren und Standardvertragsklauseln.

- Verhaltensregeln

Der Ausschuss hat Leitlinien[96] herausgegeben, die „Urheber" bei der Erstellung, Änderung oder Ausweitung von Verhaltensregeln unterstützen und fördern sowie praktische Orientierungshilfe und Unterstützung bei der Auslegung geben sollen. In diesen Leitlinien werden außerdem die Verfahren für die Einreichung, Genehmigung und Veröffentlichung von Verhaltensregeln auf nationaler und europäischer Ebene erläutert, indem die zu erfüllenden Mindestkriterien aufgeführt werden.

Die Interessenträger erachten Verhaltensregeln als äußerst nützliche Instrumente. Obwohl viele Verhaltensregeln auf nationaler Ebene umgesetzt werden, wird derzeit eine Reihe EU-weiter Verhaltensregeln ausgearbeitet (z. B. zu mobilen Gesundheits-Apps, Gesundheitsforschung im Bereich Genomik, Cloud-Computing, Direktmarketing, Versicherung, Verarbeitung durch Präventions- und Beratungsdienste für Kinder).[97] Die Akteure sind der Ansicht, dass EU-weite Verhaltensregeln stärker propagiert werden sollten, da sie die einheitliche Anwendung der DSGVO in allen Mitgliedstaaten fördern.

Verhaltensregeln erfordern aber auch Zeit und Investitionen seitens der Akteure sowohl für deren Entwicklung als auch für die Einrichtung der erforderlichen unabhängigen Überwachungsstellen. Vertreter der KMU betonen, wie wichtig und hilfreich auf sie zugeschnittene Verhaltensregeln seien, die keine unverhältnismäßigen Kosten nach sich ziehen.

Folglich haben Wirtschaftsverbände in einer Reihe von Sektoren andere Arten von Selbstregulierungsinstrumenten eingeführt, z. B. Regeln der guten Praxis oder Leitfäden. Solche Instrumente können zwar nützliche Informationen liefern, sind aber nicht von den Datenschutzbehörden genehmigt und können nicht als Instrument zum Nachweis der Einhaltung der DSGVO dienen.

Der Ausschuss betont, dass bei Verhaltensregeln besonderes Augenmerk auf die Verarbeitung von Daten von Kindern sowie von Gesundheitsdaten gelegt werden müsse. Die Kommission unterstützt Verhaltensregeln, die zu einem einheitlichen

---

[95] Mitteilung der Kommission an das Europäische Parlament und den Rat: Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (COM(2019) 250 final).

[96] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_de.pdf

[97] Siehe Bericht der Multi-Stakeholder-Gruppe.

Ansatz in den Bereichen Gesundheit und Forschung beitragen und die grenzüberschreitende Verarbeitung personenbezogener Daten erleichtern werden.[98] Derzeit befasst sich der Ausschuss mit der Genehmigung mehrerer Entwürfe von Kriterien für die Akkreditierung von Stellen zur Überwachung der Verhaltensregeln, die von einigen Datenschutzbehörden eingebracht wurden.[99] Sobald den Datenschutzbehörden transnationale oder EU-weite Verhaltensregeln zur Genehmigung vorgelegt werden können, erfolgt eine Konsultation des Ausschusses. In Bereichen, in denen erhebliche Datenmengen (z. B. Cloud-Computing) oder sensible Daten (z. B. Gesundheitswesen und Forschung) verarbeitet werden, ist die rasche Einführung transnationaler Verhaltensregeln besonders wichtig.

- Zertifizierung

Die Zertifizierung kann ein nützliches Instrument sein, um die Einhaltung spezifischer Anforderungen der DSGVO nachzuweisen. Sie kann auf der Unternehmensseite zu mehr Rechtssicherheit führen und die DSGVO global stärker in den Fokus rücken.

Wie in der im April 2019 veröffentlichten Studie über die Zertifizierung[100] dargelegt, sollte das Ziel darin bestehen, die Einführung einschlägiger Regelungen zu erleichtern. Die Entwicklung von Zertifizierungssystemen in der EU wird durch die Leitlinien des Ausschusses zu Zertifizierungskriterien[101] und die Leitlinien zur Akkreditierung von Zertifizierungsstellen[102] unterstützt.

Sicherheit und Datenschutz durch Technikgestaltung sind wichtige Elemente, die es in Zertifizierungssystemen gemäß der DSGVO zu beachten gilt und die von einem gemeinsamen und ehrgeizigen EU-weiten Ansatz profitieren könnten. Die Kommission wird auch künftig die gegenwärtigen Kontakte zwischen der Agentur der Europäischen Union für Cybersicherheit (ENISA), den Datenschutzbehörden und dem Ausschuss unterstützen.

Im Bereich der Cybersicherheit forderte die Kommission nach Erlass des Rechtsakts zur Cybersicherheit die ENISA dazu auf, zwei Zertifizierungssysteme auszuarbeiten, darunter ein System für Cloud-Dienste.[103] Weitere Systeme im Bereich der Cybersicherheit von Diensten und Produkten für Verbraucher werden derzeit geprüft. Auch wenn sich diese im Rahmen des Rechtsakts zur Cybersicherheit entwickelten Zertifizierungssysteme nicht ausdrücklich auf den Datenschutz und die Privatsphäre beziehen, tragen sie dennoch dazu bei, das Vertrauen der Verbraucher in digitale Dienste und Produkte zu stärken. Solche Systeme können als Nachweis für die Einhaltung des Grundsatzes der Sicherheit durch Technikgestaltung sowie für die

---

98 Siehe hierzu die in der Europäischen Datenstrategie angekündigten Maßnahmen, S. 35.

99 Nach Artikel 41 Absatz 3 der DSGVO. Siehe Stellungnahmen des Ausschusses unter: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de.

100 https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en

101 https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_en

102 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_de.pdf. Mehrere Aufsichtsbehörden haben dem Ausschuss bereits ihre Akkreditierungsanforderungen sowohl für die Stellen für die Überwachung der Einhaltung der Verhaltensregeln als auch für die Zertifizierungsstellen vorgelegt. Ein Überblick ist zu finden unter: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de.

103 https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

Umsetzung geeigneter technischer und organisatorischer Maßnahmen im Zusammenhang mit der sicheren Verarbeitung personenbezogener Daten dienen.

- Standardvertragsklauseln

Die Kommission arbeitet an Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter[104], auch mit Blick auf die Aktualisierung der Standardvertragsklauseln für internationale Datenübermittlungen (siehe Abschnitt 7.2.). Ein von der Kommission erlassener Rechtsakt der Union wird EU-weit verbindlich sein und eine vollständige Harmonisierung sowie Rechtssicherheit gewährleisten.

6 DIE ANWENDUNG DER DSGVO AUF NEUE TECHNOLOGIEN

Ein für neue Technologien offener technologieneutraler Rahmen

Die DSGVO ist technologieneutral, schafft Vertrauen und beruht auf Datenschutzgrundsätzen.[105] Diese Grundsätze, darunter die rechtmäßige und transparente Verarbeitung, die Zweckbindung und die Datenminimierung, bieten unabhängig von den angewandten Verarbeitungsvorgängen und -techniken eine solide Grundlage für den Schutz personenbezogener Daten.

Den Mitgliedern der Multi-Stakeholder-Gruppe zufolge hat die DSGVO insgesamt positive Auswirkungen auf die Entwicklung neuer Technologien und bietet eine gute Grundlage für Innovation. Die DSGVO wird als wichtiges und flexibles Instrument erachtet, um die Entwicklung neuer Technologien im Einklang mit den Grundrechten sicherzustellen. Die Umsetzung ihrer wichtigsten Grundsätze ist insbesondere bei einer datenintensiven Verarbeitung von Bedeutung. Der risikobasierte und technologieneutrale Ansatz der DSGVO bietet ein angemessenes Datenschutzniveau, um Verarbeitungsrisiken, auch in Verbindung mit neuen Technologien, zu begegnen.

Insbesondere weisen die Interessenträger darauf hin, dass die Grundsätze der DSGVO in Bezug auf die Zweckbindung und die mit dem ursprünglichen Erhebungszweck vereinbare Weiterverarbeitung, die Datenminimierung, Speicherbegrenzung, Transparenz, Rechenschaftspflicht und die Bedingungen, unter denen automatisierte Entscheidungsprozesse[106] rechtmäßig eingesetzt werden können, den Bedenken im Zusammenhang mit der Nutzung künstlicher Intelligenz weitgehend Rechnung tragen.

Der zukunftssichere und risikobasierte Ansatz der DSGVO wird auch im möglichen künftigen Rahmen für künstliche Intelligenz und bei der Umsetzung der Datenstrategie Anwendung finden. Die Datenstrategie zielt darauf ab, die Datenverfügbarkeit zu fördern und gemeinsame europäische Datenräume zu schaffen, die von Diensten in Bezug auf zusammengeschlossene Cloud-Infrastrukturen unterstützt werden. Was den Schutz personenbezogener Daten anbelangt, bildet die DSGVO den wichtigsten Rechtsrahmen, innerhalb dessen je nach Art und Inhalt der

---

[104] Artikel 28 Absatz 7 der DSGVO.

[105] Wie der Rat, das Europäische Parlament und der Ausschuss in ihren Beiträgen zur Bewertung hervorgehoben haben.

[106] Die Interessenträger stellen jedoch fest, dass nicht alle automatisierten Entscheidungsprozesse im Kontext der künstlichen Intelligenz unter Artikel 22 DSGVO fallen.

einzelnen Datenräume von Fall zu Fall wirksame Lösungen entwickelt werden können.

Die DSGVO hat das Bewusstsein für den Schutz personenbezogener Daten sowohl innerhalb als auch außerhalb der EU geschärft und die Unternehmen dazu veranlasst, ihre Verfahren anzupassen, um den Datenschutzgrundsätzen bei Innovationen Rechnung zu tragen. Laut Organisationen der Zivilgesellschaft haben sich die Praktiken großer digitaler Akteure bisher jedoch noch nicht grundlegend in Richtung einer datenschutzfreundlicheren Verarbeitung entwickelt, auch wenn der Einfluss der DSGVO auf die Entwicklung neuer Technologien positiv erscheint. Eine strenge und wirksame Durchsetzung der DSGVO gegenüber großen Online-Plattformen und integrierten Unternehmen, darunter in Bereichen wie Online-Werbung und Mikrotargeting, ist entscheidend für den Schutz der Bürgerinnen und Bürger.

Im Rahmen des Legislativpakets über digitale Dienste[107] untersucht die Kommission gegenwärtig weitreichendere Fragen bezüglich des Marktverhaltens großer digitaler Akteure. Im Hinblick auf Forschung im Bereich der sozialen Medien weist die Kommission darauf hin, dass die DSGVO von den Plattformen der sozialen Medien nicht als Vorwand genutzt werden könne, um den Zugang von Forschern und Faktenprüfern zu nicht-personenbezogenen Daten zu beschränken, zum Beispiel Statistiken darüber, welche Personengruppen welche Werbung erhalten, die Kriterien für die Gestaltung dieser gezielten Werbung, Informationen über gefälschte Konten usw.

Der technologieneutrale und zukunftssichere Ansatz der DSGVO stand während der COVID-19-Pandemie auf dem Prüfstand und hat sich als erfolgreich erwiesen. Die auf Datenschutzgrundsätzen basierten Vorschriften der DSGVO unterstützten die Entwicklung von Instrumenten zur Bekämpfung und Überwachung der Ausbreitung des Virus.

Anstehende Herausforderungen

Durch die Entwicklung und Anwendung neuer Technologien werden diese Datenschutzgrundsätze nicht infrage gestellt. Die Herausforderungen liegen in der Klarstellung dahingehend, wie die bewährten Datenschutzgrundsätze auf die Nutzung bestimmter Technologien wie künstliche Intelligenz, Blockchain, das Internet der Dinge, die Gesichtserkennung oder die Quanteninformatik angewendet werden können.

In diesem Zusammenhang betonten das Europäische Parlament und der Rat, dass eine kontinuierliche Überwachung erforderlich sei, um zu klären, wie die DSGVO auf neue Technologien und Big-Tech-Unternehmen Anwendung findet. Darüber hinaus mahnten die Interessenträger an, dass eine Bewertung dessen, ob die DSGVO weiterhin ihren Zweck erfüllt, ebenfalls eine ständige Überwachung erfordere.

Interessenträgern aus der Industrie zufolge setzt Innovation voraus, dass die DSGVO grundsatzbezogen und im Einklang mit ihrer Konzeption und nicht auf starre und formelle Weise angewendet wird. Sie sind der Ansicht, dass Leitlinien des Ausschusses im Hinblick auf die Anwendung der Grundsätze, Begriffe und Vorschriften der DSGVO auf neue Technologien wie künstliche Intelligenz,

[107] https://ec.europa.eu/commission/presscorner/detail/de/ip_20_962

Blockchain oder Internet der Dinge unter Berücksichtigung des risikobasierten Ansatzes zu Klarstellungen und mehr Rechtssicherheit beitragen würden. Solche Soft-Law-Instrumente seien gut geeignet, die Anwendung der DSGVO auf die neuen Technologien zu begleiten, da sie mehr Rechtssicherheit bieten und entsprechend den technologischen Entwicklungen überarbeitet werden können. Einige Interessenträger schlagen auch vor, dass sektorspezifische Leitlinien dahingehend, wie die DSGVO auf neue Technologien anzuwenden ist, hilfreich sein könnten.

Der Ausschuss erklärte, dass er die Auswirkungen neu entstehender Technologien auf den Schutz personenbezogener Daten weiterhin prüfen werde.

Die Interessenträger betonen ferner, wie wichtig es für die Regulierungsbehörden sei, ein gründliches Verständnis davon zu erlangen, wie Technologien genutzt werden, und in einen Dialog mit der Industrie über die Entwicklung neu entstehender Technologien zu treten. Ihrer Auffassung nach könnte der Ansatz eines „regulatorischen Sandkastens" – als Mittel für Orientierungshilfen bezüglich der Anwendung der Vorschriften – eine interessante Option sein, um neue Technologien zu erproben und Unternehmen dabei zu unterstützen, den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen innerhalb neuer Technologien anzuwenden.

Im Hinblick auf weitere politische Maßnahmen empfehlen die Interessenträger, dass künftige politische Vorschläge zu künstlicher Intelligenz auf den bestehenden Rechtsrahmen aufbauen und auf die DSGVO ausgerichtet sein sollten. Bevor neue verbindliche Vorschriften vorgeschlagen werden, sollten potenzielle spezifische Fragen auf der Grundlage einschlägiger Erkenntnisse sorgfältig geprüft werden.

Das Weißbuch der Kommission zur Künstlichen Intelligenz enthält eine Reihe politischer Optionen, zu denen die Interessenträger bis zum 14. Juni 2020 Stellung nehmen sollten. In Bezug auf die Gesichtserkennung, eine Technologie, die sich erheblich auf die Rechte des Einzelnen auswirken kann, wird im Weißbuch auf den derzeitigen Rechtsrahmen verwiesen. Ferner wird eine öffentliche Debatte über die möglichen besonderen Umstände, die die Nutzung künstlicher Intelligenz für die Gesichtserkennung und für andere Zwecke der biometrischen Fernidentifikation im öffentlichen Raum rechtfertigen könnten, sowie über gemeinsame Sicherheitsvorkehrungen eingeleitet.

7 INTERNATIONALE DATENÜBERMITTLUNGEN UND GLOBALE ZUSAMMENARBEIT

7.1 Schutz der Privatsphäre: ein weltweites Anliegen

Die Forderung nach Schutz personenbezogener Daten kennt keine Grenzen, da Menschen auf der ganzen Welt zunehmend Wert auf den Schutz und die Sicherheit ihrer Daten legen.

Gleichzeitig ist die Bedeutung des Datenverkehrs für Personen, Regierungen, Unternehmen und allgemein für die Gesellschaft eine unausweichliche Tatsache in unserer vernetzten Welt. Der Datenverkehr ist ein integrierter Bestandteil beim Handel, bei der Zusammenarbeit zwischen Behörden und bei sozialen Interaktionen. In diesem Zusammenhang zeigt die derzeitige COVID-19-Pandemie auch, wie wichtig die Übermittlung und der Austausch personenbezogener Daten für viele unbedingt notwendige Tätigkeiten sind, darunter die Gewährleistung der

Aufrechterhaltung von Regierungsgeschäften und des Geschäftsbetriebs von Unternehmen – indem Telearbeit und andere Lösungen, die in hohem Maße auf Informations- und Kommunikationstechnologien beruhen, ermöglicht werden –, die Zusammenarbeit in der wissenschaftlichen Forschung bei Diagnose, Therapie und Impfstoffen sowie die Bekämpfung neuer Formen der Cyberkriminalität wie Online-Betrugsmechanismen, die gefälschte Arzneimittel anbieten, welche vorgeben, COVID-19 zu verhindern oder zu heilen.

Vor diesem Hintergrund müssen mehr denn je der Schutz der Privatsphäre und die Erleichterung des Datenverkehrs Hand in Hand gehen. Die EU ist mit ihrer Datenschutzregelung, die Offenheit für die internationale Übermittlung von Daten mit einem hohen Schutzniveau für den Einzelnen verbindet, sehr gut aufgestellt, um den sicheren und vertrauenswürdigen Datenverkehr zu fördern. Die DSGVO hat sich auf internationaler Ebene bereits als Bezugspunkt etabliert und für viele Länder in der ganzen Welt als Katalysator gewirkt, die Einführung moderner Datenschutzvorschriften in Erwägung zu ziehen.

Dieser tatsächlich weltweite Trend ist unter anderem in Chile, Südkorea, Brasilien, Japan, Kenia, Indien, Tunesien, Indonesien, Kalifornien und Taiwan, um nur einige zu nennen, zu beobachten. Diese Entwicklungen sind nicht nur in quantitativer, sondern auch in qualitativer Hinsicht bemerkenswert: Viele der Datenschutzgesetze, die kürzlich verabschiedet wurden oder deren Verabschiedung derzeit läuft, beruhen auf einem grundlegenden Paket gemeinsamer Garantien, Rechte und Durchsetzungsmechanismen, welche von der EU geteilt werden. In einer Welt, die allzu oft durch unterschiedliche, wenn nicht sogar divergierende Regulierungskonzepte gekennzeichnet ist, ist dieser Trend hin zu einer globalen Annäherung eine äußerst positive Entwicklung, die neue Chancen für einen besseren Schutz des Einzelnen in Europa eröffnet und gleichzeitig den Datenverkehr erleichtert und die Übermittlungskosten für die Unternehmen senkt.

Um diese Chancen zu nutzen und die in ihrer Mitteilung über den Austausch und Schutz personenbezogener Daten in einer globalisierten Welt[108] aus dem Jahr 2017 dargelegte Strategie umzusetzen, hat die Kommission ihre Arbeit im Hinblick auf die internationale Dimension des Datenschutzes erheblich intensiviert, indem sie – wie nachstehend erläutert – das verfügbare Instrumentarium für Datenübermittlungen voll ausgeschöpft hat. Hierzu zählte auch die aktive Zusammenarbeit mit wichtigen Partnern, um zu einer „Angemessenheitsfeststellung“ zu gelangen, sowie die Erzielung bedeutsamer Ergebnisse, wie die Schaffung des weltweit größten Raums für freien und sicheren Datenverkehr zwischen der EU und Japan.

Neben ihrer Arbeit in Bezug auf Angemessenheitsfeststellungen und -beschlüsse hat die Kommission mit den Datenschutzbehörden innerhalb des Ausschusses sowie mit anderen Interessenträgern eng zusammengearbeitet, um die flexiblen Vorschriften der DSGVO in Bezug auf internationale Datenübermittlungen in vollem Umfang zu nutzen. Dies betrifft die Modernisierung von Instrumenten wie Standardvertragsklauseln, die Entwicklung von Zertifizierungssystemen,

[108] Mitteilung der Kommission an das Europäische Parlament und den Rat: Austausch und Schutz personenbezogener Daten in einer globalisierten Welt, 10.1.2017 (COM(2017) 7 final).

Verhaltensregeln oder Verwaltungsvereinbarungen für den Datenaustausch zwischen Behörden sowie die Klarstellung von Schlüsselkonzepten, die beispielsweise den räumlichen Anwendungsbereich der EU-Datenschutzvorschriften oder die Anwendung sogenannter „Ausnahmen“ für die Übermittlung personenbezogener Daten betreffen.

Und nicht zuletzt hat die Kommission ihren Dialog in mehreren bilateralen, regionalen und multilateralen Foren verstärkt, um eine globale Kultur der Achtung der Privatsphäre zu fördern und Elemente der Angleichung zwischen verschiedenen Datenschutzsystemen zu entwickeln. Bei ihren Bemühungen konnte die Kommission sich auf die aktive Unterstützung durch den Europäischen Auswärtigen Dienst und das Netz der EU-Delegationen in Drittländern und der Vertretungen bei internationalen Organisationen stützen. Auf diese Weise wurden bei den verschiedenen Aspekten der externen Dimension der EU-Politik – vom Handel bis hin zur neuen Partnerschaft zwischen Afrika und der EU – auch Kohärenz und eine größere Komplementarität sichergestellt.

7.2 Das Instrumentarium der DSGVO für Datenübermittlungen

Da immer mehr private und öffentliche Akteure im Rahmen ihrer routinemäßigen Tätigkeiten auf internationalen Datenverkehr angewiesen sind, besteht ein steigender Bedarf an flexiblen Instrumenten, die an verschiedene Sektoren, Geschäftsmodelle und Übermittlungssituationen angepasst werden können. Um diesem Bedarf Rechnung zu tragen, bietet die DSGVO ein modernisiertes Instrumentarium, das die Übermittlung personenbezogener Daten aus der EU an Drittländer und internationale Organisationen erleichtert und gleichzeitig ein hohes Datenschutzniveau gewährleistet. Ein solcher kontinuierlicher Schutz ist wichtig, da der Datenverkehr in der heutigen Welt grenzüberschreitend ist und die durch die DSGVO garantierten Schutzmaßnahmen, würden sie auf eine Verarbeitung innerhalb der EU beschränkt, unvollständig wären.

Mit Kapitel V der DSGVO bestätigte der Gesetzgeber die Struktur der Übermittlungsvorschriften, die bereits gemäß der Richtlinie 95/46/EG bestanden hatten: Datenübermittlungen können stattfinden, wenn die Kommission eine Angemessenheitsfeststellung in Bezug auf ein Drittland oder eine internationale Organisation getroffen hat oder wenn mangels einer solchen Feststellung der Verantwortliche oder der Auftragsverarbeiter in der EU („Datenexporteur“) geeignete Garantien, beispielsweise durch einen Vertrag mit dem Empfänger („Datenimporteur“), bereitgestellt hat. Darüber hinaus sind weiterhin gesetzliche Gründe für Datenübermittlungen (sogenannte Ausnahmen) für bestimmte Situationen verfügbar, in Bezug auf die der Gesetzgeber entschieden hat, dass aufgrund einer Interessenabwägung eine Datenübermittlung unter bestimmten Bedingungen möglich ist. Gleichzeitig wurden die bestehenden Vorschriften durch die Reform klarer gefasst und vereinfacht, indem beispielsweise die Bedingungen für eine Angemessenheitsfeststellung oder für verbindliche interne Datenschutzvorschriften im Einzelnen festgelegt, die Genehmigungsanforderungen auf sehr wenige spezifische Fälle beschränkt und Meldepflichten vollständig abgeschafft wurden. Darüber hinaus wurden neue Instrumente für Datenübermittlungen wie Verhaltensregeln oder Zertifizierungssysteme eingeführt und die Möglichkeiten für die Nutzung bestehender Instrumente (z. B. Standardvertragsklauseln) erweitert.

Die heutige digitale Wirtschaft ermöglicht es ausländischen Wirtschaftsteilnehmern, (aus der Ferne) direkt am EU-Binnenmarkt teilzunehmen und um europäische Kunden und deren personenbezogene Daten zu konkurrieren. Sofern ausländische Wirtschaftsteilnehmer ihr Waren- oder Dienstleistungsangebot speziell an europäische Verbraucher richten oder deren Verhalten beobachten, sollten sie in gleicher Weise wie in der EU angesiedelte Wirtschaftsteilnehmer Unionsrecht einhalten. Dieser Sachverhalt spiegelt sich in Artikel 3 der DSGVO wider, der die unmittelbare Anwendbarkeit der EU-Datenschutzvorschriften auf bestimmte Verarbeitungsvorgänge von nicht in der EU niedergelassenen Verantwortlichen und Auftragsverarbeitern ausdehnt. Dadurch werden die erforderlichen Garantien und obendrein gleiche Wettbewerbsbedingungen für alle auf dem Unionsmarkt tätigen Unternehmen gewährleistet.

Ihre breite Reichweite ist einer der Gründe, warum die Auswirkungen der DSGVO auch in anderen Teilen der Welt spürbar waren. Die ausführlichen Leitlinien, die der Ausschuss im Anschluss an eine umfassende öffentliche Konsultation zum räumlichen Anwendungsbereich der DSGVO herausgegeben hat, sind daher wichtig, um ausländische Wirtschaftsteilnehmer, unter anderem durch konkrete Beispiele, bei der Bestimmung dessen zu unterstützen, ob und welche Verarbeitungstätigkeiten unmittelbar den in der DSGVO genannten Garantien unterliegen.[109]

Die Ausweitung des Anwendungsbereichs des EU-Datenschutzrechts allein reicht jedoch nicht aus, um dessen Einhaltung in der Praxis zu garantieren. Wie auch der Ausschuss betont hat[110], ist es von entscheidender Bedeutung, die Einhaltung der Vorschriften durch ausländische Wirtschaftsteilnehmer und ihre wirksame Durchsetzung gegenüber diesen Wirtschaftsteilnehmern sicherzustellen. Die Benennung eines Vertreters in der EU (Artikel 27 Absätze 1 und 2 der DSGVO), an den sich Einzelpersonen und Aufsichtsbehörden zusätzlich zu dem im Ausland operierenden verantwortlichen Unternehmen oder an dessen Stelle wenden können[111], sollte in dieser Hinsicht eine Schlüsselrolle spielen. Dieser Ansatz, der zunehmend auch in anderen Kontexten[112] übernommen wird, sollte energischer verfolgt werden, um klar zu machen, dass ausländische Unternehmen ohne Niederlassung in der EU nicht von ihrer Verantwortung gemäß der DSGVO entbunden sind. Kommen diese Wirtschaftsteilnehmer ihrer Verpflichtung zur Benennung eines Vertreters nicht nach[113], sollten die Aufsichtsbehörden das in Artikel 58 der DSGVO zur

---

[109] EDSA, Leitlinien 2/2018 zum räumlichen Anwendungsbereich der DSGVO, 12.11.2019. In den Leitlinien werden mehrere der bei der öffentlichen Konsultation angesprochenen Punkte behandelt, z. B. die Auslegung der Kriterien für die Zielgerichtetheit und die Überwachung.

[110] Siehe Standpunkt und Feststellungen des Rates, Rn. 34, 35 und 38.

[111] Siehe Artikel 27 Absatz 4 und Erwägungsgrund 80 der DSGVO: „Bei Verstößen des Verantwortlichen oder Auftragsverarbeiters sollte der bestellte Vertreter Durchsetzungsverfahren unterworfen werden."

[112] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren (COM(2018) 226 final), Artikel 3; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte (COM(2018) 640 final), Artikel 16 Absätze 2 und 3.

[113] In einer Stellungnahme zur öffentlichen Konsultation ist einer der wichtigsten Punkte, die angegangen werden müssen, die wirksame Durchsetzung und die tatsächlichen Folgen für diejenigen, die diese Anforderung ignorieren Dabei sollte insbesondere berücksichtigt werden, dass dadurch in der Union niedergelassene Unternehmen zudem Wettbewerbsnachteile gegenüber nicht

Durchsetzung vorgesehene Instrumentarium (z. B. öffentliche Warnungen, ein vorübergehendes oder endgültiges Verbot der Verarbeitung in der EU, Durchsetzung gegenüber gemeinsam für die Verarbeitung Verantwortlichen mit Sitz in der EU) in vollem Umfang nutzen.

Letztendlich ist es sehr wichtig, dass der Ausschuss seine Arbeit zur weiteren Klärung des Zusammenhangs zwischen Artikel 3 über die unmittelbare Anwendung der DSGVO und den Vorschriften über internationale Datenübermittlungen in Kapitel V zum Abschluss bringt.[114]

Angemessenheitsbeschlüsse

Die Beiträge von Interessenträgern bestätigen, dass Angemessenheitsbeschlüsse für Wirtschaftsteilnehmer in der EU nach wie vor ein wesentliches Instrument für die sichere Übermittlung personenbezogener Daten in Drittländer sind.[115] Solche Beschlüsse sind die umfassendste, einfachste und kostengünstigste Lösung für Datenübermittlungen, da sie mit Datenübermittlungen innerhalb der EU gleichzusetzen sind und somit den sicheren und freien Verkehr personenbezogener Daten ohne weitere Bedingungen oder eine Genehmigungspflicht gewährleisten. Angemessenheitsbeschlüsse eröffnen demnach EU-Wirtschaftsteilnehmern kommerzielle Kanäle und erleichtern die Zusammenarbeit zwischen den Behörden bei gleichzeitiger Gewährung eines privilegierten Zugangs zum EU-Binnenmarkt. Aufbauend auf der Praxis gemäß der Richtlinie von 1995 sieht die DSGVO ausdrücklich vor, dass die Angemessenheit für ein bestimmtes Gebiet oder einen bestimmten Sektor oder Wirtschaftszweig in einem Drittland festgestellt werden kann (sogenannte „teilweise“ Angemessenheit).

Die DSGVO baut auf den Erfahrungen der vergangenen Jahre und den Klarstellungen des Gerichtshofs auf, indem ein detaillierter Katalog von Elementen festgelegt wird, die die Kommission bei ihrer Bewertung berücksichtigen muss. Der Angemessenheitsstandard verlangt ein Schutzniveau, das mit dem in der EU gewährleisteten vergleichbar (bzw. „der Sache nach gleichwertig “) ist.[116] Hierzu zählt eine umfassende Bewertung des gesamten Systems des Drittlands, einschließlich des Inhalts der Datenschutzvorschriften, ihrer wirksamen Umsetzung und Durchsetzung sowie der Vorschriften über den Zugang der Behörden zu

---

konformen Unternehmen erleiden, die außerhalb der Union niedergelassen sind und in der Union Handel treiben.“ Siehe Stellungnahme der EU-Wirtschaftspartner vom 29. April 2020.

[114] Dieser Punkt wurde in mehreren Beiträgen im Rahmen der öffentlichen Konsultation angesprochen, beispielsweise in Bezug auf die Übermittlung personenbezogener Daten an Empfänger außerhalb der EU, die jedoch unter die DSGVO fallen.

[115] Standpunkt und Feststellungen des Rates, Rn. 17; Beitrag des Ausschusses, S. 5/6. In mehreren Stellungnahmen im Rahmen der öffentlichen Konsultation, unter anderem von einer Reihe von Wirtschaftsverbänden (z. B. dem französischen Verband für Großunternehmen, Digital Europe, der Global Data Alliance/BSA, der Computer & Communication Industry Association (CCIA) oder der US-Handelskammer), wurde eine Intensivierung der Arbeit an Angemessenheitsfeststellungen gefordert, insbesondere mit wichtigen Handelspartnern.

[116] Urteil des Gerichtshofs vom 6. Oktober 2015, Maximillian Schrems/Data Protection Commissioner („Schrems I“), C-362/14, Rn. 73, 74 und 96. Siehe auch Erwägungsgrund 104 der DSGVO, in dem auf den Grundsatz der „Gleichwertigkeit der Sache nach“ Bezug genommen wird.

personenbezogenen Daten, insbesondere zu Zwecken der Strafverfolgung und der nationalen Sicherheit.[117]

Diese Forderung spiegelt sich auch in den Leitlinien wider, die von der ehemaligen Artikel-29-Datenschutzgruppe angenommen (und vom Ausschuss gebilligt) wurden, insbesondere in der „Referenzgrundlage für Angemessenheit", in der die Elemente näher erläutert werden, die die Kommission bei ihrer Beurteilung der Angemessenheit berücksichtigen muss, unter anderem durch eine Übersicht über die „wesentlichen Garantien" für den Zugang von Behörden zu personenbezogenen Daten.[118] Letzterer stützt sich insbesondere auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte. Der Grundsatz der „Gleichwertigkeit der Sache nach" besagt zwar nicht, dass die EU-Vorschriften Punkt für Punkt wiederzugeben (zu „kopieren") sind, da die Mittel zur Gewährleistung eines vergleichbaren Schutzniveaus je nach Datenschutzsystem unterschiedlich sein können und häufig unterschiedliche Rechtstraditionen widerspiegeln, verlangt aber dennoch ein hohes Schutzniveau.

Dieser Grundsatz ist dadurch gerechtfertigt, dass ein Angemessenheitsbeschluss die Vorteile des Binnenmarkts im Hinblick auf den freien Datenverkehr im Wesentlichen auf ein Drittland ausdehnt. Das bedeutet aber auch, dass es bisweilen erhebliche Unterschiede zwischen dem in dem betreffenden Drittland gewährleisteten Schutzniveau und der DSGVO gibt, die überbrückt werden müssen, beispielsweise durch Verhandlungen über zusätzliche Garantien. Solche Garantien sollten positiv bewertet werden, da sie den Schutz, der Personen in der EU zur Verfügung steht, weiter stärken. Gleichzeitig stimmt die Kommission mit dem Ausschuss darin überein, dass es wichtig ist, die Anwendung der Garantien in der Praxis kontinuierlich zu überwachen, wozu auch eine wirksame Durchsetzung durch die Datenschutzbehörde des Drittlands gehört.[119]

In der DSGVO wird klargestellt, dass Angemessenheitsbeschlüsse „lebendige Instrumente" sind, die fortlaufend überwacht und regelmäßig überprüft werden sollten.[120] Im Einklang mit diesen Anforderungen tauscht sich die Kommission regelmäßig mit den zuständigen Behörden aus, um neue Entwicklungen proaktiv zu verfolgen. Beispielsweise wurden seit Annahme des Beschlusses über das EU-US-Datenschutzschild im Jahr 2016[121] zusammen mit den Vertretern des Ausschusses

---

[117] Artikel 45 Absatz 2 und Erwägungsgrund 104 der DSGVO. Siehe auch Schrems I, Rn. 75 und 91.

[118] Referenzgrundlage für Angemessenheit, WP 254/rev.01, 6. Februar 2018 (abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

[119] Beitrag des Ausschusses, S. 5/6.

[120] Nach Artikel 45 Absätze 4 und 5 der DSGVO ist die Kommission verpflichtet, die Entwicklungen in Drittländern fortlaufend zu überwachen und eine Angemessenheitsfeststellung regelmäßig – mindestens alle vier Jahre – zu überprüfen. Ferner wird der Kommission dadurch die Befugnis verliehen, einen Angemessenheitsbeschluss aufzuheben, zu ändern oder auszusetzen, wenn sie feststellt, dass das betreffende Land oder die betreffende internationale Organisation kein angemessenes Schutzniveau mehr gewährleistet. Außerdem muss die Kommission nach Artikel 97 Absatz 2 Buchstabe a der DSGVO dem Europäischen Parlament und dem Rat 2020 einen Bewertungsbericht vorlegen. Siehe auch Urteil des Gerichtshofs vom 6. Oktober 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, Rn. 76.

[121] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes. Dieser Angemessenheitsbeschluss ist ein Sonderfall, der sich in Ermangelung allgemeiner Datenschutzvorschriften in den USA auf Zusagen der teilnehmenden Unternehmen (die nach US-amerikanischem Recht durchsetzbar sind) zur

drei jährliche Überprüfungen durchgeführt, um alle Aspekte der Funktionsweise dieses Datenschutzschildes zu bewerten.[122] Diese Überprüfungen stützten sich auf Informationen, die durch den Austausch mit den US-Behörden gewonnen wurden, sowie auf Beiträge anderer Interessenträger wie EU-Datenschutzbehörden, der Zivilgesellschaft und Branchenverbände. Auf diese Weise konnte die praktische Funktionsweise verschiedener Elemente des Datenschutzschildes verbessert werden. Im weiteren Sinne trugen die jährlichen Überprüfungen dazu bei, einen umfassenderen Dialog mit der US-Regierung über Datenschutz im Allgemeinen sowie die Einschränkungen und Garantien in Bezug auf die nationale Sicherheit im Besonderen aufzubauen.

Im Rahmen der ersten Bewertung der DSGVO ist die Kommission auch verpflichtet, die nach der Richtlinie von 1995 angenommenen Angemessenheitsbeschlüsse zu überprüfen.[123] Die Kommissionsdienststellen haben einen intensiven Dialog mit jedem der elf betroffenen Länder und Gebiete eingeleitet, um zu bewerten, wie sich deren Systeme zum Schutz personenbezogener Daten seit der Annahme des Angemessenheitsbeschlusses entwickelt haben und ob diese Systeme die in der DSGVO festgelegten Standards erfüllen. Die Notwendigkeit, die Kontinuität dieser Beschlüsse zu gewährleisten, da sie ein wichtiges Instrument für den Handel und die internationale Zusammenarbeit sind, ist einer der Faktoren, der mehrere dieser Länder und Gebiete dazu bewogen hat, ihre Datenschutzgesetze zu aktualisieren und zu verstärken. Das sind in jedem Fall begrüßenswerte Entwicklungen. Mit einigen dieser Länder und Gebiete werden derzeit weitere Garantien erörtert, um wesentliche Unterschiede hinsichtlich des Datenschutzes anzugehen.

Da der Gerichtshof in seinem am 16. Juli zu verkündenden Urteil möglicherweise Klarstellungen liefert, die für bestimmte Elemente des Angemessenheitsstandards relevant sein könnten, wird die Kommission über die Bewertung der vorstehend erwähnten elf Angemessenheitsbeschlüsse gesondert Bericht erstatten, nachdem der Gerichtshof sein Urteil in dieser Rechtssache erlassen hat.[124]

Anwendung der in dieser Regelung festgelegten Datenschutzstandards stützt. Darüber hinaus stützt sich der Datenschutzschild auf die spezifischen Erklärungen und Zusicherungen der US-Regierung in Bezug auf die Sammlung und Nutzung personenbezogener Daten aus Gründen der nationalen Sicherheit, welche die Angemessenheitsfeststellung untermauern.

122 Überprüfungen fanden 2017 (Bericht der Kommission an das Europäische Parlament und Rat – Erster Bericht zur jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds (COM(2017) 611 final)), 2018 (Bericht der Kommission an das Europäische Parlament und den Rat zur zweiten jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds (COM(2018) 860 final)) und 2019 (Bericht der Kommission an das Europäische Parlament und den Rat zur dritten jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds (COM(2019) 495 final)) statt.

123 Diese bestehenden Angemessenheitsbeschlüsse betreffen Länder, die eng mit der Europäischen Union und ihren Mitgliedstaaten verbunden sind (Schweiz, Andorra, Faröer, Guernsey, Jersey, Insel Man), wichtige Handelspartner (z. B Argentinien, Kanada, Israel) und Länder, die eine Vorreiterrolle bei der Entwicklung von Datenschutzgesetzen in ihrer Region spielten (Neuseeland, Uruguay).

124 In der Rechtssache C-311/18, Data Protection Commissioner/Facebook Ireland Limited und Maximillian Schrems („Schrems II“), geht es um eine Vorlage zur Vorabentscheidung über sogenannte Standardvertragsklauseln. Bestimmte Aspekte des Angemessenheitsstandards könnten jedoch durch den Gerichtshof noch weiter präzisiert werden. Die mündliche Verhandlung in dieser Sache fand am 9. Juli 2019 statt, und das Urteil wurde am 16. Juli 2020 verkündet.

Zur Umsetzung der in ihrer Mitteilung über den Austausch und Schutz personenbezogener Daten in einer globalisierten Welt von 2017 dargelegten Strategie hat die Kommission ebenfalls neue Angemessenheitsdialoge aufgenommen.[125] Diese Arbeit hat bereits zu bedeutenden Ergebnissen geführt, an denen wichtige Partner der EU beteiligt waren. Im Januar 2019 nahm die Kommission ihren Angemessenheitsbeschluss für Japan an, der auf einem hohen Maß an Konvergenz beruht, unter anderem durch spezifische Garantien zum Beispiel im Bereich der Weiterübermittlung personenbezogener Daten und durch die Schaffung eines Mechanismus zur Untersuchung und Beilegung von Individualbeschwerden über den Zugang staatlicher Behörden zu personenbezogenen Daten aus Gründen der Strafverfolgung und der nationalen Sicherheit.

Als erste Angemessenheitsfeststellung, die im Rahmen der DSGVO angenommen wurde, bietet der mit Japan vereinbarte Rahmen einen nützlichen Präzedenzfall für künftige Beschlüsse.[126] Dazu gehört auch die Tatsache, dass sie auf japanischer Seite durch eine „Angemessenheitsfeststellung" für die EU erwidert wurde. Diese gegenseitigen Angemessenheitsfeststellungen bilden zusammen den weltweit größten Raum für einen sicheren und freien Verkehr personenbezogener Daten und ergänzen damit das Wirtschaftspartnerschaftsabkommen zwischen der EU und Japan. Die Vereinbarung unterstützt den Handel mit Waren im Wert von rund 124 Mrd. EUR und den Handel mit Dienstleistungen im Wert von 42,5 Mrd. EUR jährlich.

Das Angemessenheitsverfahren mit Südkorea befindet sich ebenfalls in einem fortgeschrittenen Stadium. Ein wichtiges Ergebnis ist die jüngste Gesetzesreform Südkoreas, die zur Einrichtung einer unabhängigen Datenschutzbehörde mit starken Durchsetzungsbefugnissen geführt hat. Dies zeigt, wie ein Angemessenheitsdialog zu einer stärkeren Annäherung zwischen den Datenschutzvorschriften der EU und denen eines anderen Landes beitragen kann.

Die Kommission stimmt der Aufforderung der Interessenträger voll und ganz zu, den Dialog mit ausgewählten Drittländern im Hinblick auf mögliche neue Angemessenheitsfeststellungen zu intensivieren.[127] Sie prüft diese Möglichkeit aktiv mit anderen wichtigen Partnern in Asien, Lateinamerika und der Nachbarschaft

---

[125] Siehe Fußnote 109 oben. Die Kommission erklärte, dass bei der Bewertung der Frage, mit welchen Drittländern ein Dialog über die Angemessenheit geführt werden sollte, folgende Kriterien berücksichtigt werden: i) der Umfang der (tatsächlichen oder potenziellen) Handelsbeziehungen der EU zu dem jeweiligen Drittland, einschließlich der Frage, ob ein Freihandelsabkommen besteht oder entsprechende Verhandlungen im Gange sind, ii) der Umfang der Übermittlung personenbezogener Daten aus der EU in das Drittland, der die geografischen und/oder kulturellen Bindungen widerspiegelt, iii) die Vorreiterrolle des Landes im Bereich des Schutzes der Privatsphäre und des Datenschutzes, die als Modell für andere Länder in der Region dienen könnte, und iv) die allgemeinen politischen Beziehungen zu dem Land, insbesondere in Bezug auf die Förderung gemeinsamer Werte und Ziele auf internationaler Ebene.

[126] Entschließung des Europäischen Parlaments vom 13. Dezember 2018 zu der Angemessenheit des von Japan gewährten Schutzes personenbezogener Daten (2018/2979(RSP)), Rn. 27; Beitrag des Ausschusses, S. 5/6.

[127] Siehe z. B. Entschließung des Europäischen Parlaments vom 12. Dezember 2017 zu dem Thema „Auf dem Weg zu einer Strategie für den digitalen Handel" (2017/2065(INI)), Rn. 8 und 9; Standpunkt und Feststellungen des Rates zur Anwendung der Datenschutz-Grundverordnung (DSGV), 14994/1/19 REV 1, 19.12.2019, Rn. 17; Beitrag des Ausschusses, S. 5.

Europas und stützt sich dabei auf den derzeitigen Trend einer weltweiten Aufwärtskonvergenz bei Datenschutzstandards. So wurden beispielsweise umfassende Rechtsvorschriften zum Datenschutz in Lateinamerika (Brasilien, Chile) verabschiedet oder befinden sich in einem fortgeschrittenen Stadium des Gesetzgebungsprozesses; außerdem finden vielversprechende Entwicklungen in Asien (z. B. Indien, Indonesien, Malaysia, Sri Lanka, Taiwan und Thailand), in Afrika (z. B. Äthiopien, Kenia) sowie in der östlichen und südlichen Nachbarschaft Europas (z. B. Georgien, Tunesien) statt. Soweit möglich, wird die Kommission auf umfassende Angemessenheitsbeschlüsse sowohl für den privaten als auch für den öffentlichen Sektor hinarbeiten.[128]

Darüber hinaus sieht die DSGVO die Möglichkeit für die Kommission vor, Angemessenheitsfeststellungen für internationale Organisationen anzunehmen. Sobald einige internationale Organisationen ihre Datenschutzregelungen aktualisieren, indem sie umfassende Vorschriften sowie Mechanismen für eine unabhängige Aufsicht und Rechtsbehelfe einführen, könnte diese Möglichkeit erstmals geprüft werden.

Der Aspekt der Angemessenheit spielt auch eine wichtige Rolle bei den künftigen Beziehungen zum Vereinigten Königreich nach dem Brexit, sofern die geltenden Voraussetzungen erfüllt sind. Angemessenheitsbeschlüsse sind ein Wegbereiter für den Handel, einschließlich des digitalen Handels, und eine wichtige Voraussetzung für eine enge und ambitionierte Zusammenarbeit im Bereich der Strafverfolgung und der Sicherheit.[129] Darüber hinaus ist angesichts der Bedeutung des Datenverkehrs mit dem Vereinigten Königreich und seiner Nähe zum EU-Markt ein hohes Maß an Konvergenz zwischen den Datenschutzvorschriften auf beiden Seiten des Kanals ein wichtiges Element zur Gewährleistung gleicher Wettbewerbsbedingungen. Im Einklang mit der Politischen Erklärung zur Festlegung des Rahmens für die künftigen Beziehungen zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien und Nordirland führt die Kommission derzeit eine Beurteilung der Angemessenheit nach der DSGVO sowie der Richtlinie zum Datenschutz bei der Strafverfolgung durch.[130] Angesichts des autonomen und einseitigen Charakters einer Angemessenheitsbeurteilung werden diese Gespräche separat von den Verhandlungen über ein Abkommen über die künftigen Beziehungen zwischen der EU und dem Vereinigten Königreich geführt.

[128] Wie dies auch vom Rat gefordert wurde, siehe Standpunkt und Feststellungen des Rates zur Anwendung der Datenschutz-Grundverordnung (DSGVO), 14994/1/19 REV 1, 19.12.2019, Rn. 17 und 40. Dies setzt jedoch voraus, dass die Bedingungen für eine Angemessenheitsfeststellung in Bezug auf Datenübermittlungen an Behörden, auch was eine unabhängige Aufsicht anbelangt, erfüllt sind.

[129] Siehe die Verhandlungsrichtlinien im Anhang des Beschlusses des Rates über die Ermächtigung zur Aufnahme von Verhandlungen mit dem Vereinigten Königreich Großbritannien und Nordirland über ein neues Partnerschaftsabkommen (ST 5870/20 ADD 1 REV 3), Rd. 13 und 118.

[130] Siehe überarbeiteter Text der Politischen Erklärung zur Festlegung des Rahmens für die künftigen Beziehungen zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien, wie er am 17. Oktober 2019 auf Ebene der Verhandlungsführer vereinbart wurde, Rn. 8-10 (abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.CI.2019.384.01.0178.01.DEU&toc=OJ:C:2019:384I:TOC).

Und nicht zuletzt begrüßt es die Kommission, dass andere Länder Mechanismen für die Datenübermittlung einführen, die mit einer Angemessenheitsfeststellung vergleichbar sind. Dabei werden die EU und Länder, für die die Kommission einen Angemessenheitsbeschluss erlassen hat, häufig als sichere Ziele für Datenübermittlungen anerkannt.[131] Indem einerseits immer mehr Länder von Angemessenheitsbeschlüssen der EU profitieren und dieser Mechanismus andererseits durch andere Länder anerkannt wird, besteht das Potenzial, ein Netzwerk von Ländern zu schaffen, in denen sich der Datenverkehr frei und sicher entfalten kann. Die Kommission erachtet dies als begrüßenswerte Entwicklung, die den Nutzen von Angemessenheitsbeschlüssen für Drittländer weiter erhöhen und zur globalen Konvergenz beitragen wird. Diese Art der Synergie kann außerdem einen nützlichen Beitrag zur Entwicklung von Rahmenbedingungen für den sicheren und freien Datenverkehr leisten, etwa im Kontext der Initiative für den „vertrauensvollen, freien Datenverkehr“ (siehe unten).

Geeignete Garantien

Die DSGVO sieht eine Reihe anderer Instrumente für Datenübermittlungen vor, die über die umfassende Lösung einer Angemessenheitsfeststellung hinausgehen. Die Flexibilität dieses Instrumentariums wird durch Artikel 46 der DSGVO belegt, in dem Datenübermittlungen auf der Grundlage „geeigneter Garantien“ geregelt sind, einschließlich durchsetzbarer Rechte der betroffenen Personen und wirksamer Rechtsbehelfe. Zur Gewährleistung geeigneter Garantien stehen verschiedene Instrumente zur Verfügung, um dem Übermittlungsbedarf sowohl von Wirtschaftsteilnehmern als auch von öffentlichen Stellen gerecht zu werden.

- Standardvertragsklauseln

Die erste Gruppe dieser Instrumente betrifft vertragliche Instrumente, bei denen es sich entweder um zwischen einem Datenexporteur aus der EU und einem Datenimporteur außerhalb der EU vereinbarte maßgeschneiderte Ad-hoc-Datenschutzklauseln handeln kann, die von der zuständigen Datenschutzbehörde genehmigt wurden (Artikel 46 Absatz 3 Buchstabe a der DSGVO), oder um von der Kommission vorab genehmigte Musterklauseln (Artikel 46 Absatz 2 Buchstaben c und d der DSGVO[132]). Die wichtigsten dieser Instrumente sind sogenannte Standardvertragsklauseln, d. h. Musterdatenschutzklauseln, die der Datenexporteur und der Datenimporteur auf freiwilliger Basis in ihre vertraglichen Vereinbarungen (z. B. einen Dienstleistungsvertrag, der die Übermittlung personenbezogener Daten erfordert) aufnehmen können und die die Anforderungen bezüglich geeigneter Garantien festlegen.

Standardvertragsklauseln stellen den bei Weitem am häufigsten genutzten Mechanismus für Datenübermittlungen dar.[133] Tausende von EU-Unternehmen

---

[131] Beispielsweise Argentinien, Israel, Kolumbien, Schweiz oder Uruguay.

[132] Standardvertragsklauseln für internationale Übermittlungen bedürfen immer der Zustimmung der Kommission, können aber entweder von der Kommission selbst oder von einer nationalen Datenschutzbehörde ausgearbeitet werden. Alle bestehenden Standardvertragsklauseln fallen in die erste Kategorie.

[133] Laut dem IAPP-EY Annual Privacy Governance Report 2019 „sind die gängigsten dieser (Übermittlungs-)Instrumente im Jahresvergleich mit überwältigender Mehrheit Verträge mit Standardvertragsklauseln: 88 % der Befragten in der diesjährigen Umfrage gaben

vertrauen auf Standardvertragsklauseln, um ihren Kunden, Lieferanten, Partnern und Beschäftigten eine breite Palette von Dienstleistungen zu bieten, einschließlich Dienstleistungen, die für das Funktionieren der Wirtschaft entscheidend sind. Die weitreichende Nutzung von Standardvertragsklauseln deutet darauf hin, dass sie für die Unternehmen bei ihren Bemühungen um Einhaltung der Vorschriften sehr hilfreich sind und insbesondere Unternehmen zugutekommen, die nicht über die Ressourcen verfügen, um mit jedem ihrer Geschäftspartner einzelne Verträge auszuhandeln. Durch ihre Standardisierung und Vorabgenehmigung stellen Standardvertragsklauseln den Unternehmen ein einfach umzusetzendes Instrument zur Verfügung, mit dem sie die Datenschutzanforderungen im Zusammenhang mit Datenübermittlungen erfüllen können.

Die bestehenden Pakete von Standardvertragsklauseln[134] wurden auf der Grundlage der Richtlinie von 1995 angenommen und genehmigt. Diese Standardvertragsklauseln bleiben so lange in Kraft, bis sie erforderlichenfalls mit einem Beschluss der Kommission geändert, ersetzt oder aufgehoben werden (Artikel 46 Absatz 5 der DSGVO). Mit der DSGVO werden die Möglichkeiten zur Verwendung von Standardvertragsklauseln sowohl innerhalb der EU als auch für internationale Datenübermittlungen erweitert. Die Kommission arbeitet derzeit mit den Interessenträgern zusammen, um diese Möglichkeiten zu nutzen und bestehende Klauseln zu aktualisieren.[135] Um sicherzustellen, dass die künftige Gestaltung von Standardvertragsklauseln ihren Zweck erfüllt, hat die Kommission im Rahmen der „Multi-Stakeholder-Gruppe zur DSGVO“ und eines im September 2019 durchgeführten speziellen Workshops Rückmeldungen zu den Erfahrungen der Interessenträger mit den Standardvertragsklauseln gesammelt; zudem hat die Kommission aber auch Rückmeldungen durch zahlreiche Kontakte mit Unternehmen, die Standardvertragsklauseln verwenden, sowie von Organisationen der Zivilgesellschaft eingeholt. Darüber hinaus aktualisiert der Ausschuss gegenwärtig eine Reihe von Leitlinien, die für die Überprüfung von Standardvertragsklauseln relevant sein könnten, beispielsweise in Bezug auf die Begriffe des Verantwortlichen und des Auftragsverarbeiters.

Standardvertragsklauseln als wichtigste Methode für extraterritoriale Datenübermittlungen an, gefolgt von der Einhaltung des EU-US-Datenschutzschilds (60 %). Von den Befragten, die Daten zwischen der EU und dem Vereinigten Königreich (52 %) übermitteln, gaben 91 % an, dass sie nach dem Brexit Standardvertragsklauseln zur Einhaltung der Vorgaben für Datenübermittlungen verwenden wollen.“

[134] Derzeit existieren drei Pakete von Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer, die von der Kommission angenommen wurden: zwei für Datenübermittlungen von einem Verantwortlichen im EWR an einen Verantwortlichen außerhalb des EWR und eine für Datenübermittlungen von einem Verantwortlichen im EWR an einen Auftragsverarbeiter außerhalb des EWR. Sie wurden 2016 im Anschluss an das Urteil des Gerichtshofs in der Rechtssache Schrems I (C-362/14) geändert, um alle Beschränkungen der zuständigen Aufsichtsbehörden bezüglich der Ausübung ihrer Befugnisse zur Überwachung von Datenübermittlungen zu beseitigen. Siehe https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[135] Siehe Beitrag des Ausschusses, S. 6/7. Ebenso hat der Rat die Kommission aufgefordert, „[die Standardvertragsklauseln] in naher Zukunft zu überprüfen und zu überarbeiten, um den Bedürfnissen der Verantwortlichen und der Auftragsverarbeiter Rechnung zu tragen“. Siehe Standpunkt und Feststellungen des Rates.

Derzeit überarbeiten die Kommissionsdienststellen die Standardvertragsklauseln auf Grundlage der eingegangenen Rückmeldungen. In diesem Zusammenhang wurden einige Bereiche ermittelt, in denen Verbesserungen erforderlich sind, insbesondere in Bezug auf folgende Aspekte:

1. Aktualisierung der Standardvertragsklauseln vor dem Hintergrund der durch die DSGVO eingeführten neuen Anforderungen, z. B. in Bezug auf die Beziehung zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Artikel 28 der DSGVO (insbesondere die Pflichten des Auftragsverarbeiters), die Verpflichtung zu Transparenz des Datenimporteurs (in Bezug auf die erforderlichen Informationen, die der betroffenen Person zur Verfügung zu stellen sind) usw.;
2. Behandlung einer Reihe von Übermittlungsszenarien, die von den derzeitigen Standardvertragsklauseln nicht abgedeckt werden, wie die Übermittlung von Daten von einem EU-Auftragsverarbeiter an einen nicht in der EU ansässigen Auftragsverarbeiter/Unterauftragsverarbeiter, aber auch Situationen, in denen der Verantwortliche seinen Sitz außerhalb der EU hat;[136]
3. bessere Widerspiegelung der Realität von Verarbeitungsvorgängen in der modernen digitalen Wirtschaft, die häufig mehrere Datenimporteure und -exporteure, lange und oft komplexe Verarbeitungsketten, sich entwickelnde Geschäftsbeziehungen usw. beinhalten. Um solchen Situationen Rechnung zu tragen, umfassen die in Betracht gezogenen Lösungen zum Beispiel die Möglichkeit, dass Standardvertragsklauseln von mehreren Parteien unterzeichnet werden oder dass während der Vertragslaufzeit neue Parteien beitreten.

Um auf diese Aspekte einzugehen, prüft die Kommission auch, wie die derzeitige „Architektur“ der Standardvertragsklauseln benutzerfreundlicher gestaltet werden kann, indem beispielsweise mehrere Pakete von Standardvertragsklauseln durch ein einziges umfassendes Dokument ersetzt werden. Die Herausforderung besteht darin, ein ausgewogenes Verhältnis zwischen dem Erfordernis der Klarheit und einem gewissen Grad an Standardisierung einerseits und der notwendigen Flexibilität andererseits herzustellen, damit die Klauseln von einer Reihe von Akteuren mit unterschiedlichen Anforderungen in unterschiedlichen Kontexten und für unterschiedliche Arten von Übermittlungen verwendet werden können.

Vor dem Hintergrund der laufenden Rechtsstreitigkeit vor dem Gerichtshof[137] sollte als weiterer wichtiger Aspekt erwogen werden, ob unter Umständen eine Klarstellung der Garantien für den Zugang ausländischer Behörden zu Daten notwendig ist, die auf der Grundlage von Standardvertragsklauseln übermittelt wurden, insbesondere im Hinblick auf den Zugang aus Gründen der nationalen Sicherheit. Dazu kann gehören, dass der Datenimporteur oder der Datenexporteur oder auch beide zur Ergreifung von

[136] In mehreren im Rahmen der öffentlichen Konsultation eingegangenen Beiträgen wurde zum letztgenannten Szenario Stellung genommen, wobei häufig Bedenken geäußert wurden, dass die Verpflichtung der in der EU ansässigen Auftragsverarbeiter, in ihren Beziehungen zu nicht in der EU ansässigen Verantwortlichen geeignete Garantien zu gewährleisten, einen Wettbewerbsnachteil gegenüber ausländischen Auftragsverarbeitern, die ähnliche Dienstleistungen anbieten, darstellen würde.

[137] Siehe Rechtssache Schrems II.

Maßnahmen verpflichtet werden und dass die Rolle der Datenschutzbehörden in diesem Zusammenhang zu klären ist. Obwohl bei der Überarbeitung der Standardvertragsklauseln gute Fortschritte erzielt wurden, muss das Urteil des Gerichtshofs abgewartet werden, um etwaige zusätzliche Anforderungen in den überarbeiteten Klauseln widerzuspiegeln, bevor dem Ausschuss der Entwurf eines Beschlusses über ein neues Paket von Standardvertragsklauseln zur Stellungnahme vorgelegt und anschließend zur Annahme im „Ausschussverfahren" vorgeschlagen werden kann.[138]

Parallel dazu steht die Kommission in Kontakt mit internationalen Partnern, die ähnliche Instrumente entwickeln.[139] Dieser Dialog, der den Austausch von Erfahrungen und bewährten Verfahren ermöglicht, könnte erheblich zur Weiterentwicklung der Konvergenz „an der Basis" beitragen und auf diese Weise die Einhaltung der Vorschriften für grenzüberschreitende Datenübermittlungen für Unternehmen, die in verschiedenen Regionen der Welt tätig sind, erleichtern.

- Verbindliche interne Datenschutzvorschriften

Ein weiteres wichtiges Instrument sind die sogenannten verbindlichen internen Datenschutzvorschriften. Hierbei handelt es sich um rechtlich bindende Strategien und Vereinbarungen, die für die Mitglieder einer Unternehmensgruppe, einschließlich ihrer Beschäftigten, gelten (Artikel 46 Absatz 2 Buchstabe b und Artikel 47 der DSGVO). Die Verwendung verbindlicher interner Datenschutzvorschriften ermöglicht den freien Verkehr personenbezogener Daten zwischen den verschiedenen Gruppenmitgliedern weltweit – unter Verzicht auf vertragliche Vereinbarungen zwischen jedem einzelnen Unternehmen der Gruppe – und gewährleistet gleichzeitig die Einhaltung desselben hohen Schutzniveaus für personenbezogene Daten innerhalb der gesamten Gruppe. Verbindliche interne Datenschutzvorschriften sind vor allem eine gute Lösung für große, komplexe Unternehmensgruppen und bei einer engen Zusammenarbeit von Unternehmen, die Daten über mehrere Rechtsräume hinweg austauschen. Anders als bei der Richtlinie von 1995 können verbindliche interne Datenschutzvorschriften nach der DSGVO von einer Gruppe von Unternehmen verwendet werden, die eine gemeinsame Wirtschaftstätigkeit ausüben, jedoch nicht derselben Unternehmensgruppe angehören.

Verfahrenstechnisch müssen verbindliche interne Datenschutzvorschriften von den zuständigen Datenschutzbehörden auf der Grundlage einer unverbindlichen Stellungnahme des Ausschusses genehmigt werden.[140] Als Orientierungshilfe für dieses Verfahren hat der Ausschuss die „Referenzgrundlage" verbindlicher interner

---

[138] Im Einklang mit Artikel 46 Absatz 2 Buchstabe c der DSGVO müssen Standardvertragsklauseln gemäß dem Prüfverfahren nach Artikel 5 der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13), erlassen werden. Dies umfasst insbesondere einen positiven Beschluss eines Ausschusses, der sich aus Vertretern der Mitgliedstaaten zusammensetzt.

[139] Dies umfasst zum Beispiel die gegenwärtige Arbeit der ASEAN-Mitgliedstaaten zur Entwicklung von „ASEAN-Mustervertragsklauseln". Siehe ASEAN, „Key Approaches for ASEAN Cross Border Data Flows Mechanism" (abrufbar unter: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

[140] Eine Übersicht über die bisherigen Stellungnahmen des Ausschusses ist unter https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de zu finden.

Datenschutzvorschriften (in der materielle Standards festgelegt sind) für Verantwortliche[141] und Auftragsverarbeiter[142] vor dem Hintergrund der DSGVO überprüft und aktualisiert diese Dokumente weiterhin auf Grundlage der praktischen Erfahrungen der Aufsichtsbehörden. Darüber hinaus hat der Ausschuss verschiedene Leitfäden angenommen, um Antragsteller zu unterstützen und das Antrags- und Genehmigungsverfahren für verbindliche interne Datenschutzvorschriften zu optimieren.[143] Dem Ausschuss zufolge stehen derzeit mehr als 40 verbindliche interne Datenschutzvorschriften zur Genehmigung an, wobei eine Genehmigung der Hälfte davon bis Ende 2020 erwartet wird.[144] Wichtig ist, dass die Datenschutzbehörden weiterhin an der Optimierung des Genehmigungsverfahrens arbeiten, da von Interessenträgern häufig der Hinweis kommt, dass die lange Dauer solcher Verfahren in der Praxis ein Hindernis für die breitere Verwendung verbindlicher interner Datenschutzvorschriften darstellt.

Was schließlich speziell die verbindlichen internen Datenschutzvorschriften betrifft, die von der britischen Datenschutzbehörde – dem Information Commissioner's Office – genehmigt wurden, können Unternehmen diese nach Ablauf des Übergangszeitraums im Rahmen des Austrittsabkommens zwischen der EU und dem Vereinigten Königreich weiterhin als gültigen Datenübermittlungsmechanismus gemäß der DSGVO nutzen, allerdings nur, wenn diese Vorschriften dahingehend geändert werden, dass jegliche Verbindung zur Rechtsordnung des Vereinigten Königreichs durch geeignete Verweise auf Unternehmen und zuständige Behörden innerhalb der EU ersetzt wird. Neue verbindliche interne Datenschutzvorschriften sollten von einer der Aufsichtsbehörden in der EU genehmigt werden.

- Zertifizierungsverfahren und Verhaltensregeln

Neben der Modernisierung und Erweiterung der Anwendung der bereits bestehenden Übermittlungsinstrumente wurden mit der DSGVO auch neue Instrumente eingeführt, wodurch die Möglichkeiten für internationale Übermittlungen ausgedehnt wurden. Dies schließt unter bestimmten Bedingungen die Verwendung genehmigter Verhaltensregeln und Zertifizierungsverfahren (wie Datenschutzsiegel oder -prüfzeichen) ein, um geeignete Garantien zu gewährleisten. Dabei handelt es sich um Bottom-up-Instrumente, die maßgeschneiderte Lösungen – als allgemeiner Rechenschaftsmechanismus (siehe Artikel 40 bis 42 der DSGVO) und insbesondere für internationale Datenübermittlungen – ermöglichen, welche beispielsweise die spezifischen Merkmale und Erfordernisse eines bestimmten Sektors, einer bestimmten Branche oder eines bestimmten Datenverkehrs widerspiegeln. Durch die Austarierung von Pflichten und Risiken können Verhaltensregeln für kleine und mittlere Unternehmen außerdem eine hilfreiche und kostenwirksame Methode zur Erfüllung ihrer Pflichten nach der DSGVO sein.

---

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109
[142] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110
[143] Diese Dokumente wurden (von der früheren Artikel-29-Datenschutzgruppe) nach Inkrafttreten der DSGVO, aber vor Ablauf des Übergangszeitraums angenommen. Siehe WP263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056), WP264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf) und WP265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).
[144] Beitrag des Ausschusses, S. 7.

Bezüglich Zertifizierungsverfahren hat der Ausschuss zwar Leitlinien angenommen, um die Nutzung dieser Verfahren innerhalb der EU zu fördern, allerdings ist die Arbeit des Ausschusses zur Entwicklung von Kriterien für die Genehmigung von Zertifizierungsverfahren als Instrument für internationale Datenübertragungen noch nicht abgeschlossen. Das Gleiche gilt für Verhaltensregeln; hier erarbeitet der Ausschuss derzeit Leitlinien für ihre Verwendung als Übermittlungsinstrument.

Da es wichtig ist, den Akteuren eine breite Palette von bedarfsgerechten Übermittlungsinstrumenten an die Hand zu geben, und weil speziell Zertifizierungsverfahren Datenübermittlungen erleichtern und gleichzeitig ein hohes Datenschutzniveau gewährleisten können, fordert die Kommission den Ausschuss nachdrücklich auf, seine diesbezüglichen Leitlinien so bald wie möglich fertigzustellen. Dies betrifft sowohl materielle Aspekte (Kriterien) als auch verfahrenstechnische Aspekte (Genehmigung, Überwachung usw.). Die Interessenträger haben großes Interesse an diesen Übermittlungsinstrumenten bekundet und sollten in der Lage sein, das Instrumentarium der DSGVO in vollem Umfang zu nutzen. Außerdem würden die Leitlinien des Ausschusses dazu beitragen, das EU-Datenschutzmodell weltweit zu befördern und die Angleichung voranzutreiben, weil in anderen Datenschutzsystemen ähnliche Instrumente genutzt werden.

Aus den bestehenden Normungsbemühungen im Bereich des Datenschutzes können sowohl auf europäischer als auch auf internationaler Ebene wertvolle Lehren gezogen werden. Ein interessantes Beispiel ist die kürzlich veröffentlichte internationale Norm ISO 27701[145], mit der Unternehmen dabei unterstützt werden sollen, Datenschutzanforderungen zu erfüllen und Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten mithilfe von „Datenschutz-Managementsystemen“ (Privacy Information Management Systems) zu bewältigen. Obwohl die Zertifizierung nach dieser Norm an sich die Anforderungen der Artikel 42 und 43 der DSGVO nicht erfüllt, kann die Anwendung von Datenschutz-Managementsystemen zur Rechenschaftspflicht beitragen, auch im Zusammenhang mit internationalen Datenübermittlungen.

- Internationale Übereinkünfte und Verwaltungsvereinbarungen

Die DSGVO ermöglicht auch geeignete Garantien für Datenübermittlungen zwischen Behörden oder öffentlichen Stellen auf der Grundlage von internationalen Übereinkünften (Artikel 46 Absatz 2 Buchstabe a) oder von Verwaltungsvereinbarungen (Artikel 46 Absatz 3 Buchstabe b). Während beide Instrumente in Bezug auf Garantien, einschließlich durchsetzbarer Rechte der betroffenen Personen und wirksamer Rechtsbehelfe, dasselbe Ergebnis gewährleisten müssen, unterscheiden sie sich hinsichtlich ihrer Rechtsnatur und des Verfahrens ihrer Annahme.

Im Gegensatz zu internationalen Übereinkünften, die völkerrechtlich bindende Verpflichtungen begründen, sind Verwaltungsvereinbarungen (z. B. in Form einer gemeinsamen Absichtserklärung) in der Regel nicht verbindlich und erfordern daher eine vorherige Genehmigung durch die zuständige Datenschutzbehörde (siehe auch

[145] Die Liste der spezifischen Anforderungen dieser ISO-Norm ist abrufbar unter: https://www.iso.org/standard/71670.html.

Erwägungsgrund 108 der DSGVO). Ein frühes Beispiel ist die Verwaltungsvereinbarung über die Übermittlung personenbezogener Daten zwischen Finanzaufsichtsbehörden im EWR und Finanzaufsichtsbehörden außerhalb des EWR, die unter dem Dach der Internationalen Organisation der Wertpapieraufsichtsbehörden (IOSCO) zusammenarbeiten, zu der der Ausschuss Anfang 2019 eine Stellungnahme[146] abgegeben hat. Seitdem hat der Ausschuss seine Auslegung der „Mindestgarantien" weiterentwickelt, die internationale (Kooperations-)Abkommen und Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen (einschließlich internationaler Organisationen) gewährleisten müssen, um die Anforderungen des Artikels 46 der DSGVO zu erfüllen. Am 18. Januar 2020 nahm der Ausschuss einen Leitlinienentwurf[147] an, mit dem er dem Ersuchen der Mitgliedstaaten um weitere Klarstellungen und Orientierungshilfen dahingehend nachkam, welche Garantien für Datenübermittlungen zwischen Behörden als geeignet betrachtet werden können[148]. Der Ausschuss empfiehlt den Behörden nachdrücklich, diese Leitlinien als Bezugspunkt für ihre Verhandlungen mit Dritten zu verwenden.[149]

Die Leitlinien bieten Flexibilität bei der Gestaltung solcher Instrumente, auch in Bezug auf wichtige Aspekte wie Aufsicht[150] und Rechtsbehelfe[151]. Dadurch sollte es

---

[146] EDSA, Stellungnahme 4/2019 zu dem Entwurf einer Verwaltungsvereinbarung über die Übermittlung personenbezogener Daten zwischen Finanzaufsichtsbehörden im Europäischen Wirtschaftsraum (EWR) und Finanzaufsichtsbehörden außerhalb des EWR, 12.2.2019.

[147] EDSA, Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies (Leitlinien 2/2020 zu Artikel 46 Absatz 2 Buchstabe a und Artikel 46 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten zwischen Behörden und öffentlichen Stellen im EWR und Behörden und öffentlichen Stellen außerhalb des EWR) (Entwurf abrufbar unter: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en). Dem Ausschuss zufolge „stützt die zuständige Aufsichtsbehörde ihre Prüfung auf die in diesen Leitlinien enthaltenen allgemeinen Empfehlungen, kann aber je nach Einzelfall mehr Garantien verlangen". Der Ausschuss legte diesen Leitlinienentwurf zur öffentlichen Konsultation vor, die am 18. Mai 2020 endete.

[148] Standpunkt und Feststellungen des Rates, Rn. 20.

[149] Gleichzeitig stellt der Ausschuss klar, dass es den Behörden weiterhin „freisteht, sich auf andere einschlägige Instrumente zu stützen, die geeignete Garantien gemäß Artikel 46 der DSGVO bieten". In Bezug auf die Wahl des Instruments betont der Ausschuss, dass „im Hinblick auf den Zweck der Verarbeitung und der Art der betreffenden Daten sorgfältig geprüft werden sollte, ob rechtlich unverbindliche Verwaltungsvereinbarungen zu verwenden sind, um Garantien im öffentlichen Sektor zu bieten. Sind Datenschutzrechte und Rechtsbehelfe für EWR-Bürger im innerstaatlichen Recht des Drittlandes nicht vorgesehen, sollte dem Abschluss eines rechtsverbindlichen Übereinkommens der Vorzug gegeben werden. Unabhängig von der Art des angenommenen Instruments müssen die bestehenden Maßnahmen wirksam sein, um eine angemessene Umsetzung, Durchsetzung und Überwachung zu gewährleisten" (Rn. 67).

[150] Dies kann beispielsweise die Kombination interner Kontrollen (mit der Verpflichtung, die andere Partei über jeden Verstoß zu informieren) mit einer unabhängigen Aufsicht durch externe oder zumindest funktionell autonome Mechanismen umfassen sowie die Möglichkeit für die übermittelnde öffentliche Stelle, die Datenübermittlung auszusetzen oder zu beenden.

[151] Dies kann beispielsweise quasi-gerichtliche, verbindliche Mechanismen (z. B. Schiedsverfahren) oder alternative Streitbeilegungsverfahren umfassen, kombiniert mit der Möglichkeit für die übermittelnde Behörde, die Übermittlung personenbezogener Daten auszusetzen oder zu beenden, wenn den Parteien keine gütliche Beilegung der Streitigkeit gelingt, zuzüglich einer Verpflichtung der empfangenden öffentlichen Stelle, die personenbezogenen Daten zurückzugeben oder zu löschen. Wenn in verbindlichen und durchsetzbaren Instrumenten alternative Rechtsbehelfsmechanismen gewählt werden, weil es keine Möglichkeit gibt, einen wirksamen

den Behörden möglich sein, die Schwierigkeiten, beispielsweise bei der Gewährleistung durchsetzbarer Rechte der betroffenen Personen mittels unverbindlicher Vereinbarungen, zu überwinden. Ein wichtiger Aspekt bei solchen Vereinbarungen ist ihre kontinuierliche Überwachung durch die zuständige Datenschutzbehörde – unterstützt durch Informations- und Aufzeichnungsanforderungen – und die Aussetzung des Datenverkehrs, wenn geeignete Garantien in der Praxis nicht mehr gewährleistet werden können.

Ausnahmen

Schließlich wird in der DSGVO die Verwendung sogenannter „Ausnahmen" klargestellt. Hierbei handelt es sich um spezifische Gründe für Datenübermittlungen (z. B. ausdrückliche Einwilligung[152], Erfüllung eines Vertrags oder wichtige Gründe des öffentlichen Interesses), die rechtlich anerkannt sind und auf die sich Unternehmen unter bestimmten Bedingungen stützen können, wenn keine anderen Instrumente für die Datenübermittlung zur Verfügung stehen.

Um die Anwendung solcher rechtlichen Gründe klarzustellen, hat der Ausschuss spezifische Leitlinien[153] herausgegeben und hat Artikel 49 in einer Reihe von Fällen im Zusammenhang mit spezifischen Übermittlungsszenarien[154] ausgelegt. Aufgrund des besonderen Charakters von Ausnahmen ist der Ausschuss der Auffassung, dass diese von Fall zu Fall restriktiv ausgelegt werden müssen. Trotz der strengen Auslegung decken die genannten Gründe ein breites Spektrum von Übermittlungsszenarien ab. Dazu zählen insbesondere Datenübermittlungen durch Behörden sowie private Einrichtungen, die aus „wichtigen Gründen des öffentlichen Interesses" erforderlich sind, z. B. zwischen Wettbewerbs-, Finanz-, Steuer- oder Zollbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten (beispielsweise im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Beseitigung des Dopings im Sport).[155] Ein weiterer Bereich ist die grenzüberschreitende Zusammenarbeit zum Zweck der Strafverfolgung, insbesondere im Bereich der schweren Kriminalität.[156]

---

gerichtlichen Rechtsbehelf zu gewährleisten, empfiehlt der Ausschuss, vor der endgültigen Einrichtung solcher Instrumente die zuständige Aufsichtsbehörde um Rat zu ersuchen.

[152] Es handelt sich hierbei um eine Änderung gegenüber der Richtlinie 95/46/EG, nach der lediglich eine Einwilligung „ohne jeden Zweifel" verlangt wurde. Darüber hinaus gelten die allgemeinen Anforderungen an die Einwilligung gemäß Artikel 4 Absatz 11 der DSGVO.

[153] EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, 25.5.2018 (abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf).

[154] Dies umfasst beispielsweise die internationale Übermittlung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch. Siehe EDSA, Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch, 21.4.2020 (abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_de.pdf).

[155] Siehe Erwägungsgrund 112 der DSGVO.

[156] Siehe „Brief of the European Commission on Behalf of the European Union as *Amicus Curiae* in Support of Neither Party" in der Rechtssache US gegen Microsoft, S. 15: „Im Allgemeinen erkennt sowohl das Unionsrecht als auch das Recht der Mitgliedstaaten die Bedeutung der Bekämpfung der schweren Kriminalität – und somit der Strafverfolgung und der internationalen Zusammenarbeit in

Der Ausschuss hat klargestellt, dass das einschlägige öffentliche Interesse zwar im Unionsrecht oder im Recht der Mitgliedstaaten anerkannt werden muss, jedoch kann das „Vorliegen eines internationalen Abkommens oder einer internationalen Übereinkunft, welche(s) ein bestimmtes Ziel anerkennt und zur Förderung dieses Ziels eine internationale Zusammenarbeit vorsieht, … ein Hinweis auf das Vorliegen eines öffentlichen Interesses nach Artikel 49 Absatz 1 Buchstabe d sein, wenn die EU oder die Mitgliedstaaten zu den Unterzeichnern dieses Abkommens bzw. dieser Übereinkunft gehören“[157].

Urteile von Gerichten und Entscheidungen von Behörden eines Drittlands: keine Grundlage für Datenübermittlungen

Neben der positiven Darlegung der Gründe für Datenübermittlungen wird in Kapitel V Artikel 48 der DSGVO klargestellt, dass Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden außerhalb der EU *für sich genommen* keine solchen Gründe darstellen, wenn sie nicht durch eine internationale Übereinkunft (z. B. ein Rechtshilfeabkommen) anerkannt oder vollstreckbar werden. Jegliche Offenlegung gegenüber dem Gericht oder der Verwaltungsbehörde eines Drittlands, die von der ersuchten Einrichtung in der EU in Reaktion auf ein solches Urteil oder eine solche Entscheidung verlangt wird, stellt eine internationale Datenübermittlung dar und muss sich auf eines der genannten Übermittlungsinstrumente stützen.[158]

Die DSGVO stellt kein „Verbotsgesetz“ dar und gestattet unter bestimmten Bedingungen eine Datenübermittlung als Reaktion auf ein entsprechendes Ersuchen eines Drittlands zum Zweck der Strafverfolgung. Der wichtige Punkt dabei ist, dass durch Unionsrecht bestimmt werden sollte, ob dieser Fall gegeben ist und auf der Grundlage welcher Garantien eine solche Datenübermittlung erfolgen kann.

Die Kommission erläuterte die Funktionsweise von Artikel 48 der DSGVO,

---

diesem Bereich – als Ziel von allgemeinem Interesse an. … Artikel 83 AEUV nennt mehrere Bereiche von besonders schwerwiegender Kriminalität, die eine grenzüberschreitende Dimension haben, etwa der illegale Drogenhandel.“ (Abrufbar unter: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

157 EDSA, Leitlinien zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 (siehe Fußnote 153 oben), S. 12/13. Der Ausschuss stellte ferner klar, dass Datenübermittlungen auf der Grundlage der Ausnahmeregelung im öffentlichen Interesse zwar nicht in „großem Umfang“ oder „systematisch“ erfolgen dürfen, sondern „spezifischen Situationen vorzubehalten sind, und … dass das strenge Kriterium der Erforderlichkeit bei den Übermittlungen eingehalten wird“, diese Ausnahme jedoch nicht auf „gelegentliche“ Datenübermittlungen beschränkt sein muss.

158 Dies wird durch den Wortlaut von Artikel 48 der DSGVO („unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel“) und dem entsprechenden Erwägungsgrund 115 („Datenübermittlungen sollten daher nur zulässig sein, wenn die Bedingungen dieser Verordnung für Datenübermittlungen an Drittländer eingehalten werden. Dies kann unter anderem der Fall sein, wenn die Offenlegung aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt ist.“) verdeutlicht. Diese Auslegung wird auch vom Ausschuss anerkannt; siehe Leitlinien zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 (Fußnote 153 oben), S. 6. Wie bei allen Verarbeitungsvorgängen müssen auch die anderen in der Verordnung vorgesehenen Garantien eingehalten werden (z. B. dass Daten für einen bestimmten Zweck übermittelt werden, dass sie maßgeblich sind, dass sie auf das für die Zwecke ihrer Anforderung notwendige Maß beschränkt sind usw.).

einschließlich der möglichen Berufung auf die Ausnahme aus Gründen des öffentlichen Interesses, im Zusammenhang mit einer Herausgabeanordnung („Warrant“) einer ausländischen Strafverfolgungsbehörde in der Microsoft-Rechtssache vor dem Obersten Gerichtshof der Vereinigten Staaten.[159] In ihrer Stellungnahme betonte die Kommission das Interesse der EU, sicherzustellen, dass die Zusammenarbeit bei der Strafverfolgung „in einem rechtlichen Rahmen erfolgt, der Rechtskonflikte vermeidet und auf … der Achtung der grundlegenden Interessen der jeweils anderen Partei bezüglich des Datenschutzes sowie bezüglich der Strafverfolgung beruht“.[160] Insbesondere werden „aus Sicht des Völkerrechts das Territorialitäts- und das Comity-Prinzip nach dem Völkerrecht angewandt, wenn eine Behörde von einem in ihrem eigenen Hoheitsgebiet niedergelassenen Unternehmen verlangt, elektronische Daten zu erstellen, die auf einem Server in einem ausländischen Hoheitsgebiet gespeichert sind“.[161]

Dies spiegelt sich auch in dem Vorschlag der Kommission für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen[162] wider, der eine spezifische „Comity-Klausel“ enthält, die es ermöglicht, Einwände gegen eine Herausgabeanordnung zu erheben, wenn deren Einhaltung gegen das Recht eines Drittlandes verstoßen würde, das die Offenlegung untersagt, insbesondere weil dies zum Schutz der Grundrechte der betroffenen Personen erforderlich ist[163].

---

[159] Stellungnahme in der Rechtssache Microsoft (siehe Fußnote 156 oben). Wie die Kommission erläuterte, werden daher Rechtshilfeabkommen in der DSGVO zur „bevorzugten Option“ für Datenübermittlungen erklärt, da solche Abkommen „die Erhebung von Beweismitteln durch Einwilligung vorsehen und auf einem sorgfältig ausgehandelten Gleichgewicht zwischen den Interessen der verschiedenen Staaten beruhen, mit dem Ziel, Zuständigkeitskonflikte, die andernfalls auftreten können, zu verringern“. Siehe auch EDSA, Leitlinien zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 (Fußnote 153 oben), S. 6: „Besteht eine internationale Übereinkunft wie etwa ein Rechtshilfeabkommen, sollten die Unternehmen in der EU direkte Anfragen generell ablehnen und die ersuchende Behörde des Drittstaates auf das bestehende Rechtshilfeabkommen oder die entsprechende Übereinkunft verweisen.“

[160] Stellungnahme in der Rechtssache Microsoft (siehe Fußnote 156 oben), S. 4.

[161] Stellungnahme in der Rechtssache Microsoft (siehe Fußnote 156 oben), S. 6.

[162] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, 17.4.2018 (COM(2018) 225 final). Der Rat hat seine allgemeine Ausrichtung zu der vorgeschlagenen Verordnung am 7.12.2018 festgelegt (abrufbar unter: https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-eevidence-council-agrees-its-position/#). Siehe auch Stellungnahme 7/2019 des EDSB zu den Vorschlägen über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (abrufbar unter: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

[163] In der Begründung, S. 24, wird klargestellt, dass neben der Sicherstellung eines entgegenkommenden Verhaltens im Hinblick auf die souveränen Interessen von Drittländern, dem Schutz der betroffenen Person und der Vermeidung von Rechtskonflikten für Diensteanbieter ein wichtiger Grund für die Comity-Klausel die Gegenseitigkeit ist, d. h. die Einhaltung der EU-Vorschriften, einschließlich des Schutzes personenbezogener Daten, zu gewährleisten (Artikel 48 der DSGVO). Siehe auch Stellungnahme der Artikel-29-Datenschutzgruppe vom 29. November 2017 über Datenschutzaspekte beim grenzüberschreitenden Zugang zu elektronischen Beweismitteln (WP29-Stellungnahme) (abrufbar unter: file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20(1).pdf), S. 9.

Die Sicherstellung eines entgegenkommenden Verhaltens ist wichtig, da die Strafverfolgung – wie die Kriminalität und insbesondere die Cyberkriminalität – zunehmend grenzüberschreitend ist und daher häufig Zuständigkeitsfragen aufwirft und zu potenziellen Rechtskonflikten führt.[164] Es überrascht nicht, dass diese Probleme am besten durch internationale Übereinkommen gelöst werden können, die die notwendigen Beschränkungen und Garantien für den grenzüberschreitenden Zugang zu personenbezogenen Daten vorsehen, unter anderem durch die Gewährleistung eines hohen Datenschutzniveaus seitens der ersuchenden Behörde.

Die Kommission, die im Namen der Europäischen Union handelt, führt derzeit multilaterale Verhandlungen über ein Zweites Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität (Budapester Übereinkommen), das darauf abzielt, die bestehenden Vorschriften für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln in strafrechtlichen Ermittlungen zu verbessern und gleichzeitig geeignete Datenschutzgarantien als Teil des Protokolls zu gewährleisten.[165] Ebenso wurden bilaterale Verhandlungen über ein Abkommen zwischen der EU und den Vereinigten Staaten über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen aufgenommen.[166] Die Kommission baut während dieser Verhandlungen auf die Unterstützung durch das Europäische Parlament und den Rat sowie auf die Leitlinien des Ausschusses.

Allgemeiner muss sichergestellt werden, dass auf dem europäischen Markt tätige Unternehmen, die mittels eines berechtigten Ersuchens zur Weitergabe von Daten zu Strafverfolgungszwecken aufgefordert werden, dies ohne Rechtskollisionen und unter uneingeschränkter Achtung der Grundrechte der EU tun können. Um solche Datenübermittlungen zu verbessern, ist die Kommission entschlossen, mit ihren internationalen Partnern geeignete Rechtsrahmen auszuarbeiten, um Rechtskollisionen zu vermeiden und – insbesondere durch das Vorsehen der erforderlichen Datenschutzgarantien – wirksame Formen der Zusammenarbeit zu

---

[164] Siehe WP29-Stellungnahme (Fußnote 163 oben), S. 6.

[165] Empfehlung für einen Beschluss des Rates zur Genehmigung der Teilnahme an Verhandlungen über ein Zweites Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität (SEV Nr. 185), 5.2.2019 (COM(2019) 71 final). Siehe auch EDSB, Stellungnahme 3/2019 zu der Teilnahme an den Verhandlungen mit Blick auf ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität, 2.4.2019 (abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_de.pdf); EDSA, EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) (Beitrag des EDSB zur Konsultation zum Entwurf eines Zweiten Zusatzprotokolls zum Übereinkommen des Europarats über Computerkriminalität (Budapester Übereinkommen)), 13.11.2019 (abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

[166] Siehe Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen, 5.2.2019, (COM(2019) 70 final). Siehe auch EDSB, Stellungnahme 2/2019 zu dem Mandat für die Verhandlung eines Abkommens zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln (abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_eu_us_agreement_e-evidence_en_de.pdf).

unterstützen und auf diese Weise zu einer wirksameren Kriminalitätsbekämpfung beizutragen.

7.3 Internationale Zusammenarbeit im Bereich des Datenschutzes

Die Förderung der Konvergenz zwischen verschiedenen Datenschutzsystemen heißt auch, durch den Austausch von Wissen, Erfahrungen und bewährten Verfahren voneinander zu lernen. Ein solcher Austausch ist von entscheidender Bedeutung, um neue Herausforderungen, die zunehmend globaler Natur und von globaler Tragweite sind, zu bewältigen. Aus diesem Grund hat die Kommission ihren Dialog über Datenschutz und Datenverkehr mit einem breiten Spektrum von Akteuren sowie in verschiedenen Foren auf bilateraler, regionaler und multilateraler Ebene intensiviert.

Die bilaterale Dimension

Nach der Annahme der DSGVO ist das Interesse hinsichtlich der Erfahrungen der EU mit der Gestaltung, Aushandlung und Umsetzung moderner Datenschutzvorschriften gestiegen. Der Dialog mit Ländern, die ähnliche Prozesse durchlaufen, hat verschiedene Formen angenommen.

Die Kommissionsdienststellen haben zu einer Reihe öffentlicher Konsultationen Stellungnahmen abgegeben, die von ausländischen Regierungen, wie den USA[167], Indien[168], Malaysia und Äthiopien, zu Rechtsvorschriften im Bereich des Datenschutzes durchgeführt wurden. In einigen Drittländern hatten die Kommissionsdienststellen das Privileg, sich in den zuständigen parlamentarischen Gremien zu äußern, beispielsweise in Brasilien[169], Chile[170], Ecuador und Tunesien[171].

---

[167] Siehe Stellungnahme der GD Justiz und Verbraucher vom 9. November 2018 zu einer Aufforderung zur öffentlichen Stellungnahme in Bezug auf ein vorgeschlagenes Konzept für den Schutz der Privatsphäre von Verbrauchern [Unterlage Nr. 180821780-8780-01] der US-amerikanischen Telekommunikationsbehörde (National Telecommunications and Information Administration) (abrufbar unter: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf).

[168] Siehe Stellungnahme der GD Justiz und Verbraucher vom 19. November 2018 zum Entwurf des indischen Gesetzes über den Schutz personenbezogener Daten von 2018 an das Ministerium für Elektronik und Informationstechnologie (abrufbar unter: https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] Siehe Plenarsitzung des brasilianischen Senats vom 17. April 2018 (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), Sitzung des Gemischten Ausschusses zu MP 869/2018 des brasilianischen Kongresses vom 10. April 2019 (https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392) und Sitzung Sonderausschusses der brasilianischen Abgeordnetenkammer vom 26. November 2019 (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

[170] Siehe Sitzungen vom 29. Mai 2018 (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1) und vom 24. April 2019 (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2) sowie Sitzung des Ausschusses für Verfassungs-, Gesetzgebungs- und Justizangelegenheiten des chilenischen Senats.

Darüber hinaus fanden im Rahmen der fortlaufenden Reformen von Datenschutzgesetzen spezielle Treffen mit Regierungsvertretern oder parlamentarischen Delegationen aus vielen Regionen der Welt statt (z. B. Georgien, Kenia, Taiwan, Thailand, Marokko). Dazu gehörte auch die Organisation von Seminaren und Studienbesuchen, beispielsweise mit Vertretern der indonesischen Regierung und einer Delegation von Mitarbeitern des US-Kongresses. Dadurch ergab sich die Gelegenheit, wichtige Begriffe der DSGVO zu klären, das gegenseitige Verständnis von Datenschutzfragen zu verbessern und die Vorteile der Konvergenz zur Gewährleistung eines hohen Schutzniveaus für die Rechte des Einzelnen sowie zur Sicherstellung von Handel und Zusammenarbeit zu verdeutlichen. In einigen Fällen konnte auch vor gewissen falschen Vorstellungen von Datenschutz gewarnt werden, die zur Einführung protektionistischer Maßnahmen wie zwingende Anforderungen zur Datenlokalisierung führen können.

Seit der Annahme der DSGVO hat die Kommission zudem mit mehreren internationalen Organisationen zusammengearbeitet, unter anderem mit Blick auf die Bedeutung des Datenaustauschs mit diesen Organisationen in einer Reihe von Politikbereichen. Im Einzelnen wurde ein spezifischer Dialog mit den Vereinten Nationen zur Erleichterung von Gesprächen mit allen beteiligten Interessenträgern aufgenommen, um eine reibungslose Datenübermittlung zu gewährleisten und eine weitere Annäherung zwischen den jeweiligen Datenschutzregelungen zu erzielen. Im Rahmen dieses Dialogs wird die Kommission eng mit dem Ausschuss zusammenarbeiten, um weiter zu klären, wie öffentliche und private Akteure aus der EU beim Datenaustausch mit internationalen Organisationen wie den Vereinten Nationen ihren Pflichten gemäß der DSGVO nachkommen können.

Die Kommission ist bereit, die bei ihrem Reformprozess gewonnenen Erkenntnisse weiterhin mit interessierten Ländern und internationalen Organisationen auszutauschen, so wie sie bei der Ausarbeitung ihres Vorschlags für neue EU-Datenschutzvorschriften Erkenntnisse aus anderen Systemen gezogen hat. Ein solcher Dialog ist für die EU und ihre Partner von beiderseitigem Nutzen, da er die Möglichkeit bietet, ein besseres Verständnis der sich rasch entwickelnden Datenschutzlandschaft zu erlangen und Auffassungen über neue rechtliche und technologische Lösungen auszutauschen.

Ganz in diesem Sinne richtet die Kommission eine „Datenschutzakademie“ ein, um den Austausch zwischen europäischen Regulierungsbehörden und Regulierungsbehörden von Drittländern zu fördern und auf diese Weise die Zusammenarbeit „an der Basis“ zu verbessern.

Dies erfordert zudem die Entwicklung geeigneter Rechtsinstrumente für engere Formen der Zusammenarbeit und gegenseitigen Amtshilfe, unter anderem indem der erforderliche Informationsaustausch im Rahmen von Ermittlungen ermöglicht wird. Die Kommission wird daher von den in Artikel 50 der DSGVO in diesem Bereich eingeräumten Befugnissen Gebrauch machen und insbesondere um die Ermächtigung ersuchen, Verhandlungen über den Abschluss von Abkommen über die

[171] Siehe Sitzung des Ausschusses zu Rechten, Freiheiten und Außenbeziehungen der tunesischen Volksversammlung vom 2. November 2018 (https://www.facebook.com/1515094915436499/posts/2264094487203201/).

Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften mit einschlägigen Drittländern aufzunehmen. In diesem Zusammenhang wird sie auch die Standpunkte des Ausschusses dahingehend berücksichtigen, welche Länder angesichts des Umfangs von Datenübermittlungen, der Rolle und der Befugnisse der Stelle zur Durchsetzung von Datenschutzvorschriften in dem Drittland und der Notwendigkeit einer Zusammenarbeit bei der Rechtsdurchsetzung in Fällen von gemeinsamem Interesse vorrangig behandelt werden sollten.

Die multilaterale Dimension

Über den bilateralen Austausch hinaus beteiligt sich die Kommission auch aktiv an einer Reihe multilateraler Foren, um gemeinsame Werte zu fördern und Konvergenz auf regionaler und globaler Ebene aufzubauen.

Die zunehmend universelle Mitgliedschaft im Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten („Übereinkommen 108“) des Europarats, dem einzigen rechtsverbindlichen multilateralen Instrument im Bereich des Schutzes personenbezogener Daten, ist ein deutliches Zeichen für diesen Trend hin zu einer (Aufwärts-)Konvergenz.[172] Das Übereinkommen, das auch Nichtmitgliedern des Europarats offensteht, wurde bereits von 55 Ländern ratifiziert, darunter von mehreren afrikanischen und lateinamerikanischen Staaten.[173] Die Kommission hat erheblich zum erfolgreichen Abschluss der Verhandlungen über die Modernisierung des Übereinkommens[174] beigetragen und dafür gesorgt, dass es die gleichen Grundsätze widerspiegelt wie die in den Datenschutzvorschriften der EU verankerten. Die meisten EU-Mitgliedstaaten haben inzwischen das Änderungsprotokoll unterzeichnet, obwohl die Unterzeichnung Dänemarks, Maltas und Rumäniens noch aussteht. Bislang haben nur vier Mitgliedstaaten (Bulgarien, Kroatien, Litauen und Polen) das Änderungsprotokoll ratifiziert. Die Kommission appelliert an die drei verbleibenden Mitgliedstaaten, das modernisierte Übereinkommen zu unterzeichnen, und fordert alle Mitgliedstaaten nachdrücklich dazu auf, die Ratifizierung zügig voranzutreiben, damit das Übereinkommen in naher Zukunft in Kraft treten kann.[175] Darüber hinaus fördert die Kommission den Beitritt von Drittländern weiterhin proaktiv.

---

[172] Zu betonen ist, dass das modernisierte Übereinkommen nicht nur ein Vertrag ist, der strenge Datenschutzgarantien vorsieht, sondern dass mit ihm auch ein Netzwerk von Aufsichtsbehörden geschaffen wird, denen Instrumente für die Zusammenarbeit bei der Rechtsdurchsetzung zur Verfügung stehen; darüber hinaus bietet das Übereinkommen mit seinem Ausschuss ein Forum für Diskussionen, den Austausch bewährter Verfahren und die Entwicklung internationaler Standards.

[173] Eine vollständige Liste der Mitglieder ist zu finden unter: https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108/signatures. Zu den afrikanischen Ländern zählen Cabo Verde, Mauritius, Marokko, Senegal und Tunesien, die lateinamerikanischen Länder umfassen Argentinien, Mexiko und Uruguay. Burkina Faso wurde eingeladen, dem Übereinkommen beizutreten.

[174] Siehe den Wortlaut des modernisierten Übereinkommens: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

[175] Gemäß seinem Beschluss über das Änderungsprotokoll vom 18. Mai 2018 forderte das Ministerkomitee „die Mitgliedstaaten und die anderen Parteien des Übereinkommens nachdrücklich dazu auf, unverzüglich die erforderlichen Maßnahmen zu ergreifen, damit das Protokoll innerhalb von drei Jahren nach seiner Auflage zur Unterzeichnung in Kraft treten kann, sowie auf schnellstem

Die Themen Datenverkehr und Datenschutz wurden in jüngster Zeit auch im Rahmen der G20 und der G7 behandelt. 2019 unterstützten die führenden Politiker weltweit erstmals die Idee, dass der Datenschutz zum Aufbau von Vertrauen in die digitale Wirtschaft beiträgt und den Datenverkehr erleichtert. Mit aktiver Unterstützung der Kommission[176] billigten die Staats- und Regierungschefs den Ansatz des „vertrauensvollen, freien Datenverkehrs", der ursprünglich von Japan in der Erklärung der Staats- und Regierungschefs der G20 von Osaka[177] sowie auf dem G7-Gipfel in Biarritz[178] vorgeschlagen wurde. Dieser Ansatz spiegelt sich auch in der Mitteilung der Kommission von 2020 über „Eine europäische Datenstrategie"[179] wider, in der die Kommission ihre Absicht betont, den Datenaustausch mit vertrauenswürdigen Partnern weiterhin zu fördern und gleichzeitig Missbräuche wie den unverhältnismäßigen Datenzugriff von (ausländischen) Behörden zu bekämpfen.

Dabei wird sich die EU auch auf eine Reihe von Instrumenten in verschiedenen Politikbereichen stützen können, in denen die Auswirkungen auf den Datenschutz zunehmend berücksichtigt werden: So gibt beispielsweise der erste EU-Rahmen für die Überprüfung ausländischer Investitionen, der ab Oktober 2020 in vollem Umfang gilt, der EU und ihren Mitgliedstaaten die Möglichkeit, Investitionstransaktionen zu überprüfen, die sich auf „den Zugang zu sensiblen Informationen, einschließlich personenbezogener Daten, oder die Fähigkeit, solche Informationen zu kontrollieren" auswirken, wenn sie die Sicherheit oder die öffentliche Ordnung beeinträchtigen.[180]

Die Kommission arbeitet mit gleich gesinnten Ländern in mehreren anderen multilateralen Foren zusammen, um ihre Werte und Standards aktiv zu fördern. Ein wichtiges Forum ist die kürzlich von der OECD eingerichtete Arbeitsgruppe für Datenqualitätsmanagement und Privatsphäre (Working Party on Data Governance and Privacy, DGP), die eine Reihe wichtiger Initiativen im Zusammenhang mit

---

Weg, jedoch spätestens ein Jahr nach dem Datum, an dem das Protokoll zur Unterzeichnung aufgelegt wurde, das zur Ratifizierung führende Verfahren nach ihrem jeweiligen nationalen Recht einzuleiten". Das Ministerkomitee wies außerdem „seine Mitglieder dazu an, den Gesamtfortschritt bei der Ratifizierung alle zwei Jahre zu überprüfen, wobei die erste Überprüfung ein Jahr nach dem Datum der Auflage zur Unterzeichnung des Protokolls erfolgen soll; diese Überprüfung findet auf Grundlage der Informationen statt, die jeder Mitgliedstaat und alle anderen Parteien des Übereinkommens dem Generalsekretär spätestens einen Monat vor einer solchen Überprüfung zur Verfügung stellen müssen". Siehe https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f.

[176] Am Rande des Gipfeltreffens zwischen der EU und Japan im April 2019 bekundete Kommissionspräsident Juncker seine Unterstützung für Japans Initiative zum „vertrauensvollen, freien Datenverkehr" und die Einführung des „Osaka-Track" und verpflichtete die Kommission, „bei beiden Initiativen eine aktive Rolle zu spielen".

[177] Siehe Text der Erklärung von Osaka der Staats- und Regierungschefs der G20 unter: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[178] Siehe Text der Biarritz-Strategie der G7 für einen offenen, freien und sicheren digitalen Wandel unter: https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf.

[179] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, 19.2.2020 (COM(2020) 66 final) (https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_de.pdf), S. 29.

[180] Artikel 4 Absatz 1 Buchstabe d der Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19.3.2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union (ABl. L 79I vom 21.3.2019, S. 1).

Datenschutz, Datenaustausch und Datenübermittlung verfolgt. Dies umfasst auch die Bewertung der OECD-Datenschutzleitlinien von 2013. Darüber hinaus leistete die Kommission einen aktiven Beitrag zur Empfehlung des Rates der OECD zur künstlichen Intelligenz (Recommendation of the Council on Artificial Intelligence[181]) und stellte sicher, dass der auf den Menschen ausgerichtete Ansatz der EU, d. h., dass KI-Anwendungen im Einklang mit den Grundrechten und insbesondere dem Datenschutz stehen müssen, in den endgültigen Text Eingang fand. Insbesondere sei darauf hingewiesen, dass in der KI-Empfehlung – die anschließend in die der Erklärung der Staats- und Regierungschefs der G20 von Osaka[182] beigefügten KI-Grundsätze der G20 aufgenommen wurde – die Grundsätze der Transparenz und der Erklärbarkeit verankert wurden, um „denjenigen, auf die sich ein KI-System nachteilig auswirkt, die Möglichkeit zu geben, dessen Ergebnis auf der Grundlage einfacher und leicht verständlicher Informationen über die Faktoren und die Logik anzufechten, auf die sich die Vorhersage, Empfehlung oder Entscheidung stützte“, wodurch die Grundsätze der DSGVO hinsichtlich einer automatisierten Entscheidungsfindung[183] in hohem Maße widergespiegelt werden.

Darüber hinaus intensiviert die Kommission ihren Dialog mit regionalen Organisationen und Netzwerken, die zunehmend eine zentrale Rolle bei der Gestaltung gemeinsamer Datenschutzstandards[184] spielen, um den Austausch bewährter Verfahren sowie die Zusammenarbeit zwischen den Durchsetzungsbehörden zu fördern. Dies betrifft insbesondere den Verband südostasiatischer Nationen (ASEAN) – auch im Rahmen seiner laufenden Arbeiten zu Datenübertragungsinstrumenten –, die Afrikanische Union, das Forum der asiatisch-pazifischen Datenschutzbehörden (APPA) und das iberoamerikanische Datenschutz-Netzwerk, die alle wichtige Initiativen in diesem Bereich eingeleitet haben und Foren für einen fruchtbaren Dialog zwischen Datenschutzbehörden und anderen Interessenträgern bieten.

Afrika ist ein gutes Beispiel für die Komplementarität zwischen der nationalen, regionalen und globalen Dimension des Datenschutzes. Digitale Technologien verändern den afrikanischen Kontinent rasch und tief greifend. Dies birgt das Potenzial, die Verwirklichung der Ziele für nachhaltige Entwicklung durch Steigerung des Wirtschaftswachstums, Linderung der Armut und Verbesserung der Lebensbedingungen der Menschen zu beschleunigen. Ein moderner Datenschutzrahmen, der Investitionen anzieht und die Entwicklung wettbewerbsfähiger Unternehmen fördert und gleichzeitig zur Achtung der Menschenrechte, der Demokratie und der Rechtsstaatlichkeit beiträgt, ist ein Kernelelement dieses Wandels. Eine Harmonisierung der Datenschutzvorschriften auf dem gesamten afrikanischen Kontinent würde die Integration des digitalen

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[182] G20-Ministererklärung zu Handel und Digitaler Wirtschaft unter: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

[183] Siehe Artikel 13 Absatz 2 Buchstabe f, Artikel 14 Absatz 2 Buchstabe g und Artikel 22 der DSGVO.

[184] Siehe beispielsweise das Übereinkommen der Afrikanischen Union über Cybersicherheit und Schutz personenbezogener Daten (*Convention on Cyber Security and Personal Data Protection*, „Übereinkommen von Malabo“) und die vom iberoamerikanischen Datenschutz-Netzwerk entwickelten Datenschutzstandards für die iberoamerikanischen Staaten (*Standards for Data Protection for the Ibero-American States*).

Marktes ermöglichen, während eine Angleichung an globale Standards den Datenaustausch mit der EU erleichtern würde. Diese unterschiedlichen Dimensionen des Datenschutzes sind miteinander verknüpft und verstärken sich gegenseitig.

In vielen afrikanischen Ländern wächst derzeit das Interesse an Datenschutz, und die Zahl der afrikanischen Länder, die moderne Datenschutzvorschriften verabschiedet haben oder im Begriff sind, welche zu verabschieden, die das Übereinkommen 108 des Europarats[185] oder das Übereinkommen von Malabo[186] ratifiziert haben, nimmt weiter zu.[187] Gleichzeitig ist der Rechtsrahmen auf dem afrikanischen Kontinent nach wie vor sehr uneinheitlich und fragmentiert. In vielen Ländern gibt es immer noch nur wenige oder gar keine Datenschutzgarantien. Auch heute noch sind Maßnahmen zur Beschränkung des Datenverkehrs weitverbreitet und behindern die Entwicklung einer regionalen digitalen Wirtschaft.

Um die gegenseitigen Vorteile angeglichener Datenschutzvorschriften zu nutzen, wird die Kommission mit ihren afrikanischen Partnern sowohl bilateral als auch in regionalen Foren zusammenarbeiten.[188] Diese Zusammenarbeit stützt sich auf die Arbeit der Taskforce „Digitale Wirtschaft" der EU und der Afrikanischen Union im Rahmen der neuen Partnerschaft zwischen Europa und Afrika im Bereich der digitalen Wirtschaft (New Africa-Europe Digital Economy Partnership[189]). Um diese Ziele zu unterstützen, wurde zudem der Geltungsbereich des Partnerschaftsinstruments der Kommission „Enhanced Data Protection and Data Flows" (Verbesserter Datenschutz und Datenverkehr) auf Afrika ausgeweitet. Mit dem Projekt sollen afrikanische Länder unterstützt werden, die beabsichtigen, moderne Datenschutzrahmen zu entwickeln oder die Kapazitäten ihrer Regulierungsbehörden durch Schulungen, Wissensaustausch und den Austausch bewährter Verfahren zu stärken.

---

[185] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarats, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD.

[186] Übereinkommen der Afrikanischen Union über Cybersicherheit und Schutz personenbezogener Daten, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Darüber hinaus haben mehrere regionale Wirtschaftsgemeinschaften Datenschutzvorschriften entwickelt, z. B. die Wirtschaftsgemeinschaft der westafrikanischen Staaten (ECOWAS) und die Entwicklungsgemeinschaft des Südlichen Afrika (SADC). Siehe jeweils http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf und http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf.

[188] Unter anderem im Rahmen der „Policy and Regulation Initiative for Digital Africa" (PRIDA), siehe Informationen unter: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida.

[189] Siehe Gemeinsame Mitteilung an das Europäische Parlament und den Rat: Auf dem Weg zu einer umfassenden Strategie mit Afrika (abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020JC0004&qid=1596115173459&from=DE); Taskforce „Digitale Wirtschaft", New Africa-Europe Digital Economy Partnership: Accelerating the Achievement of the Sustainable Development Goals (abrufbar unter: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

Und nicht zuletzt setzt die Kommission sich zwar für die Angleichung der Datenschutzstandards auf internationaler Ebene ein, um den Datenverkehr und somit den Handel zu erleichtern, ist aber – wie kürzlich in der Datenstrategie hervorgehoben – auch entschlossen, digitalen Protektionismus zu bekämpfen.[190] Daher hat sie konkrete Bestimmungen zum Datenverkehr und Datenschutz bei Handelsabkommen ausgearbeitet, die sie bei ihren bilateralen – zuletzt mit Australien, Neuseeland und dem Vereinigten Königreich – und multilateralen Verhandlungen wie beispielsweise den laufenden Gesprächen mit der WTO zum elektronischen Geschäftsverkehr systematisch vorlegt. Diese horizontalen Bestimmungen schließen ungerechtfertigte Beschränkungen, z. B. zwingende Anforderungen zur Datenlokalisierung, aus, ohne die Regelungsautonomie der Parteien in Bezug auf die Wahrung des Grundrechts auf Datenschutz zu beeinträchtigen.

Die Datenschutzdialoge und Handelsgespräche müssen zwar getrennt geführt werden, können sich aber ergänzen. Eine auf hohen Standards beruhende Angleichung, flankiert durch einen wirksamen Durchsetzungsmechanismus, bildet die stärkste Grundlage für den Austausch personenbezogener Daten, was von den internationalen Partnern zunehmend anerkannt wird. Da Unternehmen vermehrt grenzüberschreitend arbeiten und lieber in allen ihren Geschäftsbetrieben weltweit ähnliche Regeln befolgen, trägt eine solche Angleichung dazu bei, ein Umfeld zu schaffen, das förderlich für Direktinvestitionen ist, den Handel erleichtert und das Vertrauen zwischen Geschäftspartnern stärkt. Daher sollten Synergien zwischen Handels- und Datenschutzinstrumenten weiter geprüft werden, um den freien und sicheren internationalen Datenverkehr zu gewährleisten, der für die Geschäftstätigkeit, die Wettbewerbsfähigkeit und das Wachstum europäischer Unternehmen, einschließlich KMU, in unserer zunehmend digitalisierten Wirtschaft unerlässlich ist.

[190] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_de.pdf, S. 27.

ANHANG I – Klauseln für fakultative Spezifikationen durch die nationale Gesetzgebung

Gegenstand	Anwendungsbereich	Artikel der DSGVO
Spezifikationen für rechtliche Verpflichtungen und öffentliche Aufgaben	Anpassung der Anwendung der Bestimmungen in Bezug auf die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder einer öffentlichen Aufgabe, einschließlich besonderer Verarbeitungssituationen gemäß Kapitel IX	Artikel 6 Absatz 2 und Artikel 6 Absatz 3
Altersgrenze für die Einwilligung in Bezug auf Dienste der Informationsgesellschaft	Festlegung des Mindestalters zwischen 13 und 16 Jahren	Artikel 8 Absatz 1
Verarbeitung besonderer Datenkategorien	Einführung oder Aufrechterhaltung zusätzlicher Bedingungen, einschließlich Beschränkungen, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist	Artikel 9 Absatz 4
Ausnahmen von Informationsanforderungen	Erlangung oder Offenlegung, die durch Rechtsvorschriften ausdrücklich geregelt ist oder unter das gesetzlich geregelte Berufsgeheimnis fällt	Artikel 14 Absatz 5 Buchstaben c und d
Automatisierte Entscheidungsfindung im Einzelfall	Zulässigkeit für die automatisierte Entscheidungsfindung als Ausnahme von dem allgemeinen Verbot	Artikel 22 Absatz 2 Buchstabe b
Beschränkungen der Rechte betroffener Personen	Beschränkungen gemäß den Artikeln 12 bis 22, Artikel 34 und den entsprechenden Bestimmungen des Artikels 5, wenn dies zur Wahrung erschöpfend aufgeführter wichtiger Ziele notwendig und verhältnismäßig ist	Artikel 23 Absatz 1
Verpflichtende Konsultation und Genehmigung	Verpflichtung der Verantwortlichen, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe die Datenschutzbehörde zu konsultieren oder deren Genehmigung einzuholen	Artikel 36 Absatz 5
Benennung eines Datenschutzbeauftragten in weiteren Fällen	Benennung eines Datenschutzbeauftragten in anderen als den in Artikel 37 Absatz 1 genannten	Artikel 37 Absatz 4

	Fällen	
Beschränkungen von Datenübermittlungen	Beschränkung der Übermittlung bestimmter Kategorien personenbezogener Daten	Artikel 49 Absatz 5
Einreichen von Beschwerden und gerichtlichen Klagen durch Organisationen aus eigenem Recht	Ermächtigung von Datenschutzorganisationen zur Einreichung von Beschwerden und gerichtlichen Klagen unabhängig vom Auftrag einer betroffenen Person	Artikel 80 Absatz 2
Zugang zu amtlichen Dokumenten	Vereinbarung des Zugangs der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten	Artikel 86
Verarbeitung der nationalen Kennziffer	Spezifische Bedingungen für die Verarbeitung einer nationalen Kennziffer	Artikel 87
Datenverarbeitung im Beschäftigungskontext	Spezifischere Vorschriften hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten	Artikel 88
Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu Forschungszwecken und zu statistischen Zwecken	Ausnahmen von bestimmten Rechten der betroffenen Personen insoweit, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen	Artikel 89 Absätze 2 und 3
Vereinbarkeit des Datenschutzes mit Geheimhaltungspflichten	Spezifische Vorschriften zu Untersuchungsbefugnissen von Datenschutzbehörden gegenüber Verantwortlichen oder Auftragsverarbeitern, die dem Berufsgeheimnis unterliegen	Artikel 90

ANHANG II – Übersicht über die Ressourcen der Datenschutzbehörden

Die nachstehende Tabelle enthält eine Übersicht über die personellen und finanziellen Ressourcen der Datenschutzbehörden für jeden EU- bzw. EWR-Mitgliedstaat.[191]

Beim Vergleich der Zahlen zwischen den Mitgliedstaaten ist zu berücksichtigen, dass den Behörden möglicherweise Aufgaben übertragen wurden, die über die in der DSGVO vorgesehenen hinausgehen, und dass diese Aufgaben von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein können. Das Verhältnis des von den Behörden pro eine Million Einwohner beschäftigten Personals und das Verhältnis des Budgets der Behörden pro eine Million Euro des BIP werden nur angeführt, um zusätzliche Vergleichselemente zwischen Mitgliedstaaten ähnlicher Größe zu liefern, und sollten nicht isoliert betrachtet werden. Bei der Beurteilung der Ressourcen einer bestimmten Behörde sollten die absoluten Zahlen, Quoten und Entwicklungen der vergangenen Jahre zusammengenommen betrachtet werden.

	PERSONAL (Vollzeitäquivalente)					BUDGET (in EUR)				
EU-/EWR-Mitgliedstaat	2019	Prognose 2020	% Zuwachs 2016–2019	% Zuwachs 2016–2020 (Prognose)	Personal pro eine Million Einwohner (2019)	2019	Prognose 2020	% Zuwachs 2016–2019	% Zuwachs 2016–2020 (Prognose)	Budget pro eine Million EUR des BIP (2019)
Österreich	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Belgien	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
Bulgarien	60	60	-14 %	-14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Kroatien	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Zypern	24	22	k. A.	k. A.	27,4	503 855	k. A.	114 %	k. A.	23,0
Tschechische Republik	101	109	0 %	8 %	9,5	6 541 288	6 720 533	10 %	13 %	29,7
Dänemark	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Estland	16	18	-11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Finnland	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
Frankreich	215	225	9 %	14 %	3,2	18 506 734	20 143 889	-2 %	7 %	7,7
Deutschland	888	1002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Griechenland	33	46	-15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Ungarn	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Island	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Irland	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Italien	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Lettland	19	31	-10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Litauen	46	52	-8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Luxemburg	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Malta	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Niederlande	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Norwegen	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Polen	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Portugal	25	27	-4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Rumänien	39	47	-3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9
Slowakei	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Slowenien	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7
Spanien	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Schweden	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5

[191] Mit Ausnahme von Liechtenstein.

INSGESAMT	2 966	3 372	42 %	62 %	6,6	249 127 139	273 782 870	49 %	64 %	17,4

Quelle der Rohdaten: Beitrag des Ausschusses. Berechnungen der Kommission.