EUROPÄISCHE
KOMMISSION

Brüssel, den 24.6.2020
COM(2020) 264 final

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

{SWD(2020) 115 final}

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

1 DATENSCHUTZVORSCHRIFTEN ALS GRUNDPFEILER DER TEILHABE DER BÜRGERINNEN UND BÜRGER UND DES ANSATZES DER EU FÜR DEN DIGITALEN WANDEL

Bei diesem Bericht handelt es sich um den ersten Bericht über die Bewertung und Überprüfung der Datenschutz-Grundverordnung[1] (im Folgenden „DSGVO"), insbesondere über die Anwendung und die Funktionsweise der Vorschriften über die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen sowie der Vorschriften über die Zusammenarbeit und Kohärenz nach Artikel 97 der DSGVO.

Die seit dem 25. Mai 2018 geltende DSGVO bildet das Kernstück des EU-Rahmens[2], der das in der Charta der Grundrechte der Europäischen Union (Artikel 8) und in den Verträgen (Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union, im Folgenden „AEUV") verankerte Grundrecht auf Datenschutz garantiert. Die DSGVO stärkt die Datenschutzgarantien, gewährt dem Einzelnen zusätzliche und stärkere Rechte, erhöht die Transparenz und begründet eine erhöhte Rechenschaftspflicht und Verantwortung all derjenigen, die in ihren Anwendungsbereich fallende personenbezogene Daten verarbeiten. Sie stattet die unabhängigen Datenschutzbehörden mit stärkeren und harmonisierten Durchsetzungsbefugnissen aus und führt ein neues Verwaltungssystem ein. Zudem schafft sie gleiche Wettbewerbsbedingungen für alle im EU-Markt tätigen Unternehmen, unabhängig davon, wo sie niedergelassen sind, und gewährleistet den freien Datenverkehr innerhalb der EU, wodurch der Binnenmarkt gestärkt wird.

Die DSGVO ist ein wichtiger Bestandteil des auf den Menschen ausgerichteten technologischen Ansatzes und eine Orientierungshilfe für den Einsatz von Technologie im doppelten Übergang zu einer grünen und digitalen Wirtschaft, der für die Politikgestaltung der EU kennzeichnend ist. Dies wurde kürzlich im Weißbuch zur künstlichen Intelligenz[3] und in der Mitteilung über eine europäische Datenstrategie[4] (im Folgenden „Datenstrategie") vom Februar 2020 hervorgehoben.

---

[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 (ABl. L 119 vom 4.5.2016, S. 1).

[2] Nach ihrer Aufnahme in das Abkommen über den Europäischen Wirtschaftsraum (EWR) gilt die Verordnung auch für Norwegen, Island und Liechtenstein.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

In einer Wirtschaft, die zunehmend auf der Verarbeitung von Daten, einschließlich personenbezogener Daten, beruht, ist die DSGVO ein wesentliches Instrument, mit dem sichergestellt werden soll, dass der Einzelne eine bessere Kontrolle über seine personenbezogenen Daten hat und dass diese Daten rechtmäßig, nach Treu und Glauben und transparent verarbeitet werden. Gleichzeitig trägt die DSGVO zur Förderung vertrauenswürdiger Innovationen bei, insbesondere durch ihren risikobasierten Ansatz und Grundsätze wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Die Kommission hat vorgeschlagen, den Rechtsrahmen für den Datenschutz und den Schutz der Privatsphäre[5] durch die e-Datenschutz-Verordnung[6] zu ergänzen, die die derzeitige e-Datenschutz-Richtlinie[7] ersetzen soll. Dieser Vorschlag wird derzeit von den gesetzgebenden Organen geprüft und sollte unbedingt rasch angenommen werden.

Im Rahmen der zentralen Prioritäten der Kommission eines „Europa für das digitale Zeitalter“[8] und des „europäischen Grünen Deals“[9] können neue Initiativen entwickelt werden, um die Bürgerinnen und Bürger in die Lage zu versetzen, eine aktivere Rolle bei der digitalen Umstellung und bei der Nutzung digitaler Instrumente zu spielen, um eine klimaneutrale Gesellschaft und eine nachhaltigere Entwicklung zu erreichen. Die DSGVO setzt einen Rahmen für diese Initiativen und stellt sicher, dass sie so konzipiert sind, dass sie den Einzelnen wirksam befähigen.

In der Datenstrategie[10] wird die Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarkts für Daten sowie zehn sektorspezifischer gemeinsamer europäischer Datenräume gefordert, die für den doppelten Übergang zu einer grünen und digitalen Wirtschaft relevant sind[11]. Für all diese Prioritäten ist ein klarer und praktikabler Rahmen für einen sicheren Datenaustausch und eine bessere Datenverfügbarkeit von entscheidender Bedeutung. In der Datenstrategie teilte die Kommission zudem ihre Absicht mit, in künftigen Rechtsvorschriften zu prüfen, wie die Nutzung von Daten in öffentlichen Datenbanken für wissenschaftliche

---

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy

[5] Dieser Rechtsrahmen umfasst auch die Richtlinie zum Datenschutz bei der Strafverfolgung (Richtlinie (EU) 2016/680) und die Datenschutzverordnung für Organe und Einrichtungen der EU (Verordnung (EU) 2018/1725).

[6] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 010 final – 2017/03 (COD).

[7] 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 (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 0037).

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_de

[9] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Der europäische Grüne Deal (COM(2019) 640 final).

[10] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, COM(2020) 66 final.

[11] Diese zehn sektorspezifischen gemeinsamen europäischen Datenräume decken folgende Bereiche ab: Gesundheit, verarbeitendes Gewerbe, Energie, Mobilität, Landwirtschaft, Finanzdaten, öffentliche Verwaltung, einen gemeinsamen europäischen Datenraum für Datenkompetenzen, einen Datenraum für den europäischen Grünen Deal und eine europäische Cloud für offene Wissenschaft.

Forschungszwecke im Einklang mit der DSGVO ermöglicht werden kann. Die Datenräume sollen von dem europäischen Cloud-Zusammenschluss unterstützt werden, der Datenverarbeitungs- und Cloud-Infrastrukturdienste im Einklang mit der DSGVO anbietet. Die DSGVO gewährleistet ein hohes Schutzniveau für personenbezogene Daten und eine zentrale Rolle für den Einzelnen in all diesen Datenräumen und bietet gleichzeitig die notwendige Flexibilität, um unterschiedlichen Ansätzen Rechnung zu tragen.

Die Notwendigkeit, Vertrauen zu gewährleisten, und der Bedarf am Schutz personenbezogener Daten sind sicherlich nicht auf die EU beschränkt. Menschen in der ganzen Welt schätzen die Privatsphäre und die Sicherheit ihrer Daten zunehmend. Wie eine kürzlich durchgeführte weltweite Umfrage zeigt[12], empfinden sie dies als wichtigen Faktor, der ihre Kaufentscheidungen und ihr Online-Verhalten beeinflusst. Eine wachsende Zahl von Unternehmen hat auf diesen Bedarf an Privatsphäre reagiert, insbesondere indem sie freiwillig einige der in der DSGVO vorgesehenen Rechte und Garantien auf ihre nicht in der EU ansässigen Kunden ausgeweitet haben. Viele Unternehmen nutzen auch den Schutz personenbezogener Daten als Alleinstellungsmerkmal und Verkaufsargument auf dem Weltmarkt, indem sie innovative Produkte und Dienste mit neuartigen Datenschutz- oder Datensicherheitslösungen anbieten. Darüber hinaus wirft die verbesserte Fähigkeit privater und öffentlicher Akteure, Daten in großem Maßstab zu erheben und zu verarbeiten, wichtige und komplexe Fragen auf, die den Schutz der Privatsphäre zunehmend in den Mittelpunkt der öffentlichen Debatte in verschiedenen Teilen der Welt stellen.

Die Annahme der DSGVO hat andere Länder in vielen Regionen der Welt veranlasst zu erwägen, diesem Beispiel zu folgen. Dieser tatsächlich weltweite Trend ist unter anderem in Chile, Südkorea, Brasilien, Japan, Kenia, Indien, Kalifornien und Indonesien zu beobachten. Die Vorreiterrolle der EU im Bereich des Datenschutzes zeigt, dass sie weltweit Maßstäbe für die Regulierung der digitalen Wirtschaft fungieren kann. Diese Vorreiterrolle wurde von wichtigen Stimmen der internationalen Gemeinschaft wie dem Generalsekretär der Vereinten Nationen António Guterres begrüßt, dem zufolge die DSGVO als Blaupause für ähnliche Instrumente in anderen Regionen der Welt dient und der die EU und ihre Mitgliedstaaten nachdrücklich aufgefordert hat, nicht darin nachzulassen, als Vorreiter das digitale Zeitalter zu gestalten und bei technologischer Innovation und Regulierung an vorderster Front zu stehen.[13]

Die derzeitige Krise der COVID-19-Pandemie veranschaulicht lebhaft diese Globalisierung der Datenschutzdebatte, sowohl während der Krise als auch in der anschließenden Zeit der Wiederaufbaubemühungen. In der EU haben mehrere Mitgliedstaaten Notmaßnahmen ergriffen, um die öffentliche Gesundheit zu schützen.

---

[12] Siehe z. B. Cisco's Consumer Privacy Study 2019 (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Dieser Studie zufolge, in der 2600 Verbraucher weltweit befragt wurden, hat eine beträchtliche Zahl von Verbrauchern bereits Maßnahmen zum Schutz ihrer Privatsphäre ergriffen, beispielsweise durch einen Wechsel von Unternehmen oder Anbietern aufgrund deren Datenrichtlinien oder Verfahren des Datenaustauschs.

[13] Rede des Generalsekretärs der Vereinten Nationen vor dem italienischen Senat, 18. Dezember 2019 (abrufbar unter: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

Gemäß DSGVO muss bei jeder Beschränkung der Wesensgehalt der Grundrechte und Grundfreiheiten geachtet werden, und es muss sich dabei um eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft zum Schutz eines öffentlichen Interesses wie der öffentlichen Gesundheit handeln. Mit der Aufhebung von Eindämmungsmaßnahmen müssen die Entscheidungsträger den Erwartungen der Bürger gerecht werden, dass ihnen vertrauenswürdige digitale Lösungen angeboten werden, die das Recht auf Privatsphäre und den Schutz personenbezogener Daten achten.

In vielen Ländern wird der integrierte Schutz der Privatsphäre, wie er beispielsweise in der freiwilligen Nutzung, Datenminimierung und -sicherheit sowie im Ausschluss der Geolokalisierung zum Ausdruck kommt, als wesentlich erachtet, um die Zuverlässigkeit und gesellschaftliche Akzeptanz datengestützter Lösungen zur Überwachung und Eindämmung der Ausbreitung des Virus, zur Kalibrierung politischer Gegenmaßnahmen, zur Unterstützung von Patienten oder zur Umsetzung von Ausstiegsstrategien zu gewährleisten. In der EU hat sich der Rechtsrahmen für den Datenschutz und den Schutz der Privatsphäre[14] als ausreichend flexibles Instrument erwiesen, um die Entwicklung praktischer Lösungen (z. B. Nachverfolgungs-Apps) zu ermöglichen und gleichzeitig ein hohes Schutzniveau für personenbezogene Daten sicherzustellen. In diesem Zusammenhang veröffentlichte die Kommission am 16. April 2020 datenschutzrelevante Leitlinien zu Apps, die die Bekämpfung der Pandemie unterstützen.[15]

Der Schutz personenbezogener Daten ist auch von entscheidender Bedeutung, wenn es darum geht, die Manipulation von Wählerstimmen – insbesondere durch das Mikrotargeting von Wählerinnen und Wählern auf der Grundlage der unrechtmäßigen Verarbeitung personenbezogener Daten – zu verhindern, Eingriffe in demokratische Prozesse zu vermeiden und die offene Debatte, die Fairness und die Transparenz, die für eine Demokratie von wesentlicher Bedeutung sind, zu erhalten. Aus diesem Grund veröffentlichte die Kommission im September 2018 ihren Leitfaden zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen[16].

Bei dieser Bewertung und Überprüfung berücksichtigte die Kommission die Beiträge des Rates[17], des Europäischen Parlaments[18], des Europäischen

---

[14] Dieser Rahmen umfasst neben der DSGVO auch die e-Datenschutz-Richtlinie (Richtlinie 2002/58/EG), die unter anderem Vorschriften für den Zugang zu und die Speicherung von Informationen auf den Endgeräten des Nutzers enthält.

[15] Mitteilung C(2020) 2523 der Kommission „Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie“ (ABl. C 124I vom 17.4.2020, S. 1). Am 16. April 2020 haben die EU-Mitgliedstaaten mit Unterstützung der Kommission ein EU-Instrumentarium für den Einsatz mobiler Anwendungen zur Kontaktnachverfolgung und Warnung als Reaktion auf die Coronavirus-Pandemie entwickelt. Dies ist Teil eines gemeinsamen koordinierten Ansatzes zur Unterstützung der schrittweisen Aufhebung von Eindämmungsmaßnahmen. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Leitfaden der Kommission zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen – Ein Beitrag der Europäischen Kommission zum Treffen der Führungsspitzen in Salzburg am 19./20. September 2018 (COM(2018) 638 final).

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

Datenschutzausschusses[19] (im Folgenden der „Ausschuss“) und einzelner Datenschutzbehörden[20], der Multi-Stakeholder-Expertengruppe[21] und anderer Interessenträger, unter anderem durch Rückmeldungen zum Fahrplan[22].

Nach allgemeiner Auffassung hat die DSGVO zwei Jahre nach Beginn ihrer Anwendung ihre Ziele, nämlich die Stärkung des Rechts des Einzelnen auf Schutz personenbezogener Daten und die Gewährleistung des freien Verkehrs personenbezogener Daten innerhalb der EU, erreicht.[23] Es wurde jedoch auch eine Reihe von Bereichen ermittelt, in denen weitere Verbesserungen erforderlich sind. Wie die meisten Interessenträger und Datenschutzbehörden ist die Kommission der Ansicht, dass es in diesem Stadium verfrüht wäre, endgültige Schlussfolgerungen in Bezug auf die Anwendung der DSGVO zu ziehen. Beim Umgang mit den meisten der von den Mitgliedstaaten und Interessenträgern ermittelten Probleme dürften mehr Erfahrungswerte mit Blick auf die Anwendung der DSGVO in den kommenden Jahren von Vorteil sein. Nichtsdestoweniger werden in diesem Bericht die bisher bei der Anwendung der DSGVO aufgetretenen Herausforderungen sowie Möglichkeiten zu deren Bewältigung aufgezeigt.

Obgleich der Schwerpunkt dieser Bewertung und Überprüfung 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 auch Fragen zu behandeln, die in den letzten beiden Jahren von verschiedenen Akteuren angesprochen wurden.

2 WICHTIGSTE ERKENNTNISSE

Durchsetzung der DSGVO und Funktionsweise der Verfahren der Zusammenarbeit und Kohärenz

Mit der DSGVO wurde ein innovatives Verwaltungssystem geschaffen, das auf unabhängigen Datenschutzbehörden in den Mitgliedstaaten und deren Zusammenarbeit in grenzüberschreitenden Fällen sowie innerhalb des Ausschusses beruht. Nach allgemeiner Auffassung haben die Datenschutzbehörden in ausgewogener Weise von ihren verstärkten Abhilfebefugnissen wie Verwarnungen und Verweisen, Geldbußen und vorübergehenden oder endgültigen Einschränkungen für die Datenverarbeitung Gebrauch gemacht.[24] Die Kommission stellt fest, dass die

---

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

[19] 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_de

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_de

[21] Die von der Kommission zur Verordnung 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

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

[23] Siehe beispielsweise den Standpunkt und die Feststellungen des Rates sowie den Beitrag des Ausschusses.

[24] Siehe Punkt 2.1 der Arbeitsunterlage der Kommissionsdienststellen.

Behörden je nach Schwere der Zuwiderhandlungen Geldbußen in Höhe von einigen Tausend bis zu mehreren Millionen Euro verhängt haben. Andere Sanktionen wie Verarbeitungsverbote können eine mindestens ebenso abschreckende, wenn nicht sogar höhere Abschreckungswirkung haben als Geldbußen. Das übergeordnete Ziel der DSGVO besteht darin, Kultur und Verhalten aller beteiligten Akteure zum Nutzen des Einzelnen zu verändern. Ausführlichere Informationen über die Ausübung der Abhilfebefugnisse durch die Datenschutzbehörden sind der beiliegenden Arbeitsunterlage der Kommissionsdienststellen zu entnehmen.

Zwar ist es noch zu früh, um die Funktionsweise der neuen Verfahren für Zusammenarbeit und Kohärenz umfassend zu bewerten, doch haben die Datenschutzbehörden ihre Zusammenarbeit im Wege des Verfahrens der Zusammenarbeit und Kohärenz[25] und der umfassenden gegenseitigen Amtshilfe[26] ausgebaut. Das Verfahren der Zusammenarbeit und Kohärenz, das für den Binnenmarkt von zentraler Bedeutung ist, wird genutzt, um über viele grenzüberschreitende Fälle zu entscheiden.[27] Derzeit sind wichtige Entscheidungen mit grenzüberschreitender Dimension anhängig, die dem Verfahren der Zusammenarbeit und Kohärenz unterliegen. Diese Entscheidungen, die häufig große multinationale Technologieunternehmen betreffen, werden erhebliche Auswirkungen auf die Rechte des Einzelnen in vielen Mitgliedstaaten haben.

Die Entwicklung einer wirklich gemeinsamen europäischen Datenschutzkultur zwischen den Datenschutzbehörden ist jedoch noch im Gange. Die Datenschutzbehörden haben noch nicht in vollem Umfang von den Instrumenten Gebrauch gemacht, die die DSGVO bietet, wie z. B. gemeinsame Einsätze, die zu gemeinsamen Ermittlungen führen könnten. Bisweilen endete die Suche nach einem gemeinsamen Ansatz mit einer Einigung auf den kleinsten gemeinsamen Nenner, sodass Chancen zur Förderung einer stärkeren Harmonisierung vertan wurden.[28]

Weitere Fortschritte sind erforderlich, um die Bearbeitung grenzüberschreitender Fälle in der gesamten EU effizienter zu gestalten und zu harmonisieren, auch in verfahrensrechtlicher Hinsicht, u. a. in Bezug auf die Bearbeitung von Beschwerden, die Zulässigkeitskriterien für Beschwerden, die Dauer von Verfahren aufgrund unterschiedlicher Zeitrahmen oder das Fehlen von Fristen im nationalen Verwaltungsverfahrensrecht, den Zeitpunkt des Verfahrens, in dem das Recht auf Anhörung gewährt wird, oder die Unterrichtung und Beteiligung der Beschwerdeführer während des Verfahrens. Der vom Ausschuss angestoßene diesbezügliche Reflexionsprozess wird begrüßt, und die Kommission nimmt an den betreffenden Diskussionen teil.[29]

---

[25] Wenn ein Unternehmen Daten grenzüberschreitend verarbeitet, ist die zuständige Datenschutzbehörde die des Mitgliedstaats, in dem das Unternehmen seinen Hauptsitz hat.

[26] Siehe Punkt 2.2 der Arbeitsunterlage der Kommissionsdienststellen.

[27] Zwischen dem 25. Mai 2018 und dem 31. Dezember 2019 wurden 141 Entscheidungsentwürfe im Wege des Verfahrens der Zusammenarbeit und Kohärenz vorgelegt, von denen 79 in endgültigen Entscheidungen mündeten.

[28] Beispielsweise hätten die nationalen Listen der Arten von Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO erforderlich ist, besser harmonisiert werden können.

[29] Siehe Punkt 2.2 der Arbeitsunterlage der Kommissionsdienststellen.

Die Tätigkeiten und die Leitlinien des Ausschusses sind von entscheidender Bedeutung für den konsequenten Ausbau des Austauschs zwischen dem Ausschuss und den Interessenträgern.[30] Bis Ende 2019 hatte der Ausschuss 67 Dokumente angenommen, darunter 10 neue Leitlinien[31] und 43 Stellungnahmen[32]. Die Interessenträger begrüßen im Allgemeinen die Leitlinien des Ausschusses und fordern weitere Leitlinien zu Schlüsselkonzepten der DSGVO, weisen aber auch auf Ungereimtheiten zwischen den nationalen Leitlinien und den Leitlinien des Ausschusses hin. Sie betonen, dass mehr praktische Beratung und insbesondere konkretere Beispiele erforderlich sind und dass die Datenschutzbehörden mit den erforderlichen personellen, technischen und finanziellen Ressourcen ausgestattet werden müssen, um ihre Aufgaben wirksam wahrnehmen zu können.

Die Kommission hat immer wieder betont, dass die Mitgliedstaaten verpflichtet sind, den nationalen Datenschutzbehörden ausreichende personelle, finanzielle und technische Ressourcen bereitzustellen.[33] Die meisten Behörden profitierten von einer Personal- und Mittelaufstockung zwischen 2016 und 2019[34], wobei die irischen, niederländischen, isländischen, luxemburgischen und finnischen Behörden die größten relativen Personalaufstockungen verzeichneten. Da die größten multinationalen Technologieunternehmen in Irland und Luxemburg niedergelassen sind, fungieren die Datenschutzbehörden dieser Länder in vielen wichtigen grenzüberschreitenden Fällen als federführende Behörden und benötigen möglicherweise mehr Ressourcen, als die Bevölkerungszahl dieser Länder ansonsten vermuten ließe. Die Situation ist jedoch von Mitgliedstaat zu Mitgliedstaat nach wie vor uneinheitlich und insgesamt noch nicht zufriedenstellend. Die Datenschutzbehörden spielen eine wesentliche Rolle, wenn es darum geht, sicherzustellen, dass die DSGVO auf nationaler Ebene durchgesetzt wird und dass die Verfahren der Zusammenarbeit und Kohärenz innerhalb des Ausschusses wirksam funktionieren, darunter insbesondere das entsprechende Verfahren für grenzüberschreitende Fälle. Die Mitgliedstaaten werden daher aufgefordert, ihnen gemäß den Vorgaben der DSGVO angemessene Ressourcen zur Verfügung zu stellen.[35]

Harmonisierte Regelungen trotz gewisser Fragmentierung und unterschiedlicher Konzepte

Die Kommission überwacht, wie die DSGVO in der nationalen Gesetzgebung umgesetzt wird. Zum Zeitpunkt der Erstellung dieses Berichts hatten alle

[30] Insbesondere Vertreter der Wirtschaft und der Zivilgesellschaft. Siehe Punkt 2.3 der Arbeitsunterlage der Kommissionsdienststellen.

[31] Sie ergänzen die 10 Leitlinien, die von der Artikel-29-Datenschutzgruppe im Vorfeld des Inkrafttretens der Verordnung 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.

[32] 42 dieser Stellungnahmen wurden nach Artikel 64 DSGVO und eine nach Artikel 70 Absatz 1 Buchstabe s DSGVO angenommen und betrafen den Angemessenheitsbeschluss in Bezug auf Japan.

[33] 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 vom 24.7.2019).

[34] Insgesamt wurde im EWR zwischen 2016 und 2019 das Personal um 42 % und das Budget für die nationalen Datenschutzbehörden um 49 % aufgestockt.

[35] Siehe Punkt 2.4 der Arbeitsunterlage der Kommissionsdienststellen.

Mitgliedstaaten bis auf Slowenien neue Rechtsvorschriften erlassen bzw. ihr nationales Datenschutzrecht angepasst. Slowenien[36] wurde ersucht, der Kommission mitzuteilen, wann dieses Verfahren abgeschlossen sein wird.[37]

Die DSGVO sieht einen einheitlichen Ansatz für die Datenschutzvorschriften in der EU vor. Dadurch werden die Mitgliedstaaten jedoch auch verpflichtet, einige Bereiche[38] selbst gesetzlich zu regeln, während sie in anderen Bereichen die Möglichkeit haben, im Vergleich zur DSGVO konkretere Vorschriften festzulegen.[39] Folglich gibt es noch eine gewisse Fragmentierung, die insbesondere aufgrund der umfangreichen Anwendung fakultativer Spezifikationsklauseln zustande kommt. So schaffen beispielsweise die unterschiedlichen Regelungen in den Mitgliedstaaten hinsichtlich des Mindestalters von Kindern für die Einwilligung im Zusammenhang mit Diensten der Informationsgesellschaft Unsicherheit für die Kinder und ihre Eltern dahingehend, wie ihre Datenschutzrechte im Binnenmarkt Anwendung finden. Diese Fragmentierung schafft zudem Hürden für grenzüberschreitende Wirtschaftstätigkeiten, Innovation und insbesondere für die Entwicklung neuer Technologien und Cybersicherheitslösungen. Für das reibungslose Funktionieren des Binnenmarkts und um unnötige Hürden für Unternehmen zu vermeiden, ist es ferner von entscheidender Bedeutung, dass die nationalen Rechtsvorschriften nicht über die von der DSGVO gesetzten Spielräume hinausgehen oder zusätzliche Anforderungen vorschreiben, wenn es keinen Spielraum gibt.

Die Vereinbarkeit des Rechts auf Schutz der personenbezogenen Daten mit der Meinungs- und Informationsfreiheit sowie die Gewichtung dieser Rechte stellen für die nationale Gesetzgebung eine besondere Herausforderung dar. In einigen nationalen Rechtsvorschriften wird dem Grundsatz der Meinungsfreiheit Vorrang eingeräumt, während in anderen Rechtsvorschriften dem Schutz personenbezogener Daten Vorrang gewährt wird und die Anwendung von Datenschutzregeln nur in bestimmten Situationen ausgeschlossen ist, beispielsweise wenn eine Person mit öffentlichem Status betroffen ist. Andere Mitgliedstaaten sehen wiederum eine bestimmte Gewichtung durch den Gesetzgeber und/oder eine Einzelfallbewertung hinsichtlich der Abweichung von bestimmten Vorschriften der DSGVO vor.

Die Kommission wird die Bewertung der nationalen Rechtsvorschriften fortsetzen. Die Vereinbarkeit muss gesetzlich festgelegt werden, den Wesensgehalt dieser Grundrechte wahren und angemessen und erforderlich sein.[40] Die Datenschutzvorschriften (sowie deren Auslegung und Anwendung) sollten die Ausübung der Meinungs- und Informationsfreiheit nicht einschränken, indem beispielsweise eine abschreckende Wirkung geschaffen oder Druck auf Journalisten zur Preisgabe ihrer Quellen ausgeübt wird. Die Gewichtung dieser beiden Rechte im

[36] Kürzlich erst durch ein Schreiben von Kommissionsmitglied Reynders im März 2020.
[37] 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.
[38] Siehe Punkt 3.1 der Arbeitsunterlage der Kommissionsdienststellen.
[39] Siehe Punkt 3.2 der Arbeitsunterlage der Kommissionsdienststellen.
[40] Artikel 52 Absatz 1 der Charta.

nationalen Recht sollte sich an der Rechtsprechung des Gerichtshofs und des Europäischen Gerichtshof für Menschenrechte orientieren.[41]

Die Rechtsvorschriften der Mitgliedstaaten verfolgen bei der Umsetzung der Abweichungen des generellen Verbots betreffend die Verarbeitung besonderer Kategorien von personenbezogenen Daten unterschiedliche Ansätze, was den Umfang von Spezifikationen und Garantien anbelangt, darunter auch für Gesundheits- und Forschungszwecke. Um dieses Problem zu beheben, nimmt die Kommission zunächst einmal eine Aufstellung der verschiedenen Konzepte der Mitgliedstaaten[42] vor und wird im Anschluss daran die Ausarbeitung von Verhaltenskodizes unterstützen, was zu einem einheitlicheren Ansatz in diesem Bereich beitragen und die grenzüberschreitende Verarbeitung personenbezogener Daten erleichtern würde.[43] Darüber hinaus werden die künftigen Leitlinien des Ausschusses zur Verarbeitung von personenbezogenen Daten in der wissenschaftlichen Forschung zu einer Vereinheitlichung des Ansatzes beitragen. Die Kommission wird dem Ausschuss insbesondere in Bezug auf die Forschung im Gesundheitsbereich zuarbeiten, unter anderem in Form konkreter Fragen und der Analyse spezifischer Szenarien aus der Forschungsgemeinschaft.

[41] Siehe Punkt 3.1 der Arbeitsunterlage der Kommissionsdienststellen: Vereinbarkeit des Rechts auf Schutz der personenbezogenen Daten mit der Meinungs- und Informationsfreiheit.

[42] Die Kommission hat eine Studie über die Beurteilung der Rechtsvorschriften der Mitgliedstaaten bezüglich der Gesundheitsdaten mit Blick auf die DSGVO (Chafea/2018/Health/03, Einzelvertrag-Nr. 2019 70 01) eingeleitet.

[43] Siehe dazu die Maßnahmen der europäischen Datenstrategie, S. 34.

Befähigung jedes Einzelnen zur Kontrolle seiner Daten

Laut einer Umfrage zu den Grundrechten[44] haben 69 % der EU-Bevölkerung über 16 Jahren von der DSGVO gehört, und 71 % der Bürger in der EU kennen ihre nationale Datenschutzbehörde.

Immer mehr Bürger sind sich ihrer Rechte bewusst: das Recht auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten sowie auf Datenübertragbarkeit, das Recht auf Widerspruch gegen die Verarbeitung sowie auf eine höhere Transparenz. Mit der DSGVO wurden die Verfahrensrechte gestärkt, darunter auch das Recht auf Einreichen einer Beschwerde bei einer Datenschutzbehörde, unter anderem in Form von Verbandsklagen, sowie auf gerichtliche Rechtsbehelfe. Zwar machen Bürger verstärkt von diesen Rechten Gebrauch, dennoch gilt es, die Ausübung und vollständige Durchsetzung dieser Rechte zu vereinfachen. Die Überlegungen unter Federführung des Ausschusses werden die Ausübung einzelner Rechte weiter klarstellen und vereinfachen; es wird davon ausgegangen, dass sobald die vorgeschlagene Richtlinie über Verbandsklagen angenommen ist, Verbandsklagen[45] in allen Mitgliedstaaten durch Einzelpersonen eingereicht werden können und die Kosten für Klagen mit grenzüberschreitendem Bezug sinken.

Das Recht auf Datenübertragbarkeit birgt eindeutig Potenzial, das noch nicht vollständig ausgeschöpft ist, Einzelpersonen in den Mittelpunkt der Datenwirtschaft zu rücken, indem sie befähigt werden, zwischen verschiedenen Dienstleistern zu wechseln, verschiedene Dienste zu kombinieren, innovative Dienste zu nutzen und sich für die datenschutzfreundlichsten Dienste zu entscheiden. Dadurch werden Wettbewerb und Innovation indirekt angekurbelt. Zu den Prioritäten der Kommission gehört daher die Erschließung dieses Potenzials, insbesondere da angesichts der stärkeren Nutzung von IoT-Geräten immer mehr Daten durch Verbraucher generiert werden, die dadurch wiederum Gefahr laufen, unlauteren Praktiken und Abhängigkeiten von bestimmen Anbietern („Lock-in-Effekten“) ausgesetzt zu werden. Die Datenübertragbarkeit könnte wesentliche Vorteile in Bezug auf Gesundheit und Wohlbefinden, einen geringeren ökologischen Fußabdruck und den Zugang zu öffentlichen und privaten Diensten sowie eine Steigerung der Produktivität im verarbeitenden Gewerbe und der Produktqualität und -sicherheit bringen.

In der Datenstrategie wurde betont, dass Probleme, wie das Fehlen von Standards zur Bereitstellung von Daten in einem maschinenlesbaren Format behoben werden müssen, damit das Recht auf Datenübertragbarkeit, das derzeit auf einige wenige Bereiche (z. B. Banken und Telekommunikation) beschränkt ist, genutzt werden kann. Dies könnte insbesondere durch die Gestaltung geeigneter Instrumente, standardisierter Formate und von Schnittstellen erreicht werden.[46] Eine häufigere Wahrnehmung dieses Rechts könnte insbesondere auch durch die Inauftraggabe

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

[45] Mit der vorgeschlagenen Richtlinie über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher (COM(2018) 0184 final - 2018/089 (COD)) dürfte der Rahmen für Verbandsklagen auch im Bereich des Datenschutzes gestärkt werden.

[46] Dazu können Werkzeuge für die Verwaltung von Einwilligungen und Apps für die Verwaltung persönlicher Informationen gehören.

technischer Schnittstellen und maschinenlesbarer Formate erzielt werden, die eine Datenübertragbarkeit in Echtzeit ermöglichen. Eine verstärkte Nutzung des Rechts auf Datenübertragbarkeit könnte es Einzelpersonen erleichtern, die Verarbeitung ihrer Daten für das öffentliche Wohl zu gestatten (z. B. für die Förderung der Forschung im Gesundheitsbereich), sofern sie dies wünschen („Datenaltruismus"). In Vorbereitung des Legislativpakets über digitale Dienste[47] wird die Kommission die Rolle von Daten und datenbezogenen Verfahren im plattformbasierten Ökosystem umfassender untersuchen.

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

Möglichkeiten und Herausforderungen für Organisationen, insbesondere für kleine und mittlere Unternehmen

Die DSGVO und die Verordnung über den freien Verkehr nicht-personenbezogener Daten[48] bieten Chancen für Unternehmen, indem Wettbewerb und Innovation gefördert werden, der freie Verkehr von Daten innerhalb der EU gewährleistet und gleiche Wettbewerbsbedingungen für Unternehmen mit Sitz außerhalb der EU geschaffen werden.[49] Das Recht auf Datenübertragbarkeit hat in Verbindung mit der steigenden Zahl von Personen, die datenschutzfreundlichere Lösungen suchen, das Potenzial, die Hürden für den Marktzugang von Unternehmen zu senken und Wachstumsmöglichkeiten auf der Grundlage von Vertrauen und Innovation zu eröffnen. Einige Interessenträger berichten, dass die Anwendung der DSGVO insbesondere für kleine und mittlere Unternehmen (KMU) eine Herausforderung darstellt. Aus dem risikobasierten Ansatz geht hervor, dass Abweichungen auf der Grundlage der Größe des Wirtschaftsteilnehmers ungeeignet wären, da allein die Größe keine Aussage über die Risiken für Verbraucher hinsichtlich der von dem Unternehmen durchgeführten Verarbeitung personenbezogener Daten zulässt. Verschiedene Datenschutzbehörden haben praktische Werkzeuge bereitgestellt, um die Umsetzung der DSGVO für KMU, deren Verarbeitungstätigkeiten mit geringen Risiken behaftet sind, zu vereinfachen. Diese Bemühungen sollten insbesondere im Rahmen eines gemeinsamen europäischen Ansatzes intensiviert und ausgeweitet werden, um Hürden für den Binnenmarkt zu vermeiden.

Die Datenschutzbehörden haben eine Reihe von Maßnahmen entwickelt, um KMU bei der Einhaltung der DSGVO zu unterstützen, zum Beispiel durch die Bereitstellung von Mustern für Verarbeitungsverträge und Verzeichnisse von Verarbeitungstätigkeiten sowie Seminare und Hotlines zur Beratung. Eine Reihe dieser Initiativen wurden mit EU-Finanzmitteln unterstützt.[50] Weitere Maßnahmen sollten erwogen werden, um die Anwendung der DSGVO für KMU zu erleichtern.

Die DSGVO bietet für alle Unternehmen und Organisationen ein Instrumentarium mit Verhaltenskodizes, Zertifizierungsverfahren, Standardvertragsklauseln usw., um sie dabei zu unterstützen, die Einhaltung der Verordnung nachzuweisen. Von diesem Instrumentarium sollte vollumfänglich Gebrauch gemacht werden. KMU betonen insbesondere, wie wichtig und hilfreich Verhaltenskodizes sind, die auf sie zugeschnitten sind und keine unverhältnismäßigen Kosten nach sich ziehen. Die Aspekte Zertifizierungsverfahren, Sicherheit (einschließlich Cybersicherheit) und Datenschutz durch Technikgestaltung sind wichtige Elemente, die es im Rahmen der

---

[48] 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).

[49] Siehe Punkt 5 der Arbeitsunterlage der Kommissionsdienststellen. Siehe auch Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (COM(2019) 250 final), in denen die Vorschriften für die Verarbeitung gemischter Datensätze aus personenbezogenen und nicht-personenbezogenen Daten erläutert und so für Unternehmen, einschließlich KMU, praktisch dargelegt werden.

[50] Die Kommission stellte in drei Finanzierungswellen Zuschüsse in Höhe von insgesamt 5 Millionen EUR zur Verfügung, wovon die letzten beiden konkret zur Unterstützung der nationalen Datenschutzbehörden bei ihren Bemühungen, sich an Bürger und kleine und mittlere Unternehmen zu wenden, erfolgten: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en. Eine weitere Million EUR wird 2020 zugewiesen.

DSGVO zu beachten gilt und die von einem gemeinsamen und ehrgeizigen EU-weiten Ansatz profitieren könnten. Die Kommission arbeitet derzeit an Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter[51], die auf den laufenden Arbeiten zur Aktualisierung der Standardvertragsklauseln für internationale Datenübermittlungen aufbauen.[52]

Die Anwendung der DSGVO auf neue Technologien

Die DSGVO wurde technologieneutral ausgearbeitet und stützt sich auf Grundsätze; sie ist daher geeignet, auch neue, in der Entwicklung befindliche Technologien abzudecken.

Sie ist ein wichtiges und flexibles Instrument, um zu gewährleisten, dass die Entwicklung neuer Technologien im Einklang mit den Grundrechten steht. Der Rechtsrahmen für den Datenschutz und den Schutz der Privatsphäre hat während der COVID-19-Krise seine Bedeutung und Flexibilität unter Beweis gestellt, insbesondere im Zusammenhang mit der Konzeption von Kontaktnachverfolgungs-Apps und anderen technologischen Lösungen zur Bekämpfung der Pandemie. Es gibt noch einige Herausforderungen dahingehend, klarzustellen, wie die bewährten Datenschutzgrundsätze auf bestimmte Technologien wie künstliche Intelligenz, Blockchain, das Internet der Dinge oder die Gesichtserkennung angewendet werden können, die es kontinuierlich zu überwachen gilt. Das Weißbuch der Kommission zur künstlichen Intelligenz[53] leitete beispielsweise eine öffentliche Debatte über die konkreten Umstände, die den Einsatz künstlicher Intelligenz für die Zwecke der biometrischen Fernidentifizierung (wie Gesichtserkennung) im öffentlichen Raum rechtfertigen könnten, und über gemeinsame Sicherheitsvorkehrungen ein. In diesem Zusammenhang sollten Datenschutzbehörden bereit sein, technische Gestaltungsverfahren von Anbeginn zu begleiten.

Darüber hinaus ist eine strenge und wirksame Durchsetzung der DSGVO gegenüber großen digitalen Plattformen und integrierten Unternehmen, darunter in Bereichen wie Online-Werbung und Mikrotargeting, entscheidend für den Schutz der Bürger.

Ausarbeitung eines modernen Instrumentariums für internationale Datenübermittlungen

Die DSGVO bietet ein modernisiertes Instrumentarium, das die Übermittlung personenbezogener Daten aus der EU an Drittländer und internationale Organisationen erleichtert und gleichzeitig ein hohes Datenschutzniveau gewährleistet. Die Kommission hat in den letzten beiden Jahren ihre Arbeiten intensiviert, um das volle Potenzial der im Rahmen der DSGVO verfügbaren Instrumente auszuschöpfen.

Dazu zählte auch die aktive Zusammenarbeit mit wichtigen Partnern im Hinblick auf die Erzielung eines Angemessenheitsbeschlusses. Mit einem solchen Beschluss wird der sichere und freie Verkehr personenbezogener Daten in das jeweilige Drittland ermöglicht, ohne dass der Datenexporteur weitere Garantien bieten oder eine

[51] Nach Artikel 28 DSGVO.
[52] Nach Artikel 46 DSGVO.
[53] Weißbuch zur künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen (COM(2020) 65 final).

Genehmigung einholen muss. So wurde insbesondere mit den Angemessenheitsbeschlüssen zwischen der EU und Japan, die im Februar 2019 in Kraft traten, der weltweit größte Raum für den freien und sicheren Datenverkehr geschaffen. Darüber hinaus befinden sich die Verhandlung über einen Angemessenheitsbeschluss mit der Republik Korea in einem fortgeschrittenen Stadium, und Sondierungsgespräche mit anderen wichtigen Partnern in Asien und Lateinamerika sind im Gange.

Der Aspekt der Angemessenheit spielt auch eine wichtige Rolle im Zusammenhang mit den künftigen Beziehungen zum Vereinigten Königreich, sofern die geltenden Voraussetzungen erfüllt werden. Die 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. Darüber hinaus ist ein hohes Maß an Angleichung im Datenschutz wichtig, um zu gewährleisten, dass für zwei sehr eng verzahnte Wirtschaften gleiche Bedingungen herrschen. 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 DGSVO und der Richtlinie zum Datenschutz bei der Strafverfolgung[54] durch.

Im Rahmen der ersten Bewertung der DSGVO ist die Kommission auch verpflichtet, die nach den früheren Vorschriften angenommenen Angemessenheitsbeschlüsse zu überprüfen.[55] Die Kommissionsdienststellen haben einen intensiven Dialog mit jedem der elf betroffenen Drittstaaten und Gebiete[56] eingeleitet, um zu bewerten, wie sich ihre Datenschutzsysteme seit der Annahme des Angemessenheitsbeschlusses entwickelt haben und ob diese die von der DSGVO festgelegten Standards erfüllen. Die Notwendigkeit, die Kontinuität dieser Beschlüsse als wichtiges Instrument für Handel und internationale Kooperation zu gewährleisten, ist einer der Faktoren, der mehrere dieser Länder und Gebiete dazu bewogen hat, ihre Datenschutzgesetze zu aktualisieren und zu verstärken. Mit einigen dieser Länder und Gebiete werden derzeit weitere Garantien erörtert, um wesentliche Unterschiede hinsichtlich des Datenschutzes anzugehen. Angesichts der Tatsache, dass der Gerichtshof in seinem Urteil, das am 16. Juli verkündet werden soll, Klarstellungen liefern könnte, die für bestimmte Elemente des Angemessenheitsstandards relevant sein könnten, wird die Kommission über die Evaluierung der bestehenden Angemessenheitsbeschlüsse gesondert Bericht erstatten, nachdem der Gerichtshof sein Urteil in dieser Rechtssache erlassen hat.[57]

---

[54] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

[55] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

[56] Zu diesen Ländern und Gebieten gehören: Andorra, Argentinien, Färöer, Guernsey, Isle of Man, Israel, Jersey, Kanada, Neuseeland, Schweiz und Uruguay.

[57] Siehe Rechtssache C-311/18, Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems („Schrems II"), betreffend ein Vorabentscheidungsersuchen über die sogenannten

Neben ihrer Arbeiten zu den Angemessenheitsbeschlüssen beschäftigt sich die Kommission mit einer umfangreichen Modernisierung der Standardvertragsklauseln, um diese mit Blick auf die neuen mit der DSGVO eingeführten Anforderungen zu aktualisieren. Ziel ist es, die Gegebenheiten der Verarbeitungsvorgänge der modernen digitalen Wirtschaft besser widerzuspiegeln und die mögliche Notwendigkeit einer weiteren Klarstellung bestimmter Garantien auch mit Blick auf die künftige Rechtsprechung des Gerichtshofs[58] zu prüfen. Diese Klauseln sind mit Abstand das am häufigsten verwendete Datenübertragungsinstrument. Tausende EU-Unternehmen verlassen sich darauf, um ihren Kunden, Zulieferern, Partnern und Arbeitnehmern eine Vielzahl von Diensten anzubieten.

Der Ausschuss war auch aktiv an der Ausarbeitung internationaler Aspekte der DSGVO beteiligt; so auch an der Aktualisierung der Leitlinien zu bestehenden Datenübermittlungsverfahren, darunter verbindlichen internen Vorschriften und sogenannten „Abweichungen“, sowie an der Ausarbeitung der rechtlichen Infrastruktur für die Anwendung neuer, durch die DSGVO eingeführter Instrumente (wie Verhaltenskodizes und Zertifizierungsverfahren).

Damit Interessenträger das Instrumentarium der DSGVO für Datenübermittlungen uneingeschränkt nutzen können, ist es wichtig, dass der Ausschuss seine laufenden Arbeiten an den verschiedenen Übermittlungsverfahren intensiviert, unter anderem indem das Genehmigungsverfahren für verbindliche interne Vorschriften weiter vereinfacht wird, der Leitfaden für Verhaltenskodizes und die Zertifizierung als Instrumente für Datenübermittlungen abgeschlossen und das Zusammenspiel zwischen den Vorschriften für internationale Datenübermittlungen (Kapitel V) und den räumlichen Anwendungsbereich der DSGVO (Artikel 3) verdeutlicht werden.

Ein weiterer wichtiger Aspekt der internationalen Dimension der EU-Datenschutzvorschriften ist der erweiterte räumliche Anwendungsbereich der DSGVO, der auch die Verarbeitungstätigkeiten von Akteuren aus dem Nicht-EU-Ausland, die in der EU aktiv sind, erfasst werden. Um eine wirksame Einhaltung der DSGVO und gleiche Wettbewerbsbedingungen zu gewährleisten, ist es entscheidend, dass sich diese Erweiterung in den Durchsetzungsmaßnahmen der Datenschutzbehörden angemessen wiederspiegelt. Diese sollten insbesondere im Bedarfsfall den Vertreter des Verantwortlichen oder des Auftragsverarbeiters in der EU einbeziehen, der zusätzlich zu dem außerhalb der EU ansässigen Unternehmen bzw. anstelle des Unternehmens kontaktiert werden kann. Dieser Ansatz sollte energischer verfolgt werden, um klar zu machen, dass ausländische Unternehmen ohne Niederlassung in der EU nicht von den Verpflichtungen nach Maßgabe der DSGVO entbunden sind.

Förderung der Angleichung und der internationalen Zusammenarbeit im Bereich des Datenschutzes

Die DSGVO hat sich auf internationaler Ebene bereits als wichtiger Bezugspunkt etabliert und für viele Länder in der ganzen Welt als Katalysator gewirkt, die

---

Standardvertragsklauseln. Bestimmte Aspekte des Angemessenheitsstandards können jedoch durch das Gericht noch weiter präzisiert werden.

[58] Siehe Rechtssache Schrems II.

Einführung moderner Datenschutzvorschriften in Erwägung zu ziehen. Dieser Trend hin zu globaler Angleichung ist eine sehr positive Entwicklung, die neue Möglichkeiten für einen besseren Schutz von Personen in der EU bei der Übermittlung ihrer Daten ins Ausland eröffnet und gleichzeitig den Datenverkehr erleichtert.

Ausgehend von diesem Trend 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. Die Kommission hat sich bei ihren Bemühungen auf die aktive Unterstützung durch den Europäischen Auswärtigen Dienst und das Netz der EU-Delegationen in Drittländern und der Vertretungen bei internationalen Organisationen gestützt und wird dies auch weiterhin tun. Dies hat auch eine größere Kohärenz und Komplementarität zwischen den verschiedenen Aspekten der externen Dimension der EU-Politik ermöglicht – vom Handel bis hin zur neuen Partnerschaft zwischen der EU und Afrika. Auch die G20 und die G7 haben kürzlich den Beitrag des Datenschutzes zum Vertrauen in die digitale Wirtschaft und den Datenverkehr anerkannt, insbesondere durch den Ansatz des „vertrauensvollen, freien Datenverkehrs“, der ursprünglich vom japanischen G20-Vorsitz vorgeschlagen wurde.[59] In der Datenstrategie wird die Absicht der Kommission betont, den Datenaustausch mit vertrauenswürdigen Partnern weiter zu fördern und gleichzeitig gegen Missbrauch wie den unverhältnismäßigen Zugang von (ausländischen) Behörden zu personenbezogenen Daten vorzugehen.

Die Kommission setzt 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[60] hervorgehoben wurde – auch entschlossen, digitalen Protektionismus zu bekämpfen. Daher hat sie konkrete Bestimmungen zum Datenverkehr und Datenschutz bei Handelsabkommen[61] 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[62] systematisch vorlegt. Diese horizontalen Bestimmungen schließen ungerechtfertigte Beschränkungen wie zwingende Anforderungen zur Datenlokalisierung aus, ohne die Regelungsautonomie der Parteien in Bezug auf die Wahrung des Grundrechts auf Datenschutz zu beeinträchtigen.

---

[59] Siehe z. B. die Erklärung der Staats- und Regierungschefs der G20 von Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[60] Datenstrategie, S. 23.

[61] Siehe den Wortlaut der horizontalen Bestimmungen für den grenzüberschreitenden Datenverkehr und den Schutz personenbezogener Daten (in Handels- und Investitionsabkommen der EU): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[62] Im Anschluss an eine gemeinsame Erklärung, die die Minister am 25. Januar 2019 in Davos angenommen haben, führen nun 84 WTO-Mitglieder plurilaterale Verhandlungen über den elektronischen Geschäftsverkehr. Im Rahmen dieses Prozesses legte die EU am 3. Mai 2019 ihren Vorschlag zu künftigen Vorschriften und Verpflichtungen im Bereich des elektronischen Geschäftsverkehrs vor. Der Vorschlag enthält horizontale Bestimmungen über den Datenverkehr und den Schutz personenbezogener Daten: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

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 der zunehmend digitalisierten Wirtschaft unerlässlich ist.

Ebenso 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 unterstützen und auf diese Weise zu einer wirksameren Kriminalitätsbekämpfung beizutragen.

In Zeiten, in denen Probleme bei der Einhaltung von Datenschutzvorschriften oder Sicherheitsvorfälle unter Umständen in mehreren Ländern gleichzeitig viele Menschen betreffen, sollte die Zusammenarbeit „vor Ort“ zwischen europäischen und internationalen Regulierungsbehörden weiter verstärkt werden. Dies erfordert insbesondere die Entwicklung geeigneter Rechtsinstrumente für engere Formen der Zusammenarbeit und gegenseitigen Amtshilfe, unter anderem durch die Ermöglichung des erforderlichen Informationsaustauschs im Rahmen von Ermittlungen. Ganz in diesem Sinne richtet die Kommission auch eine „Datenschutzakademie“ ein, eine Plattform, auf der Datenschutzbehörden aus der EU und Drittländern Wissen, Erfahrungen und bewährte Verfahren austauschen können, um die Zusammenarbeit zwischen den für die Durchsetzung des Datenschutzes zuständigen Stellen zu erleichtern und zu unterstützen.

3 WEITERES VORGEHEN

Um das Potenzial der DSGVO voll auszuschöpfen, müssen ein harmonisiertes Konzept und eine gemeinsame europäische Datenschutzkultur geschaffen und eine effizientere und einheitlichere Bearbeitung grenzüberschreitender Fälle gefördert werden. Dies entspricht den Erwartungen der Menschen und Unternehmen und stellt ein wesentliches Ziel der Reform der EU-Datenschutzvorschriften dar. Ebenso wichtig ist es sicherzustellen, dass alle in der DSGVO vorgesehenen Instrumente in vollem Umfang genutzt werden, um eine effiziente Anwendung für Einzelpersonen und Unternehmen zu gewährleisten.

Die Kommission wird ihren bilateralen Austausch mit den Mitgliedstaaten über die Umsetzung der DSGVO fortsetzen und im Bedarfsfall weiterhin alle ihr zur Verfügung stehenden Instrumente nutzen, um die Einhaltung der Verpflichtungen aus der DSGVO durch die Mitgliedstaaten zu unterstützen.

Angesichts der laufenden Bewertung der nationalen Rechtsvorschriften, der kurzen praktischen Erfahrung seit Inkrafttreten der DSGVO und der Tatsache, dass sektorspezifische Rechtsvorschriften in vielen Mitgliedstaaten noch immer überarbeitet werden, ist es noch zu früh, endgültige Schlussfolgerungen hinsichtlich des derzeitigen Maßes an Fragmentierung zu ziehen. Was die mögliche

Rechtskollision aufgrund der Anwendung von Spezifikationsklauseln durch die Mitgliedstaaten betrifft, so bedarf es zunächst eines besseren Verständnisses der Folgen für die Verantwortlichen und die Auftragsverarbeiter.[63]

Bei der weiteren Behandlung dieser Fragen trägt die einschlägige Rechtsprechung der nationalen Gerichte und des Gerichtshofs zu einer einheitlichen Auslegung der Datenschutzvorschriften bei. So haben nationale Gerichte von der DSGVO abweichende nationale Bestimmungen unlängst für ungültig erklärt.[64]

Was die internationale Dimension anbelangt, so wird sich die Kommission weiterhin darauf konzentrieren, sich für die Angleichung der Datenschutzvorschriften als Mittel zur Gewährleistung eines sicheren Datenverkehrs einzusetzen. Dies umfasst verschiedene Formen der Arbeit „im Vorfeld", z. B. im Zusammenhang mit laufenden Reformen für neue oder aktualisierte Datenschutzgesetze oder der Forderung des Ansatzes des „vertrauensvollen, freien Datenverkehrs" in multilateralen Foren. Ferner umfasst dieses Engagement verschiedene Angemessenheitsdialoge und die Modernisierung und Erweiterung unseres Instrumentariums für Datenübermittlungen durch Aktualisierung der Standardvertragsklauseln und Schaffung der Grundlagen für Zertifizierungsverfahren. Ein weiterer Teil dieser Arbeit sind internationale Verhandlungen, etwa im Bereich des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln, um sicherzustellen, dass Daten mit angemessenen Datenschutzgarantien übermittelt werden. Darüber hinaus wird sich die Kommission darum bemühen, durch die Aufnahme von Verhandlungen über die internationale Zusammenarbeit und gegenseitige Amtshilfe zwischen den für die Durchsetzung des Datenschutzes zuständigen Stellen die Angleichung von der Theorie in die Praxis zu übertragen.

Auf der Grundlage dieser Bewertung der Anwendung der DSGVO seit Mai 2018 wurde festgestellt, dass die nachstehend aufgeführten Maßnahmen zur Unterstützung ihrer Anwendung erforderlich sind. Die Kommission wird die Umsetzung dieser Maßnahmen auch im Hinblick auf den im Jahr 2024 anstehenden Bewertungsbericht überwachen.

Umsetzung und Ergänzung des Rechtsrahmens

Die Mitgliedstaaten sollten

- die Angleichung ihrer sektorspezifischen Rechtsvorschriften an die DSGVO abschließen;
- erwägen, die Verwendung von Spezifikationsklauseln einzuschränken, die zu Fragmentierung führen und den freien Datenverkehr innerhalb der EU gefährden könnten;
- prüfen, ob die nationalen Rechtsvorschriften zur Umsetzung der DSGVO unter allen Umständen innerhalb des für die Rechtsvorschriften der Mitgliedstaaten vorgesehenen Spielraums liegen.

[63] Vgl. Standpunkt und Feststellungen des Rates zur Anwendung der DSGVO.
[64] Dies war in Deutschland und Spanien der Fall sowie in Österreich, wo eine Lücke in den nationalen Rechtsvorschriften geschlossen wurde.

Die Kommission wird

- den bilateralen Austausch mit den Mitgliedstaaten über die Vereinbarkeit der nationalen Rechtsvorschriften mit der DSGVO, einschließlich der Unabhängigkeit und der Ressourcen der nationalen Datenschutzbehörden, fortsetzen; ferner wird sie alle ihr zur Verfügung stehenden Instrumente, einschließlich Vertragsverletzungsverfahren, nutzen, um sicherzustellen, dass die Mitgliedstaaten die DSGVO einhalten;
- den weiteren Austausch von Meinungen und nationalen Vorgehensweisen zwischen den Mitgliedstaaten zu Themen unterstützen, die auf nationaler Ebene spezifiziert sind, um die Fragmentierung des Binnenmarkts zu verringern (wie etwa die Verarbeitung personenbezogener Daten im Zusammenhang mit Gesundheit und Forschung), oder die gegen andere Rechte (wie das auf freie Meinungsäußerung) abgewogen werden müssen;
- eine einheitliche Anwendung des Datenschutzrahmens in Bezug auf neue Technologien unterstützen, um Innovationen und technologische Entwicklungen zu fördern;
- die Sachverständigengruppe der Mitgliedstaaten für die DSGVO (die in der Übergangsphase vor Inkrafttreten der DSGVO eingesetzt wurde) nutzen, um Gespräche und den Erfahrungsaustausch zwischen den Mitgliedstaaten und mit der Kommission zu erleichtern;
- prüfen, ob es im Lichte weiterer Erfahrungen und der einschlägigen Rechtsprechung angebracht sein könnte, künftige gezielte Änderungen bestimmter Bestimmungen der DSGVO vorzuschlagen, insbesondere in Bezug auf Verzeichnisse von Verarbeitungstätigkeiten von KMU, deren Kerngeschäft nicht die Verarbeitung personenbezogener Daten ist (geringes Risiko)[65], und in Bezug auf die mögliche Harmonisierung des Mindestalters von Kindern für die Einwilligung im Zusammenhang mit Diensten der Informationsgesellschaft.

Volle Ausschöpfung des Potenzials des neuen Verwaltungssystems

Der Ausschuss und die Datenschutzbehörden werden ersucht,

- effiziente Vereinbarungen zwischen den Datenschutzbehörden über das Funktionieren der Verfahren für Zusammenarbeit und Kohärenz zu erarbeiten, unter anderem in Bezug auf verfahrenstechnische Aspekte; dabei sollte auf das Fachwissen der Mitglieder des Ausschusses zurückgegriffen und dessen Sekretariat stärker beteiligt werden;
- die Harmonisierung bei der Anwendung und Durchsetzung der DSGVO unter Nutzung aller ihr zur Verfügung stehenden Mittel zu unterstützen, unter anderem durch eine weitere Klarstellung der Schlüsselkonzepte der DSGVO und durch die Gewährleistung, dass die nationalen Leitlinien in vollem Einklang mit den vom Ausschuss angenommenen Leitlinien stehen;

[65] Artikel 30 Absatz 5 DSGVO.

- die Nutzung aller in der DSGVO vorgesehenen Instrumente zu fördern, um deren einheitliche Anwendung zu gewährleisten;
- die Zusammenarbeit zwischen den Datenschutzbehörden zu verstärken, z. B. durch die Durchführung gemeinsamer Untersuchungen.

Die Kommission wird

- die wirksame und vollständige Unabhängigkeit der nationalen Datenschutzbehörden weiterhin genau überwachen;
- die Zusammenarbeit zwischen den Regulierungsbehörden fördern (insbesondere in den Bereichen Wettbewerb, elektronische Kommunikation, Sicherheit von Netz- und Informationssystemen und Verbraucherpolitik);
- die Überlegungen im Ausschuss zu den Verfahren, die von den nationalen Datenschutzbehörden angewandt werden, um die Zusammenarbeit bei grenzüberschreitenden Fällen zu verbessern, unterstützen.

Die Mitgliedstaaten

- weisen den Datenschutzbehörden ausreichende Ressourcen zu, damit sie ihre Aufgaben erfüllen können.

Unterstützung der Interessenträger

Der Ausschuss und die Datenschutzbehörden werden ersucht,

- weitere Leitlinien zu verabschieden, die praktisch und leicht verständlich sind, klare Antworten liefern und Unklarheiten bei Fragen im Zusammenhang mit der Anwendung der DSGVO vermeiden, beispielsweise in Bezug auf die Verarbeitung von Daten von Kindern und die Rechte betroffener Personen, einschließlich der Ausübung des Rechts auf Auskunft und des Rechts auf Löschung, und bei diesem Prozess die Interessenträger zu konsultieren;
- die Leitlinien zu überarbeiten, wenn aufgrund von Erfahrungen und Entwicklungen, unter anderem in der Rechtsprechung des Gerichtshofs, weitere Klarstellungen erforderlich sind;
- praktische Instrumente wie einheitliche Formulare für Datenschutzverletzungen und vereinfachte Verzeichnisse von Verarbeitungstätigkeiten zu entwickeln, um KMU mit geringem Risiko bei der Erfüllung ihrer Verpflichtungen zu unterstützen.

Die Kommission wird

- Standardvertragsklauseln für internationale Datenübermittlungen und das Verhältnis zwischen dem Auftragsverarbeiter und dem Verantwortlichen bereitstellen;
- Instrumente zur Klärung/Unterstützung der Anwendung der Datenschutzvorschriften auf Kinder bereitstellen;[66]

[66] Projekt der Kommission zu Altersermittlungsinstrumenten – Pilotprojekt zur Demonstration einer interoperablen technischen Infrastruktur für den Schutz von Kindern, einschließlich Altersüberprüfung

- im Einklang mit der Datenstrategie praktische Möglichkeiten sondieren, die verstärkte Nutzung des Rechts auf Datenübertragbarkeit durch Einzelpersonen zu erleichtern, indem ihnen beispielsweise mehr Kontrolle darüber gegeben wird, wer auf maschinengenerierte Daten zugreifen und diese nutzen kann;
- die Standardisierung/Zertifizierung, insbesondere in Bezug auf Aspekte der Cybersicherheit, durch die Zusammenarbeit zwischen der Agentur der Europäischen Union für Cybersicherheit (ENISA), den Datenschutzbehörden und dem Ausschuss unterstützen;
- gegebenenfalls von ihrem Recht Gebrauch machen, den Ausschuss um die Ausarbeitung von Leitlinien und Stellungnahmen zu spezifischen Themen zu ersuchen, die für die Interessenträger wichtig sind;
- unter uneingeschränkter Achtung der Rolle des Ausschusses erforderlichenfalls Orientierungshilfe bieten;
- die Tätigkeiten der Datenschutzbehörden, welche die Umsetzung der DSGVO durch KMU erleichtern, durch finanzielle Unterstützung fördern, insbesondere für praktische Orientierungshilfen und digitale Instrumente, die in anderen Mitgliedstaaten reproduziert werden können.

Förderung von Innovation

Die Kommission wird

- die Anwendung der DSGVO auf neue Technologien überwachen, auch unter Berücksichtigung möglicher künftiger Initiativen im Bereich der künstlichen Intelligenz und im Rahmen der Datenstrategie;
- unter anderem durch finanzielle Unterstützung die Ausarbeitung von EU-Verhaltenskodizes im Bereich Gesundheit und Forschung fördern;
- die Entwicklung und Verwendung von Apps im Zusammenhang mit der COVID-19-Pandemie aufmerksam verfolgen.

Der Ausschuss wird ersucht,

- Leitlinien für die Anwendung der DSGVO in den Bereichen wissenschaftliche Forschung, künstliche Intelligenz, Blockchain und etwaige andere technologische Entwicklungen herauszugeben;
- die Leitlinien zu überarbeiten, wenn aufgrund technologischer Entwicklungen weitere Klarstellungen erforderlich sind.

Weiterentwicklung des Instrumentariums für Datenübermittlungen

Die Kommission wird

---

und Zustimmung der Eltern. Damit soll die Umsetzung der Mechanismen zum Schutz von Kindern auf der Grundlage bestehender EU-Rechtsvorschriften unterstützt werden, die für den Schutz von Kindern im Internet relevant sind.

- entsprechend der in ihrer Mitteilung „Austausch und Schutz personenbezogener Daten in einer globalisierten Welt“ von 2017 dargelegten Strategie Angemessenheitsdialoge mit interessierten Drittländern führen, in denen nach Möglichkeit auch auf Datenübermittlungen an Strafverfolgungsbehörden (gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung) und andere Behörden eingegangen wird; dazu gehört auch, dass das Angemessenheitsverfahren mit der Republik Korea so bald wie möglich abgeschlossen wird;
- die laufende Bewertung der bestehenden Angemessenheitsbeschlüsse abschließen und dem Europäischen Parlament und dem Rat Bericht erstatten;
- die Arbeiten zur Modernisierung der Standardvertragsklauseln abschließen, um sie im Lichte der DSGVO zu aktualisieren, alle relevanten Übermittlungsszenarien abzudecken und moderne Geschäftspraktiken besser widerzuspiegeln.

Der Ausschuss wird ersucht,

- das Zusammenspiel zwischen den Vorschriften für internationale Datenübermittlungen (Kapitel V) und dem räumlichen Anwendungsbereich der DSGVO (Artikel 3) weiter zu verdeutlichen;
- eine wirksame Durchsetzung gegenüber in Drittländern niedergelassenen Wirtschaftsteilnehmern, die in den räumlichen Anwendungsbereich der DSGVO fallen, zu gewährleisten, gegebenenfalls auch in Bezug auf die Benennung eines Vertreters (Artikel 27);
- die Bewertung und letztendliche Genehmigung verbindlicher interner Vorschriften zu straffen, um den Prozess zu beschleunigen;
- die Arbeiten an der Architektur, den Verfahren und den Bewertungskriterien für Verhaltenskodizes und Zertifizierungsverfahren als Instrumente für die Datenübermittlung abzuschließen.

Förderung der Angleichung und Entwicklung der internationalen Zusammenarbeit

Die Kommission wird

- laufende Reformprozesse in Drittländern zu neuen oder modernisierten Datenschutzvorschriften durch den Austausch von Erfahrungen und bewährten Verfahren unterstützen;
- mit afrikanischen Partnern zusammenarbeiten, um die Angleichung der Rechtsvorschriften zu fördern und den Kapazitätenaufbau von Aufsichtsbehörden als Teil des digitalen Kapitels der neuen Partnerschaft zwischen der EU und Afrika zu unterstützen;
- prüfen, wie die Zusammenarbeit zwischen privaten Akteuren und Strafverfolgungsbehörden erleichtert werden könnte, unter anderem durch Verhandlungen über bilaterale und multilaterale Rahmen für Datenübermittlungen im Zusammenhang mit dem Zugang ausländischer Strafverfolgungsbehörden zu elektronischen Beweismitteln, um Rechtskollisionen zu vermeiden und gleichzeitig angemessene Datenschutzgarantien zu gewährleisten;

- mit internationalen und regionalen Organisationen wie der OECD, dem ASEAN oder der G20 zusammenarbeiten, um auf hohen Datenschutzstandards basierenden, vertrauenswürdigen Datenverkehr zu fördern, auch im Rahmen des Ansatzes des „vertrauensvollen, freien Datenverkehrs“;
- eine „Datenschutzakademie“ einrichten, um den Austausch zwischen europäischen und internationalen Regulierungsbehörden zu erleichtern und zu unterstützen;
- die internationale Zusammenarbeit zwischen den Aufsichtsbehörden bei der Durchsetzung unterstützen, unter anderem durch Aushandlung von Kooperations- und Amtshilfeabkommen.