EUROPÄISCHE
KOMMISSION

Brüssel, den 24.7.2019
COM(2019) 374 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Datenschutzvorschriften als Voraussetzung für Vertrauen in die EU und darüber hinaus – eine Bilanz

Mitteilung der Kommission an das Europäische Parlament und den Rat

Datenschutzvorschriften als Voraussetzung für Vertrauen in der EU und darüber hinaus – eine Bilanz

I. Einleitung

Die Datenschutz-Grundverordnung[1] (im Folgenden „Verordnung“) gilt seit nunmehr über einem Jahr in der gesamten Europäischen Union. Sie bildet das Kernstück einer einheitlichen und modernisierten EU-Datenschutzlandschaft, zu der auch die Richtlinie zum Datenschutz bei der Strafverfolgung[2] sowie die Verordnung über den Datenschutz in den Organen und Einrichtungen der Union[3] gehören. Die derzeit im Gesetzgebungsverfahren befindliche e-Datenschutz-Verordnung soll diesen Rahmen künftig ergänzen.

Wirksame Datenschutzvorschriften sind für die Wahrung des Grundrechts auf Schutz personenbezogener Daten von wesentlicher Bedeutung. Sie spielen in einer demokratischen Gesellschaft eine zentrale Rolle[4] und sind ein wichtiger Bestandteil einer zunehmend datengestützten Wirtschaft. Die EU will die zahlreichen Chancen des digitalen Wandels im Hinblick auf Dienstleistungen, Arbeitsplätze und Innovation nutzen und gleichzeitig die damit verbundenen Herausforderungen in Angriff nehmen. Identitätsdiebstahl, das Durchsickern sensibler Daten, die Diskriminierung des Einzelnen, eingebaute Vorurteile, die Weitergabe illegaler Inhalte und die Entwicklung intrusiver Überwachungsverfahren sind nur einige Beispiele für Themen, die im öffentlichen Diskurs immer häufiger zutage treten. Dass die Bürgerinnen und Bürger erwarten, dass ihre Daten geschützt werden, ist dabei deutlich zu spüren.

Datenschutz ist inzwischen ein weltweites Phänomen: Immer mehr Menschen schätzen den Schutz und die Sicherheit ihrer Daten. Zahlreiche Länder haben in Anlehnung an die

---

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): https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679.

2 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): https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:32016L0680. Die Mitgliedstaaten mussten die Richtlinie bis zum 6. Mai 2018 umsetzen. Der Stand ihrer Umsetzung wird in den Berichten zur Sicherheitsunion festgehalten.

3 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39): https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32018R1725. Sie gilt seit dem 11. Dezember 2018.

4 Das Grundrecht auf Privatsphäre, ein „wesentlicher Aspekt der Würde des Menschen“, wurde vom Obersten Gericht Indiens am 24. August 2017 in einer Grundsatzentscheidung anerkannt.

Grundsätze der Verordnung bereits umfassende Datenschutzvorschriften erlassen oder sind dabei, das zu tun. Dadurch gleichen sich die Datenschutzvorschriften weltweit immer weiter an. Daraus ergeben sich neue Möglichkeiten für die Vereinfachung des Datenverkehrs zwischen gewerblichen Akteuren oder Behörden, gleichzeitig jedoch verbessert sich dadurch das Schutzniveau für personenbezogene Daten in der EU und rund um den Globus.

Nie zuvor wurde Datenschutz so ernst genommen wie heute. Seine Wirkung auf verschiedene Interessengruppen und Wirtschaftszweige ist bedeutend. Die Kommission ist entschlossen, die EU zu einer erfolgreichen Umsetzung der neuen Datenschutzregelung zu führen und alle Schritte, die für ihre uneingeschränkte Anwendung notwendig sind, zu unterstützen. Mit der vorliegenden Mitteilung zieht die Kommission die Bilanz der bislang erreichten Ergebnisse, und zwar in Bezug auf die einheitliche Umsetzung der Datenschutzvorschriften in der EU, die Funktionsfähigkeit des neuen Verwaltungssystems, die Auswirkungen für die Bürgerinnen und Bürger und Unternehmen sowie die Anstrengungen der EU in Verbindung mit der weltweiten Angleichung der Datenschutzregelungen. Diese Mitteilung knüpft an die Mitteilung der Kommission vom Januar 2018 zur Anwendbarkeit der Verordnung[5] an und beruht inhaltlich auf den Ausführungen der Multi-Stakeholder-Gruppe[6], insbesondere deren Beitrag zur Ein-Jahres-Bilanz, sowie auf den Diskussionen, die am 13. Juni 2019[7] im Rahmen der von der Kommission organisierten Bestandsaufnahme geführt wurden. Darüber hinaus versteht sich die Mitteilung als ein Beitrag zur Überprüfung, die die Kommission bis Mai 2020 durchführen will[8].

Der EU-Datenschutzrahmen ist ein Grundpfeiler des europäischen Innovationsansatzes, der den Menschen in den Mittelpunkt stellt. Er entwickelt sich immer mehr zu einem festen Bestandteil des Regelwerks für ein wachsendes Spektrum von Politikbereichen, darunter Gesundheit und Forschung, künstliche Intelligenz, Verkehr, Energie, Wettbewerb und Strafverfolgung. Die Kommission hat – beispielsweise in ihrer Mitteilung zur Anwendbarkeit der Verordnung vom Januar 2018 sowie in ihrem Leitfaden zur Verwendung personenbezogener Daten im Zusammenhang mit Wahlen vom September 2018[9] – immer wieder hervorgehoben, wie wichtig es ist, dass die neuen Datenschutzvorschriften ordnungsgemäß um- und durchgesetzt werden. Zwar konnten bis dato bereits erhebliche Fortschritte beim Erreichen dieses Ziels verzeichnet werden, doch die uneingeschränkte Anwendung der Verordnung erfordert weitere Anstrengungen.

---

5 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) 43 final): https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

6 Die von der Kommission eingesetzte Multi-Stakeholder-Gruppe zur Verordnung besteht aus Vertreterinnen und Vertretern aus Zivilgesellschaft, Wirtschaft, Wissenschaft und Praxis: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

7 http://europa.eu/rapid/press-release_IP-19-2956_de.htm.

8 Artikel 97 der Verordnung.

9 Leitfaden der Kommission zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen (COM(2018) 638 final): https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018DC0638&qid=1568184697484&from=DE.

II. Ein Kontinent, ein Recht: der Datenschutzrahmen gilt in allen Mitgliedstaaten

Ein Kernziel der Verordnung war es, die fragmentierte Landschaft aus 28 unterschiedlichen nationalen Regelungen, die unter der alten Datenschutzrichtlinie[10] galten, hinter sich zu lassen und für Einzelpersonen und Unternehmen EU-weit für Rechtssicherheit zu sorgen. Dieses Ziel wurde weitgehend erreicht.

Harmonisierung des Rechtsrahmens

Obwohl die Verordnung unmittelbar in allen Mitgliedstaaten gilt, verpflichtete sie diese zum Erlass einiger rechtlicher Maßnahmen auf nationaler Ebene. Hier seien insbesondere die Einrichtung nationaler Datenschutzbehörden und die Zuweisung von Befugnissen an diese[11], die Festlegung von Vorschriften zu spezifischen Themen wie der Vereinbarkeit des Schutzes personenbezogener Daten mit der Meinungs- und Informationsfreiheit sowie die Änderung oder Aufhebung sektorspezifischer Vorschriften mit datenschutzrelevanten Inhalten genannt. Bis zur Veröffentlichung dieser Mitteilung hatten alle Mitgliedstaaten bis auf drei[12] ihr allgemeines nationales Datenschutzrecht aktualisiert. Die Anpassung sektorspezifischer Vorschriften auf mitgliedstaatlicher Ebene ist noch im Gange. Im Zuge ihrer Aufnahme in das Abkommen über den Europäischen Wirtschaftsraum wurde die Geltung der Verordnung auf Norwegen, Island und Liechtenstein ausgeweitet, welche ebenfalls nationale Datenschutzvorschriften erließen.

Die betroffenen Interessengruppen fordern für bestimmte Bereiche allerdings einen noch höheren Harmonisierungsgrad.[13] Die Verordnung lässt den Mitgliedstaaten einen gewissen Spielraum für die nähere Präzisierung ihrer Anwendung in bestimmten Bereichen, etwa beim Mindestalter von Kindern für die Einwilligung bei Online-Diensten[14] oder bei der Verarbeitung personenbezogener Daten in Bereichen wie der Medizin oder der öffentlichen Gesundheit. Die Mitgliedstaaten müssen sich in diesem Fall an diese beiden Kriterien halten:

i) nationale präzisierende Vorschriften müssen den Anforderungen der Charta der Grundrechte[15] entsprechen (und dürfen die Grenzen der Verordnung, welche auf der Charta aufbaut, nicht überschreiten);
ii) sie dürfen den freien Verkehr personenbezogener Daten in der EU[16] nicht beeinträchtigen.

---

10 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: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:31995L0046.

11 Etwa die Befugnis, Bußgelder zu verhängen.

12 Griechenland, Portugal und Slowenien sind noch dabei, ihre nationalen Vorschriften zu erlassen (Stand: 23. Juli 2019).

13 Siehe Bericht der Multi-Stakeholder-Gruppe zur Verordnung vom 13. Juni 2019: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

14 13 Jahre in Belgien, Dänemark, Estland, Finnland, Lettland, Malta, Schweden und im Vereinigten Königreich; 14 Jahre in Bulgarien, Italien, Litauen, Österreich, Spanien und Zypern; 15 Jahre in Frankreich und Tschechien; 16 Jahre in Deutschland, Irland, Kroatien, Luxemburg, den Niederlanden, Polen, Rumänien, der Slowakei und Ungarn.

15 Artikel 8.

Teilweise haben die Mitgliedstaaten zusätzlich zur Verordnung Anforderungen auf nationaler Ebene festgelegt, und zwar insbesondere durch zahlreiche sektorspezifische Vorschriften, was zu einer Fragmentierung und zu unnötigen Belastungen führt. Ein Beispiel für eine Anforderung, die von den Mitgliedstaaten zusätzlich zur Verordnung festgelegt wurde, ist die Verpflichtung nach deutschem Recht, für Unternehmen mit mindestens 20 Mitarbeitern oder solche, die dauerhaft personenbezogene Daten automatisiert verarbeiten, einen Datenschutzbeauftragten zu bestellen.

Weitere Anstrengungen für eine stärkere Harmonisierung

Die Kommission führt bilaterale Gespräche mit nationalen Behörden, wobei sie in Bezug auf einzelstaatliche Vorschriften insbesondere auf folgende Punkte achtet:

- die wirksame Unabhängigkeit von Datenschutzbehörden, u. a. im Sinne ihrer angemessenen finanziellen, personellen und technischen Ausstattung;
- das Ausmaß, in dem einzelstaatliche Vorschriften die Rechte betroffener Personen einschränken;
- die Tatsache, dass einzelstaatliche Vorschriften keine über die Verordnung hinausgehende Anforderungen wie etwa Zusatzbedingungen für die Verarbeitung festlegen sollten, wenn es keinen Spielraum für Präzisierungen gibt;
- die Erfüllung der Pflicht, das Recht auf Schutz personenbezogener Daten mit der Meinungs- und Informationsfreiheit in Einklang zu bringen, und zwar mit der Maßgabe, dass diese Pflicht nicht dazu missbraucht werden darf, journalistische Tätigkeiten zu beeinträchtigen.

Die Tätigkeit der Datenschutzbehörden, die im Europäischen Datenschutzausschuss (im Folgenden „Ausschuss“) zusammenarbeiten, ist eine wesentliche Triebkraft für die einheitliche Anwendung der neuen Vorschriften: Durchsetzungsmaßnahmen, die mehrere Mitgliedstaaten betreffen, müssen das Kooperations- und Kohärenzverfahren[17] im Ausschuss durchlaufen, und die vom Ausschuss verabschiedeten Leitlinien tragen zu einem harmonisierten Verständnis der Verordnung bei. Dennoch erwarten die betroffenen Interessengruppen, dass die Datenschutzbehörden weitere Schritte in diese Richtung unternehmen.

Einen weiteren Beitrag zur einheitlichen Auslegung der Datenschutzvorschriften leisten nationale Gerichte und der Gerichtshof der Europäischen Union. So erklärten nationale Gerichte von der Verordnung abweichende einzelstaatliche Bestimmungen unlängst für ungültig.[18]

---

[16] Im Einklang mit Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union.

[17] Im Rahmen ihrer Zusammenarbeit müssen sich die Datenschutzbehörden laut Artikel 60 der Verordnung in konkreten Fällen auf eine bestimmte Auslegung der Verordnung einigen. Artikel 64 sieht vor, dass der Ausschuss in bestimmten Fällen Stellungnahmen abgibt, um die einheitliche Anwendung der Verordnung sicherzustellen. Darüber hinaus ist der Ausschuss bei Uneinigkeit zwischen den Datenschutzbehörden befugt, für diese verbindliche Beschlüsse zu erlassen.

[18] So geschehen in Deutschland und Spanien.

III. Das neue Verwaltungssystem funktioniert

Mit der Verordnung wurde eine neue Verwaltungsstruktur geschaffen, deren Herzstück die unabhängigen nationalen Datenschutzbehörden sind, die einerseits die Verordnung durchsetzen und andererseits als Anlaufstelle für Interessenträger dienen. Während die meisten Datenschutzbehörden im vergangenen Jahr von der höheren Mittelausstattung profitierten, bestehen im Ländervergleich noch erhebliche Unterschiede.[19]

Die Datenschutzbehörden nutzen ihre neuen Befugnisse

Mit der Verordnung wurden die Durchsetzungsbefugnisse der Datenschutzbehörden gestärkt. Entgegen den Bedenken einzelner Interessengruppen, die vor Mai 2018 geäußert wurden, verfolgten die Datenschutzbehörden bei der Ausübung ihrer Durchsetzungsbefugnisse einen ausgewogenen Ansatz. Sie konzentrierten sich auf Dialog anstatt auf Sanktionen, insbesondere in Bezug auf die kleinsten Marktteilnehmer, deren Kerntätigkeit nicht in der Verarbeitung personenbezogener Daten besteht. Gleichzeitig schreckten sie aber auch nicht davor zurück, bei Bedarf von ihren neuen Befugnissen Gebrauch zu machen. So leiteten sie etwa Untersuchungen im Bereich der sozialen Medien ein[20] und verhängten Geldbußen in Höhe von einigen Tausend bis zu mehreren Millionen Euro, je nach Schwere der Verletzungen der Datenschutzvorschriften.

Beispiele von Geldbußen, die von den Datenschutzbehörden verhängt wurden[21]:

- 5000 EUR gegen ein Sportwettcafé in Österreich wegen unrechtmäßiger Videoüberwachung;
- 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;
- 50 Mio. EUR gegen Google in Frankreich wegen der Bedingungen für die Einholung der Einwilligung von Nutzern.

Bei der Durchführung von Untersuchungen ist es von wesentlicher Bedeutung, dass die Datenschutzbehörden einschlägiges Beweismaterial zusammentragen, alle Verfahrensschritte nach nationalem Recht einhalten und in oftmals komplexen Sachlagen für ein faires Verfahren sorgen. Das erfordert nicht nur Zeit, sondern auch einen erheblichen Arbeitsaufwand. Die meisten Untersuchungen, die nach Inkrafttreten der Verordnung eingeleitet wurden, sind deshalb noch in Gange.

---

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

20 Die irische Datenschutzbehörde (DPC) leitete im Zusammenhang mit der Einhaltung der Verordnung durch multinationale Technologieunternehmen beispielsweise 15 Untersuchungen ein. Siehe Seite 49 des Jahresberichts 2018 der irischen Datenschutzbehörde: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

21 Mehrere Beschlüsse über die Verhängung von Geldbußen unterliegen noch einer gerichtlichen Überprüfung.

Der Erfolg der Verordnung sollte allerdings nicht an der Anzahl der verhängten Geldbußen gemessen werden, sondern am Kulturwandel und den Verhaltensänderungen bei den beteiligten Akteuren. In diesem Zusammenhang verfügen die Datenschutzbehörden über andere Instrumente, z. B. das Verhängen vorübergehender oder endgültiger Beschränkungen der Verarbeitung, einschließlich eines Verbots, oder die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland[22].

Manche Datenschutzbehörden haben neue Instrumente wie telefonische Hilfsdienste und Toolkits für Unternehmen ins Leben gerufen, andere haben neuartige Konzepte wie zum Beispiel regulatorische Sandkästen[23] entwickelt, um die Unternehmen bei ihren Konformitätsanstrengungen zu unterstützen. Teilweise sind die beteiligten Akteure – vor allem kleine und mittlere Unternehmen in bestimmten Mitgliedstaaten[24] – allerdings der Meinung, nicht ausreichend Unterstützung und Informationen erhalten zu haben. Um hier Abhilfe zu schaffen, stellt die Kommission den Datenschutzbehörden Zuschüsse zur Verfügung, um auf die betroffenen Interessengruppen, insbesondere Einzelpersonen und kleine und mittlere Unternehmen, zuzugehen.[25]

Der Europäische Datenschutzausschuss ist operativ

Die Datenschutzbehörden haben ihre Bemühungen im Rahmen des Europäischen Datenschutzausschusses[26] vorangetrieben. Dank dieser intensiven Anstrengungen konnte der Ausschuss rund 20 Leitlinien zu wesentlichen Aspekten der Verordnung[27] verabschieden. Die künftigen Arbeitsbereiche des Ausschusses werden entsprechend den Vorgaben der Verordnung in einem 2-Jahres-Programm[28] vorgestellt.

Bei grenzüberschreitenden Fällen verstehen sich die Datenschutzbehörden nicht mehr bloß als nationale Behörden, sondern als Teil eines EU-weiten Verfahrens über alle Ebenen hinweg, von der Untersuchung bis hin zur Entscheidung. Diese enge Zusammenarbeit gehört inzwischen zum Tagesgeschäft der Behörden: Bis Ende Juni 2019 wurden 516 grenzüberschreitende Fälle im Kooperationsverfahren abgewickelt.

---

22 Artikel 58 Absatz 2 Buchstaben f und j.

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/

24 Siehe Bericht der Multi-Stakeholder-Gruppe zur DSGVO: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

25 Im Jahr 2018 wurde neun Datenschutzbehörden für Tätigkeiten in den Jahren 2018 und 2019 die Summe von 2 Mio. EUR zugewiesen: Belgien, Bulgarien, Dänemark, Lettland, Litauen, Niederlande, Slowenien, Ungarn und Island: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
im Jahr 2019 soll 1 Mio. EUR bereitgestellt werden:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

26 Der Ausschuss verfügt über eine eigene Rechtspersönlichkeit und setzt sich aus den jeweiligen Leitern der nationalen Datenschutzaufsichtsbehörden und dem Europäischen Datenschutzbeauftragten zusammen.

27 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_en

Die Kommission bringt sich aktiv in die Arbeit des Ausschusses mit ein[29], um den Wortlaut und den Geist der Verordnung zu betonen und an die allgemeinen Grundsätze des EU-Rechts[30] zu erinnern.

Auf dem Weg zur einer EU-Datenschutzkultur

Das neue Verwaltungssystem muss sein ganzes Potenzial erst noch entfalten. Der Ausschuss muss seine Entscheidungsverfahren unbedingt noch stärker straffen und unter seinen Mitgliedern eine gemeinsame EU-Datenschutzkultur entwickeln. Indem die Datenschutzbehörden die Möglichkeit nutzen, ihre Anstrengungen in Bezug auf länderübergreifende Fragen zu bündeln[31], etwa bei der Durchführung gemeinsamer Untersuchungen und Umsetzung gemeinsamer Durchsetzungsmaßnahmen, können sie zu diesem Ziel beitragen und gleichzeitig die Ressourcenknappheit mildern.

Viele betroffene Akteure möchten die Zusammenarbeit sogar noch vertiefen und wünschen sich einen einheitlichen Ansatz der nationalen Datenschutzbehörden.[32] Darüber hinaus fordern sie mehr Kohärenz bei der von den Datenschutzbehörden ausgehenden Beratung[33] sowie die vollständige Angleichung der nationalen Leitlinien an jene des Ausschusses. Teilweise werden auch Erläuterungen zu wichtigen Begriffen der Verordnung wie beispielsweise dem risikobasierten Ansatz erwartet, wobei vor allem auf die Bedenken kleiner und mittlerer Unternehmen eingegangen werden soll.

In diesem Zusammenhang ist es unbedingt erforderlich, dass die Interessengruppen besser in die Arbeit des Ausschusses eingebunden werden. Deshalb begrüßt die Kommission die systematische öffentliche Konsultation, die der Ausschuss zu den Leitlinien durchführt. Neben der frühzeitig im Reflexionsprozess angesiedelten Organisation themenspezifischer Workshops für die beteiligten Akteure sollte diese Praxis weitergeführt und verstärkt werden, um die Transparenz, Inklusivität und Relevanz der Arbeit des Ausschusses sicherzustellen.

IV. Einzelpersonen nehmen ihre Rechte in Anspruch, Sensibilisierungsmaßnahmen sollten aber fortgesetzt werden

Ein weiteres Ziel der Verordnung war es, die Rechte des Einzelnen zu stärken. Die Verordnung wird von Bürgerrechtsverbänden und Verbraucherorganisation weitgehend als wichtiger Schritt auf dem Weg zu einer gerechten digitalen Gesellschaft betrachtet, die auf gegenseitigem Vertrauen beruht.

---

29 Als Mitglied ohne Stimmrecht.

30 Darüber hinaus trug die Kommission zur reibungslosen Einrichtung des Ausschusses bei und unterstützt durch Bereitstellung ihres Kommunikationssystems dessen Funktionsweise.

31 Artikel 62 der Verordnung.

32 Siehe Bericht der Multi-Stakeholder-Gruppe zur Verordnung: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670. Die Unternehmen sind beispielsweise der Meinung, dass die nationalen Listen der Arten der Verarbeitungsvorgänge, für die laut Artikel 35 der Verordnung eine Datenschutz-Folgenabschätzung erforderlich ist, hätten besser harmonisiert werden können.

33 Auch zwischen den verschiedenen Behörden einzelner Bundesstaaten.

Stärkeres Bewusstsein für Datenschutzrechte

Die EU-Bürgerinnen und -Bürger zeigen ein immer stärkeres Bewusstsein für Datenschutzvorschriften und ihre Rechte: 67 % der Befragten einer Eurobarometer-Umfrage[34] vom Mai 2019 kennen die Verordnung und 57 % wissen, dass es eine nationale Datenschutzbehörde gibt, an die sie sich bei Bedarf einer Auskunft oder bei Beschwerden richten können. 73 % haben zumindest von einem der Rechte gehört, die mit der Verordnung eingeräumt wurden. Gleichwohl unternehmen viele Einzelpersonen in der EU immer noch keine aktiven Schritte, um ihre personenbezogenen Daten online zu schützen. 44 % der Bürgerinnen und Bürger haben ihre Standarddatenschutzeinstellungen für die Nutzung sozialer Netzwerke zum Beispiel noch nicht geändert.

Einzelpersonen nehmen ihre Rechte stärker in Anspruch

Dank ihres verstärkten Rechtebewusstseins nehmen die Bürgerinnen und Bürger ihre Rechte vermehrt in Anspruch, und zwar durch Kundenanfragen oder indem sie sich häufiger an Datenschutzbehörden wenden, um sich zu informieren oder Beschwerden einzulegen[35]. Darüber hinaus berichten Unternehmen, dass die Anträge auf Auskunft über personenbezogene Daten in mehreren Branchen einschließlich des Banken- und Telekommunikationssektors zugenommen haben. Außerdem sind Einzelpersonen auch öfter dazu übergegangen, ihre Einwilligung zu widerrufen und von ihrem Recht Gebrauch zu machen, Widerspruch gegen gewerbliche Mitteilungen einzulegen.[36]

Andererseits kam es den Berichten einiger Marktteilnehmer zufolge seitens der Bürgerinnen und Bürger auch zu Missverständnissen hinsichtlich der Datenschutzvorschriften – beispielsweise zu der Annahme, dass die betreffenden Personen in jegliche Art von Verarbeitung einwilligen müssten oder dass das Recht auf Löschung uneingeschränkt gelte (während die Betreiber in manchen Fällen dazu verpflichtet sind, die personenbezogenen Daten zu speichern)[37]. Die Organisationen der Zivilgesellschaft beschweren sich ihrerseits über die langen Rücklaufzeiten einiger Unternehmen und Datenschutzbehörden.

Wichtig ist auch, dass mehrere Nichtregierungsorganisationen im Auftrag betroffener Personen Verbandsklagen erhoben haben und damit von dieser neuen Möglichkeit im Rahmen der Verordnung[38] Gebrauch gemacht haben. Die Nutzung von Verbandsklagen wäre allerdings einfacher gewesen, wenn mehr Mitgliedstaaten die in der Verordnung vorgesehene Möglichkeit in Anspruch genommen hätten, es Nichtregierungsorganisationen zu erlauben, auch ohne entsprechenden Auftrag zu klagen[39].

---

34 http://europa.eu/rapid/press-release_IP-19-2956_de.htm
35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf
36 Siehe Bericht der Multi-Stakeholder-Gruppe zur Datenschutz-Grundverordnung.
37 Siehe Bericht der Multi-Stakeholder-Gruppe zur Datenschutz-Grundverordnung.
38 Artikel 80 Absatz 1 der Verordnung.
39 Artikel 80 Absatz 2 der Verordnung.

Notwendigkeit der weiteren Bewusstseinsschärfung

Der Dialog und die Anstrengungen zur Schärfung des Bewusstseins der breiten Öffentlichkeit müssen deshalb sowohl auf EU- als auch auf nationaler Ebene weitergehen. In diesem Sinne startete die Kommission im Juli 2019 eine neue Online-Kampagne[40], um die Bürgerinnen und Bürger dazu zu bewegen, Datenschutzerklärungen durchzulesen und ihre Datenschutzeinstellungen zu optimieren.

V. Unternehmen passen ihre Praxis an

Ziel der Verordnung ist es, die Unternehmen in der digitalen Wirtschaft durch zukunftsfähige Lösungen zu unterstützen. Grundsätzlich begrüßen die Unternehmen den in der Verordnung verankerten Grundsatz der Rechenschaftspflicht, mit dem der bisherige aufwendige Ex-ante-Ansatz überwunden wird (Beseitigung von Meldevorschriften, Skalierbarkeit von Pflichten sowie Flexibilität beim Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zur Ermöglichung eines Wettbewerbs auf der Grundlage datenschutzfreundlicher Lösungen). Gleichzeitig fordern einige Akteure mehr Rechtssicherheit und zusätzliche bzw. klarere Leitlinien seitens der Datenschutzbehörden[41].

Solide Datenverwaltung

Die Unternehmen berichten zwar durchaus von Herausforderungen bei der Anpassung an die neuen Vorschriften[42], doch viele betonen, dass die Verordnung auch eine Chance darstellte, die Unternehmensspitzen auf das Thema Datenschutz aufmerksam zu machen, die Unternehmen in Bezug auf ihre gespeicherten Daten „aufzuräumen“, die Sicherheit zu verbessern, sich besser gegen Datenvorfälle zu wappnen, unnötige Risiken zu umgehen und eine vertrauensvollere Beziehung zu Kunden und Geschäftspartnern aufzubauen. Bezüglich der Transparenz weisen die Unternehmen und Organisationen der Zivilgesellschaft auf den schwierigen Balanceakt hin, den es zu meistern gilt, wenn es darum geht, den betroffenen Personen einerseits alle laut der Verordnung vorgesehenen Informationen zu erteilen und andererseits eine klare und leicht verständliche Sprache sowie eine Form zu wählen, die von den Bürgerinnen und Bürgern verstanden wird. Die Entwicklung innovativer Lösungen in diese Richtung hat bereits begonnen.

Im Großen und Ganzen berichteten die Unternehmen, dass es ihnen gelungen ist, die neuen Rechte betroffener Personen umzusetzen, obwohl es aufgrund der höheren Anzahl und der

---

40 Die Initiative knüpft an frühere Kampagnen zur Verbreitung von Informationsmaterial unter Einzelpersonen und Unternehmen an und ist verfügbar unter: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de.

41 Siehe Bericht der Multi-Stakeholder-Gruppe zur Verordnung.

42 Die Aktualisierung des IT-Systems wird oft als eine der größten Herausforderungen genannt, insbesondere was die Umsetzung der Grundsätze des Datenschutzes durch Technikgestaltung und des Datenschutzes durch datenschutzfreundliche Voreinstellungen, das Recht auf Löschung aus Sicherheitskopien etc. betrifft.

größeren Bandbreite der Anfragen[43] teilweise schwierig war, die Fristen einzuhalten oder die Identität des Antragstellers zu überprüfen.

Auswirkungen auf die Innovation

Die Entwicklung neuer Technologien wird von der Verordnung nicht nur erlaubt, sondern sogar gefördert, wobei das Grundrecht auf Schutz personenbezogener Daten stets gewahrt werden muss. Dies trifft auch auf Bereiche wie die künstliche Intelligenz zu.

Viele Unternehmen arbeiten bereits an neuen, datenschutzfreundlicheren Dienstleistungen. In manchen Mitgliedstaaten gewinnen Suchmaschinen, die keine Nutzernachverfolgung oder verhaltensorientierte Werbung einsetzen, zunehmend an Marktanteilen. Andere Unternehmen entwickeln Dienstleistungen, die auf den neuen Rechten der Einzelpersonen wie beispielsweise der Übertragbarkeit ihrer personenbezogenen Daten aufbauen. Immer mehr Unternehmen nutzen den Schutz personenbezogener Daten als ein Alleinstellungsmerkmal und Verkaufsargument. Diese Entwicklungen beschränken sich nicht nur auf die EU, sondern betreffen auch hochinnovative ausländische Volkswirtschaften.[44]

Der Sonderfall „risikoarmer" Kleinst- und Kleinunternehmen

Auch wenn die Situation je nach Mitgliedstaat variiert, gehörten Kleinst- und Kleinunternehmen[45], deren Kerntätigkeit nicht in der Verarbeitung personenbezogener Daten besteht, zu den Akteuren mit den meisten Fragen rund um die Anwendung der Verordnung. Obwohl die Fragen teils auf fehlende Kenntnisse der Datenschutzvorschriften zurückgehen, werden die Unklarheiten teilweise auch durch die Kampagnen von Beratungsfirmen, die kostenpflichtige Beratungen verkaufen wollen, durch die Verbreitung falscher Informationen, zum Beispiel über die Notwendigkeit, die Einwilligung betroffener Personen systematisch einzuholen[46], oder aber durch zusätzliche Vorgaben auf nationaler Ebene verschärft.

In diesem Zusammenhang fordern Kleinst- und Kleinunternehmen Leitlinien, die an ihre konkrete Situation angepasst sind und sehr praxisbezogene Informationen enthalten. Einige Datenschutzbehörden haben dies auf nationaler Ebene bereits umgesetzt.[47] Zur Ergänzung einzelstaatlicher Initiativen hat die Kommission entsprechendes Informationsmaterial veröffentlicht, um den Unternehmen anhand einer Reihe von praktischen Schritten dabei zu helfen, die neuen Vorschriften einzuhalten[48].

---

43 Die Unternehmen fordern vom Ausschuss unter anderem Leitlinien zu unbegründeten und übermäßigen Anfragen.

44 Gemäß einem Bericht des israelischen Industrieverbands für Cybersicherheit war im Jahre 2018 der Teilsektor „Datenschutz und Schutz der Privatsphäre" der am schnellsten wachsende Teilsektor im Bereich der Cybersicherheit, was teilweise auf das Inkrafttreten der DSGVO zurückzuführen sei.

45 Entsprechend der Definition von KMU unter: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_de.

46 Tatsächlich beruht die Verordnung nicht ausschließlich auf Einwilligung, sondern sieht indes mehrere Rechtsgrundlagen für die Verarbeitung personenbezogener Daten vor.

47 Siehe zum Beispiel den Leitfaden der französischen Datenschutzbehörde: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-de-n.pdf.

Ausschöpfung des in der Verordnung vorgesehenen Instrumentariums

Die Verordnung sieht verschiedene Instrumente vor, um die Einhaltung der Vorschriften zu belegen. Dazu gehören zum Beispiel Standardvertragsklauseln, Verhaltensregeln und das neu eingerichtete Zertifizierungsverfahren.

Standardvertragsklauseln sind Musterklauseln, die freiwillig in einen Vertrag – beispielsweise den Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter – aufgenommen werden können und die die Pflichten der Vertragsparteien entsprechend der Verordnung festhalten. Mit der Verordnung wird der mögliche Anwendungsbereich von Standardvertragsklauseln sowohl für internationale Übermittlungen als auch für solche innerhalb der EU erweitert.[49] Was internationale Datenübermittlungen betrifft, zeigt ihre breite Verwendung[50], dass sie für die Konformitätsanstrengungen der Unternehmen überaus hilfreich sind und vor allem für die Unternehmen nützlich sind, die nicht über die nötigen Mittel verfügen, um mit jedem ihrer Datenverarbeitungspartner einen Einzelvertrag abzuschließen.

In einigen Sektoren herrscht außerdem die Meinung, dass Standardvertragsklauseln ein hilfreiches Instrument zur Förderung der Harmonisierung sind, vor allem, wenn sie von der Kommission festgelegt werden. Die Kommission wird mit betroffenen Interessengruppen zusammenarbeiten, um die in der Verordnung vorgesehenen Möglichkeiten zu nutzen und bestehende Klauseln zu aktualisieren.

Die Einhaltung von Verhaltensregeln ist ein weiteres operatives und praktisches Instrument, das von der Wirtschaft dazu verwendet werden kann, die Einhaltung der Verordnung leichter zu belegen.[51] Die Verhaltensregeln sollten dabei von Industrieverbänden oder Einrichtungen erstellt werden, die sowohl Verantwortliche als auch Auftragsverarbeiter vertreten, und sollten beschreiben, wie die Datenschutzvorschriften in einem spezifischen Sektor umgesetzt werden können. Durch die Abstimmung von Pflichten und Risiken[52] können sie für kleine und mittlere Unternehmen außerdem eine hilfreiche und kostenwirksame Methode zur Erfüllung ihrer Pflichten sein.

Schlussendlich kann auch die Zertifizierung ein hilfreiches Instrument sein, um die Einhaltung einzelner Anforderungen der Verordnung nachzuweisen. Sie kann auf der Unternehmensseite zu mehr Rechtssicherheit führen und die Verordnung global stärker in den Fokus rücken. Mit den unlängst vom Europäischen Datenschutzausschuss verabschiedeten

---

49 Siehe Artikel 28 der Verordnung. Von der Kommission festgelegte Standardvertragsklauseln sind EU-weit gültig. Solche, die nach Artikel 28 Absatz 8 von einer Datenschutzbehörde festgelegt wurden, sind hingegen nur für die Behörde bindend, die sie festgelegt hat, und können deshalb nur bei Verarbeitungsvorgängen angewandt werden, die nach den Artikeln 55 und 56 in die Zuständigkeit dieser Behörde fallen.

50 Standardvertragsklauseln sind das von Unternehmen am häufigsten verwendete Instrument für Datenexporte.

51 Am 4. Juni 2019 verabschiedete der Europäische Datenschutzausschuss Leitlinien zu Verhaltensregeln. Sie erläutern die Verfahren und Vorschriften in Zusammenhang mit der Einreichung, Genehmigung und Veröffentlichung von Verhaltensregeln auf nationaler und EU-Ebene.

52 Erwägungsgrund 98 der Verordnung.

Zertifizierungs- und Akkreditierungsleitlinien[53] wird der Weg für Zertifizierungsprogramme innerhalb der EU freigemacht. Die Kommission wird diese Entwicklungen beobachten und bei Bedarf die ihr durch die Verordnung eingeräumten Befugnisse nutzen, um die Anforderungen an die Zertifizierung zu formulieren. Darüber hinaus könnte die Kommission bezüglich bestimmter Elemente, die für die Verordnung von Bedeutung sind, einen Normierungsantrag bei den Normierungsstellen der EU stellen.

VI. Aufwärtskonvergenz schreitet international voran

Die Notwendigkeit, personenbezogene Daten zu schützen, beschränkt sich nicht nur auf die EU. Laut einer aktuellen internationalen Studie zur Sicherheit im Internet nimmt das Vertrauensdefizit weltweit zu, wodurch die Menschen ihr Online-Verhalten verändern.[54] Unternehmen versuchen zunehmend, gegen diese Bedenken vorzugehen, indem sie die mit der Verordnung eingeräumten Rechte aus eigenem Antrieb auf ihre Kunden außerhalb der EU ausweiten.

Vor dem Hintergrund, dass die Länder rund um den Erdball zunehmend ähnlichen Herausforderungen gegenüberstehen, rüsten sie sich mit neuen Datenschutzvorschriften oder modernisieren ihre bestehenden Bestimmungen. Diese Vorschriften weisen oft mehrere Gemeinsamkeiten mit der Datenschutzregelung der EU auf. So beruhen sie anstatt auf sektorspezifischen Vorschriften beispielsweise auf einer übergreifenden Gesetzesstruktur und sehen durchsetzbare Individualrechte sowie eine unabhängige Aufsichtsbehörde vor. Von Südkorea bis Brasilien, von Chile bis nach Thailand, von Indien bis nach Indonesien handelt es sich dabei um einen echten Welttrend. Die zunehmend weltumfassende Mitgliedschaft des „Übereinkommens Nr. 108“[55] des Europarats, welches vor Kurzem mit starkem Mitwirken der Kommission modernisiert wurde[56], ist ein weiteres klares Zeichen für diese Entwicklung der Aufwärtskonvergenz.

---

53 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en;
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_de

54 Siehe die internationale Studie von CIGI-IPSOS zu Sicherheit und Vertrauen im Internet (*Global Survey on Internet Security and Trust*) von 2019. Laut dieser Studie sorgen sich 78 % der Befragten um ihre Privatsphäre im Internet. 49 % gaben an, dass sie aus Misstrauensgründen weniger persönliche Informationen online von sich preisgeben, 43 % gaben an, besser auf die Sicherheit ihres Geräts zu achten, und 39 % antworteten, dass sie bei der Internetnutzung neben anderen Vorkehrungen selektiver vorgingen. Die Untersuchung fand in 25 Ländern statt: Ägypten, Australien, Brasilien, China, Deutschland, Frankreich, Hongkong, Indien, Indonesien, Italien, Japan, Kanada, Kenia, Mexiko, Nigeria, Pakistan, Polen, der Republik Korea, Russland, Südafrika, Schweden, Tunesien, der Türkei, dem Vereinigten Königreich und den Vereinigten Staaten.

55 Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) und Zusatzprotokoll von 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV Nr. 181). Hierbei handelt es sich um das einzige verbindliche multilaterale Instrument im Bereich Datenschutz. Das Übereinkommen wurde zuletzt von Argentinien, Mexiko, Cabo Verde und Marokko ratifiziert.

56 Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108), vereinbart auf der 128. Tagung des

Förderung eines sicheren und freien Datenverkehrs durch Angemessenheitsbeschlüsse und andere Instrumente

Mit der zunehmenden Konvergenz bieten sich neue Chancen zur Vereinfachung des Datenverkehrs und damit auch des Handels und der Zusammenarbeit zwischen Behörden. Gleichzeitig wird das Schutzniveau der Daten betroffener Personen in der EU bei der Übermittlung ihrer Daten ins Ausland erhöht.

Als Teil ihrer Strategie, die sie 2017 in ihrer Mitteilung zum Austausch und Schutz personenbezogener Daten in einer globalisierten Welt[57] darlegte, verstärkte die Kommission ihr Engagement gegenüber Drittländern und anderen internationalen Partnern, indem sie auf bestehende Elemente der Angleichung zwischen den einzelnen Datenschutzsystemen aufbaute und diese weiterentwickelte. So prüfte sie beispielsweise den Erlass von Angemessenheitsbeschlüssen in Gemeinsamkeit mit ausgewählten Drittländern[58]. Diese Bemühungen führten zu wichtigen Ergebnissen, insbesondere zum Inkrafttreten der Regelung zur gegenseitigen Angemessenheitsfeststellung zwischen der EU und Japan im Februar 2019, durch die der weltweit größte Raum für freien und sicheren Datenverkehr geschaffen wurde. Mit Südkorea finden gerade fortgeschrittene Angemessenheitsverhandlungen statt und es laufen bereits Sondierungen zur Aufnahme von Angemessenheitsgesprächen mit mehreren lateinamerikanischen Ländern wie Chile und Brasilien, welche allerdings vom Abschluss laufender Gesetzgebungsverfahren abhängen. Genauso wie in süd- und osteuropäischen Nachbarländern zeigen sich auch in Teilen Asiens – etwa in Indien, Indonesien und Taiwan – vielversprechende Entwicklungen, die den Weg für künftige Angemessenheitsbeschlüsse frei machen könnten.

Gleichzeitig begrüßt die Kommission die Tatsache, dass andere Länder, die dem Angemessenheitsansatz der EU ähnliche Übermittlungsverfahren eingeführt haben, anerkannt haben, dass sowohl die EU selbst als auch die Länder, die von der EU als „angemessen" eingestuft werden, das erforderliche Schutzniveau gewährleisten.[59] Dadurch könnte sich ein Netzwerk von Ländern bilden, innerhalb dessen ein freier Datenverkehr herrscht.

Parallel dazu wird gemeinsam mit anderen Drittländern wie Kanada, Neuseeland, Argentinien und Israel intensiv daran gearbeitet, anhand der Angemessenheitsbeschlüsse, die auf der Grundlage der Datenschutzrichtlinie aus dem Jahr 1995 erlassen wurden, die in der Verordnung vorgesehene Kontinuität zu gewährleisten. Darüber hinaus hat sich der EU-US-Datenschutzschild mit seinen über 4700 teilnehmenden Unternehmen[60] als hilfreiches Instrument zur Sicherung des transatlantischen Datenverkehrs mit hohem Schutzniveau

---

Ministerkomitees vom 17./18. Mai 2018 in Helsingør (Dänemark). Die konsolidierte Fassung des modernisierten Übereinkommens Nr. 108 ist unter folgendem Link abrufbar: https://rm.coe.int/1680078b38.

57 Mitteilung der Kommission an das Europäische Parlament und den Rat – Austausch und Schutz personenbezogener Daten in einer globalisierten Welt (COM(2017) 7 final).

58 Als Teil der Anstrengungen der EU zur Erleichterung des Datenverkehrs mit internationalen Organisationen sieht die Verordnung auch die Möglichkeit von Angemessenheitsfeststellungen mit diesen Einrichtungen vor.

59 Dieser Ansatz wird beispielsweise von Argentinien, Israel, Kolumbien und der Schweiz verfolgt.

60 Damit nahmen in den ersten drei Jahren seines Bestehens mehr Unternehmen am Datenschutzschild teil als an seinem Vorgänger, dem Safe-Harbour-Abkommen, das insgesamt 13 Jahre lang lief.

bewährt. Im Rahmen einer jährlichen Prüfung wird sichergestellt, dass die Funktionsweise der Rahmenvereinbarung regelmäßig überprüft wird und neue Probleme rechtzeitig angegangen werden.

Da es für den Datenverkehr keine Einheitslösung gibt, arbeitet die Kommission auch mit verschiedenen Interessengruppen und dem Ausschuss zusammen, um das Potenzial der in der Verordnung vorgesehenen Verfahren im Hinblick auf grenzüberschreitende Übermittlungen voll auszuschöpfen. Im Einzelnen sind hier Instrumente wie Standardvertragsklauseln, der Aufbau von Zertifizierungsprogrammen, Verhaltensregeln oder Verwaltungsvereinbarungen für öffentliche Einrichtungen gemeint. Die Kommission ist in diesem Zusammenhang am Erfahrungsaustausch und dem Austausch bewährter Verfahren mit anderen Systemen interessiert, die in Verbindung mit einigen dieser Instrumente spezifisches Fachwissen aufgebaut haben. Die Kommission wird in Erwägung ziehen, die ihr mit der Verordnung eingeräumten Befugnisse in Verbindung mit diesen für die Datenübermittlung vorgesehenen Instrumenten und insbesondere die Standardvertragsklauseln in Anspruch zu nehmen.

Neben rein bilateralen Verfahren könnte es sich auch lohnen zu prüfen, ob gleich gesinnte Länder nicht ein multinationales Rahmenwerk in diesem Bereich auf den Weg bringen könnten. Der Datenverkehr spielt heute im Handel, in der Kommunikation und in unseren sozialen Beziehungen nämlich eine zunehmend wichtige Rolle. Mit einem solchen Verfahren könnten die Daten zwischen den einzelnen Vertragsparteien frei verkehren und gleichzeitig wäre auf der Grundlage gemeinsamer Werte und angeglichener Systeme das nötige Schutzniveau geboten. Es könnte dabei zum Beispiel auf dem modernisierten Übereinkommen Nr. 108 aufbauen oder sich an der Initiative des „vertrauensvollen freien Datenverkehrs“ orientieren, welche zu Beginn dieses Jahres in Japan gestartet wurde.

Entwicklung neuer Synergien zwischen Handels- und Datenschutzinstrumenten

Die Kommission setzt sich nicht nur für die internationale Angleichung von Datenschutzstandards, sondern auch für die Bekämpfung des digitalen Protektionismus ein. Sie hat deshalb konkrete Bestimmungen zum Datenverkehr und Datenschutz bei Handelsabkommen ausgearbeitet, die sie bei ihren bilateralen und multilateralen Verhandlungen wie beispielsweise den laufenden Gesprächen mit der WTO zum elektronischen Geschäftsverkehr systematisch vorlegt. Diese horizontalen Bestimmungen schließen rein protektionistische Maßnahmen wie zwingende Anforderungen zur Datenlokalisierung aus, ohne die Regelungsautonomie der Parteien in Bezug auf die Wahrung des Grundrechts auf Datenschutz zu beeinträchtigen.

Die Dialoge zum Datenschutz und die Handelsgespräche müssen zwar getrennt geführt werden, können sich aber ergänzen. Die gegenseitige Angemessenheitsregelung zwischen der EU und Japan ist das beste Beispiel für solche Synergien: Sie ermöglicht eine weitere Vereinfachung des Handelsaustauschs und verstärkt dadurch den Nutzen des Wirtschaftspartnerschaftsabkommens. Diese auf gemeinsamen Werten und hohen Standards beruhende Angleichung, flankiert durch einen wirksamen Durchsetzungsmechanismus, bildet die stärkste Grundlage für den Austausch personenbezogener Daten. Auch unsere

internationalen Partner erkennen dies zunehmend an.[61] Da Unternehmen vermehrt grenzüberschreitend arbeiten und lieber in all 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.

Förderung des Informationsaustauschs zur Verbrechens- und Terrorismusbekämpfung auf der Grundlage geeigneter Garantien

Eine größere Kompatibilität der Datenschutzregelungen kann den dringend benötigten Informationsaustausch zwischen Regulierungs-, Polizei- und Justizbehörden der EU und des Auslands erheblich erleichtern und dadurch zu einer wirksameren und schnelleren Zusammenarbeit bei der Strafverfolgung beitragen.[62] Die Kommission zieht deshalb in Erwägung, gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung Angemessenheitsbeschlüsse zu erlassen, um bei der Verbrechens- und Terrorismusbekämpfung ihre Zusammenarbeit mit wichtigen Partnern zu vertiefen. Darüber hinaus kann das im Februar 2017 in Kraft getretene Rahmenabkommen zwischen der EU und den USA[63] als Vorlage für ähnliche Abkommen mit anderen wichtigen Sicherheitspartnern dienen.

Andere Beispiele, die die Bedeutung hoher Datenschutzstandards als Grundlage für eine stabile Zusammenarbeit bei der Strafverfolgung mit Drittländern belegen, sind die Übermittlung von Fluggastdatensätzen (*Passenger Name Records* – PNR)[64] und der Austausch operativer Informationen zwischen Europol und wichtigen internationalen Partnern. Diesbezüglich finden bereits mit mehreren südlichen Nachbarländern[65] Verhandlungen über internationale Abkommen statt bzw. sollen demnächst beginnen.

---

[61] Wie zum Beispiel der Verweis auf den Ansatz des „vertrauensvollen freien Datenverkehrs“ in der Erklärung von Osaka der Staats- und Regierungschefs der G20 zeigt: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[62] Siehe Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Die Europäische Sicherheitsagenda (COM(2015) 185 final).

[63] Abkommen zwischen der EU und den USA über den Schutz personenbezogener Daten bei ihrer Übermittlung und Verarbeitung zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:22016A1210(01) („Rahmenabkommen“). Das Rahmenabkommen ist das erste bilaterale internationale Abkommen im Bereich der Strafverfolgung, das einen umfassenden Katalog von im Einklang mit dem Besitzstand der Union stehenden Datenschutzrechten und -pflichten enthält. Es ist ein erfolgreiches Beispiel dafür, wie die Zusammenarbeit bei der Strafverfolgung mit wichtigen internationalen Partnern durch Aushandlung eines starken Bündels von Datenschutzgarantien verbessert werden kann.

[64] In der Resolution (SCR) 2396 des Sicherheitsrates der Vereinten Nationen vom 21. Dezember 2017 werden alle Mitgliedstaaten der VN aufgefordert, Kompetenzen aufzubauen, um PNR-Daten unter uneingeschränkter Wahrung der Menschenrechte und Grundfreiheiten zu erfassen, zu verarbeiten und zu analysieren. Siehe auch Mitteilung der Kommission – Die Europäische Sicherheitsagenda (COM(2015) 185 final): https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_de.pdf.

[65] https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en

Darüber hinaus werden starke Datenschutzgarantien ein wesentlicher Bestandteil aller künftigen Vereinbarungen über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln in strafrechtlichen Ermittlungen darstellen, und das sowohl auf bilateraler (EU-US-Übereinkommen) als auch auf multilateraler Ebene (Zweites Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität)[66].

Stärkung der Zusammenarbeit zwischen Datenschutzdurchsetzungsstellen

In Zeiten, in denen Probleme bei der Einhaltung von Datenschutzvorschriften oder Sicherheitsvorfälle unter Umständen in mehreren Hoheitsgebieten gleichzeitig viele Menschen betreffen, können engere Formen der internationalen Zusammenarbeit zwischen Aufsichtsbehörden dazu beitragen, die Rechte des Einzelnen wirksamer zu schützen und ein stabileres Umfeld für Unternehmer zu schaffen. Vor diesem Hintergrund und in enger Abstimmung mit dem Ausschuss wird die Kommission deshalb an Wegen arbeiten, die Zusammenarbeit bei der Durchsetzung sowie die Rechtshilfe zwischen EU- und ausländischen Aufsichtsbehörden zu vereinfachen, auch durch Nutzung der neuen Befugnisse, die ihr diesbezüglich mit der Verordnung eingeräumt wurden[67]. Hierbei sind diverse Formen der Zusammenarbeit denkbar, von der Entwicklung gemeinsamer Auslegungs- und Praxisinstrumente[68] bis hin zum Austausch von Informationen über laufende Ermittlungen.

Schließlich beabsichtigt die Kommission weiter, ihren Dialog mit regionalen Organisationen und Netzwerken wie dem Verband südostasiatischer Nationen (ASEAN), der Afrikanischen Union, dem Forum der asiatisch-pazifischen Datenschutzbehörden (APPA) und dem Iberoamerikanischen Datenschutznetzwerk zu verstärken. Diese spielen bei der Gestaltung gemeinsamer Datenschutzstandards, der Förderung des Austauschs bewährter Verfahren und der verstärkten Zusammenarbeit zwischen den Durchsetzungsstellen eine zunehmend wichtige Rolle. Darüber hinaus wird die Kommission mit der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung sowie mit der asiatisch-pazifischen Wirtschaftsgemeinschaft zusammenarbeiten, um die Angleichung der Datenschutzbestimmungen im Sinne eines höheren Schutzniveaus voranzutreiben.

VII. Datenschutzvorschriften als fester Bestandteil zahlreicher Politikbereiche

Der Schutz personenbezogener Daten wird als fest integrierte Komponente in mehreren Politikbereichen der EU gewährleistet.

Telekommunikation und elektronische Kommunikationsdienste

Im Januar 2017 verabschiedete die Kommission ihren Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation[69]. Ziel des Vorschlags ist die Wahrung der

---

66 http://europa.eu/rapid/press-release_IP-19-2891_de.htm

67 Siehe Artikel 50 der Verordnung über die internationale Zusammenarbeit im Bereich des Datenschutzes. Die Bestimmung umfasst ein großes Spektrum von Formen der Zusammenarbeit, von Informationen über datenschutzrechtliche Vorschriften bis hin zu Beschwerdeverweisungen und Amtshilfe bei Untersuchungen.

68 Wie gemeinsame Muster für die Meldung von Datenschutzverletzungen.

69 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52017PC0010

Vertraulichkeit der Kommunikation entsprechend der Charta der Grundrechte, der Schutz personenbezogener Daten, die möglicherweise Teil eines Kommunikationsvorgangs sind, sowie der Schutz der Endeinrichtungen der Endnutzer.

Die vorgeschlagene e-Datenschutz-Verordnung enthält besondere Vorschriften für die oben genannten Zwecke und versteht sich somit als Präzisierung und Ergänzung der Datenschutz-Grundverordnung. Um neuen technischen wie rechtlichen Entwicklungen Rechnung zu tragen, sollen die bestehenden e-Datenschutz-Vorschriften der EU[70] dadurch modernisiert werden. Darüber hinaus verbessert die vorgeschlagene Verordnung die Privatsphäre des Einzelnen, da „Over-the-top"-Kommunikationsdienstleister ebenfalls von den neuen Vorschriften erfasst werden, wodurch faire Wettbewerbsbedingungen für alle elektronischen Kommunikationsdienste entstehen. Während das Europäische Parlament im Oktober 2017 ein Mandat zur Aufnahme von Trilogen annahm, konnte sich der Rat bislang noch nicht auf einen allgemeinen Ansatz einigen. Die Kommission steht weiterhin mit vollem Einsatz hinter der e-Datenschutz-Verordnung und wird die beiden Gesetzgebungsorgane in ihren Anstrengungen, die vorgeschlagene Verordnung zügig zu verabschieden, unterstützen.

Gesundheit und Forschung

Der erleichterte Austausch von Gesundheitsdaten, die gemäß der Verordnung als sensible Daten gelten, zwischen den Mitgliedstaaten wird aus Gründen des allgemeinen Interesses immer wichtiger für die öffentliche Gesundheit. Hier sind etwa die Gesundheitsversorgung und Behandlung von Patienten sowie der Schutz vor schweren grenzüberschreitenden Gesundheitsgefahren gemeint, aber auch die Gewährleistung hoher Qualitäts- und Sicherheitsstandards in der medizinischen Versorgung, bei Arzneimitteln und Medizinprodukten. Die Verordnung enthält Bestimmungen zur Gewährleistung der rechtmäßigen und vertrauenswürdigen Verarbeitung von Gesundheitsdaten in der EU sowie des entsprechenden EU-weiten Austauschs dieser Daten. Darüber hinaus gelten die Vorschriften für den Zugang von Drittparteien zu medizinischen Patientendaten einschließlich Daten in Patientendossiers, elektronische Verschreibungen und langfristig auch umfassende elektronische Patientenakten und deren Verwendung für wissenschaftliche Zwecke. Speziell für den Bereich der klinischen Prüfungen hat die Kommission zudem konkrete Fragen und Antworten zum Zusammenspiel zwischen der Verordnung über klinische Prüfungen[71] und der Datenschutz-Grundverordnung[72] ausgearbeitet.

Künstliche Intelligenz (KI)

Mit der zunehmenden strategischen Bedeutung künstlicher Intelligenz wächst auch die Notwendigkeit, weltweite Vorschriften für deren Entwicklung und Verwendung festzulegen. Die Kommission fördert die Entwicklung und den Einsatz von KI und hat sich dabei für einen auf den Menschen ausgerichteten Ansatz entschieden. Das bedeutet, dass KI-Anwendungen

---

70 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. 37).

71 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32014R0536

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf

mit den Grundrechten vereinbar sein müssen.[73] Die in der Verordnung festgelegten Vorschriften bieten in diesem Zusammenhang einen allgemeinen Rahmen und beinhalten konkrete Rechte und Pflichten, die vor allem für die Verarbeitung personenbezogener Daten im Bereich der KI relevant sind. So enthält die Verordnung beispielsweise das Recht, außer in bestimmten Situationen keinen Entscheidungen unterworfen zu werden, die ausschließlich automatisiert erfolgen.[74] Darüber hinaus sieht sie spezielle Transparenzanforderungen für automatisierte Entscheidungen vor. So besteht etwa die Pflicht, über das Bestehen solcher Entscheidungen Auskunft zu erteilen und aussagekräftige Informationen und Erklärungen über deren Bedeutung und die voraussichtlichen Folgen der Verarbeitung für den Einzelnen zu bieten.[75] Die zentralen Grundsätze der Verordnung wurden von der hochrangigen Expertengruppe für KI[76], der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung[77] und der G20[78] als besonders relevant für die Herausforderungen und Chancen der KI anerkannt. Der Europäische Datenschutzausschuss hat KI als mögliches Thema für sein Arbeitsprogramm 2019-2020 ausgewiesen.[79]

Verkehr

Die Entwicklung vernetzter Autos und intelligenter Städte hängt mehr und mehr von der Verarbeitung und dem Austausch großer Mengen personenbezogener Daten zwischen verschiedenen Parteien ab, darunter den Autos selbst, den Autoherstellern, den Anbietern von Telematikdiensten und den für die Straßenverkehrsinfrastruktur zuständigen Behörden. Dieses aus mehreren Parteien bestehende Umfeld bringt eine gewisse Komplexität mit sich, und zwar einerseits in Bezug auf die Zuweisung der Rollen und Zuständigkeiten der verschiedenen Akteure, die an der Verarbeitung personenbezogener Dateien beteiligt sind, und andererseits in Bezug auf die Frage, wie die Rechtmäßigkeit der Verarbeitung durch die beteiligten Akteure gewährleistet werden kann. Wenn es darum geht, intelligente und alle Verkehrsträger umfassende Verkehrssysteme aufzubauen sowie digitale Instrumente und Dienstleistungen zu verbreiten, die eine stärkere Mobilität von Menschen und Gütern[80] ermöglichen, ist die

---

[73] Mitteilung der Kommission vom 8. April 2019 über die Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz: https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.
Ethik-Leitlinien für eine vertrauenswürdige KI, vorgestellt von der hochrangigen Expertengruppe am 8. April 2019: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Siehe auch Empfehlung des OECD-Rates zur künstlichen Intelligenz: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, die Grundsätze der G20 zu KI, die als Teil der Erklärung von Osaka der Staats- und Regierungschefs der G20 unterstützt wurden: https://www.g20.org/pdf/documents/en/annex_08.pdf und die G20-Ministererklärung zu Handel und Digitaler Wirtschaft: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

[74] Artikel 22 der Verordnung.

[75] Artikel 13 Absatz 2 Buchstabe f der Verordnung.

[76] https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

[77] Empfehlung des Rates zur künstlichen Intelligenz: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

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

[79] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf

[80] Beispielsweise durch eine vereinfachte Planung und die Nutzung verschiedener Verkehrsmittel auf einer bestimmten Strecke.

Einhaltung der Datenschutz-Grundverordnung sowie der e-Datenschutz-Vorschriften von zentraler Bedeutung.

Energie

Die Entwicklung digitaler Lösungen im Energiesektor hängt immer stärker von der Verarbeitung personenbezogener Daten ab. Die Rechtsvorschriften, die als Teil des Pakets „Saubere Energie für alle Europäer“[81] erlassen wurden, beinhalten neue Bestimmungen, die den Weg zur Digitalisierung der Stromwirtschaft freimachen, sowie Bestimmungen über den Zugang zu Daten, deren Verwaltung und Interoperabilität. Diese ermöglichen es, die Echtzeitdaten von Verbrauchern zu verarbeiten, um Einsparungen zu erzielen und die Verbraucher gleichzeitig dazu zu bewegen, selbst Energie zu generieren und am Energiemarkt teilzunehmen. Die Einhaltung von Datenschutzvorschriften ist für die erfolgreiche Umsetzung dieser Bestimmungen daher von großer Bedeutung.

Wettbewerb

In der Wettbewerbspolitik gewinnt die Verarbeitung personenbezogener Daten zunehmend an Bedeutung[82]. Da die Datenschutzbehörden die einzigen öffentlichen Stellen sind, die Verstöße gegen die Datenschutzvorschriften feststellen dürfen, arbeiten die Wettbewerbs-, Verbraucher- und Datenschutzbehörden in Schnittbereichen ihrer Zuständigkeiten zusammen und werden dies bei Bedarf auch weiterhin tun. Die Kommission wird diese Zusammenarbeit fördern und ihre Entwicklung genau beobachten.

Im Zusammenhang mit Wahlen

In ihrem Leitfaden zur Verwendung personenbezogener Daten im Zusammenhang mit Wahlen[83], der im September 2018 als Teil des Wahlpakets[84] veröffentlicht wurde, wies die Kommission auf Vorschriften hin, die besonders für an Wahlen beteiligte Akteure wichtig sind, einschließlich Fragen in Verbindung mit dem Mikrotargeting von Wählerinnen und Wählern. Der Leitfaden wurde in einer Erklärung des Europäischen Datenschutzausschusses[85] bekräftigt, und mehrere Datenschutzbehörden verabschiedeten entsprechende Leitlinien auf nationaler Ebene. Im Rahmen des Wahlpakets wurden die Mitgliedstaaten zudem dazu aufgefordert, einzelstaatliche Wahlnetzwerke aufzubauen. Daran sollten zum einen staatliche Stellen für Wahlangelegenheiten und zum anderen Behörden teilnehmen, die für die Überwachung und Durchsetzung von Vorschriften, wie beispielsweise Datenschutzbestimmungen, für wahlrelevante Online-Tätigkeiten zuständig sind. Darüber hinaus wurden neue Maßnahmen zur Einführung von Sanktionen für die Verletzung von Datenschutzvorschriften durch europäische politische Parteien und Stiftungen erlassen. Die

---

81 Insbesondere die Stromrichtlinie: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32009L0072.

82 Beispielsweise Wettbewerbssache M.8788 – Apple/Shazam und Wettbewerbssache M.8124 – Microsoft/LinkedIn.

83 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018DC0638&qid=1568184697484&from=DE

84 http://europa.eu/rapid/press-release_IP-18-5681_de.htm

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_de.pdf

Kommission empfahl den Mitgliedstaaten, auf nationaler Ebene ebenso zu verfahren. Bei der für Oktober 2019 erwarteten Bewertung der Europawahlen 2019 werden auch Datenschutzaspekte berücksichtigt.

Strafverfolgung

Der Aufbau einer wirksamen und echten Sicherheitsunion ist nur bei voller Einhaltung der in der EU-Charta verankerten Grundrechte und der sekundären EU-Rechtsvorschriften möglich, zu denen auch geeignete Datenschutzgarantien zum sicheren Austausch personenbezogener Daten für die Strafverfolgung gehören. Jegliche Einschränkung des Grundrechts auf Privatsphäre und Datenschutz unterliegt den Anforderungen der unbedingten Erforderlichkeit und Angemessenheit.

VIII. Schlussfolgerung

Auf der Grundlage der bislang vorliegenden Informationen und des Dialogs mit den beteiligten Akteuren zieht die Kommission insgesamt vorläufig eine positive Bilanz des ersten Anwendungsjahres der Verordnung. Gleichwohl sind entsprechend den Ausführungen in der vorliegenden Mitteilung in einigen Bereichen noch weitere Fortschritte erforderlich.

Umsetzung und Ergänzung des Rechtsrahmens:

- Die drei Mitgliedstaaten, die ihr nationales Datenschutzrecht bislang noch nicht aktualisiert haben, müssen dies dringend nachholen. Die Angleichung der sektorspezifischen Rechtsvorschriften an die Anforderungen der Verordnung sollte von allen Mitgliedstaaten vollzogen werden.

- Die Kommission wird alle ihr zur Verfügung stehenden Instrumente einschließlich Vertragsverletzungsverfahren nutzen, um die Einhaltung der Verordnung durch die Mitgliedstaaten sicherzustellen und eine Fragmentierung des Datenschutzrahmens zu beschränken.

Volle Ausschöpfung des Potenzials des neuen Verwaltungssystems:

- Die Mitgliedstaaten sollten den nationalen Datenschutzbehörden ausreichende personelle, finanzielle und technische Mittel zur Verfügung stellen.

- Die Datenschutzbehörden sollten ihre Zusammenarbeit beispielsweise durch gemeinsame Untersuchungen vertiefen, während die Mitgliedstaaten die Durchführung solcher Untersuchungen ihrerseits erleichtern sollten.

- Der Ausschuss sollte daran arbeiten, die EU-Datenschutzkultur weiter aufzubauen und die in der Verordnung vorgesehenen Instrumente voll auszuschöpfen, um eine harmonisierte Anwendung der Vorschriften sicherzustellen. Er sollte seine Arbeit an der Ausarbeitung von Leitlinien fortführen, vor allem was Leitlinien für kleine und mittlere Unternehmen betrifft.

- Das Fachwissen des Sekretariats des Ausschusses sollte vertieft werden, um die Arbeit des Ausschusses wirksamer unterstützen und leiten zu können.

- Die Kommission wird die Datenschutzbehörden und den Ausschuss weiterhin unterstützen, und zwar vor allem dadurch, dass sie sich aktiv in die Arbeit des Ausschusses einbringt und diesen bei der Umsetzung der Verordnung auf die Anforderungen des Unionsrechts hinweist.

- Die Kommission wird das Zusammenspiel zwischen den Datenschutzbehörden und anderen staatlichen Stellen, insbesondere aus dem Wettbewerbsbereich, unter voller Achtung ihrer jeweiligen Zuständigkeiten unterstützen.

Unterstützung und Einbindung von Interessengruppen:

- Der Ausschuss sollte bessere Wege finden, die verschiedenen Interessengruppen in seine Arbeit einzubinden. Die Kommission wird die Datenschutzbehörden weiterhin finanziell dabei unterstützen, auf die betroffenen Interessengruppen zuzugehen.

- Die Kommission wird ihre Sensibilisierungsmaßnahmen und ihre Arbeit mit den beteiligten Akteuren fortführen.

Förderung der internationalen Angleichung:

- Die Kommission wird ihren Dialog zur Angemessenheit mit geeigneten Schlüsselpartnern verstärken, auch im Bereich der Strafverfolgung. Insbesondere will sie die laufenden Verhandlungen mit Südkorea in den kommenden Monaten abschließen. Ihren Bericht über die Überprüfung der elf Angemessenheitsbeschlüsse, die auf der Grundlage der Datenschutzrichtlinie erlassen wurden, wird die Kommission 2020 vorlegen.
- Die Kommission wird ihre Arbeit mit Ländern, die am Erlass moderner Datenschutzvorschriften interessiert sind, unter anderem durch technische Unterstützung und den Austausch von Informationen und bewährten Verfahren fortsetzen und gleichzeitig die Zusammenarbeit mit Aufsichtsbehörden und regionalen Organisationen in Drittländern fördern.
- Die Kommission wird mit multilateralen und regionalen Organisationen zusammenarbeiten, um für hohe Datenschutzstandards zu werben, die als Grundvoraussetzung für den Handel dienen und die Zusammenarbeit erleichtern sollen (z. B. im Rahmen der Initiative des „vertrauensvollen freien Datenverkehrs“, die im Rahmen der G20 von Japan ins Leben gerufen wurde).

Laut der Verordnung[86] ist die Kommission verpflichtet, 2020 einen Bericht über deren Umsetzung vorzulegen. Damit wird sich eine Chance bieten, die bisherigen Fortschritte zu bewerten und zu prüfen, ob die verschiedenen Komponenten der neuen Datenschutzregelung

[86] Artikel 97 der Verordnung.

zwei Jahre nach deren Inkrafttreten tatsächlich uneingeschränkt angewandt werden. Zu diesem Zweck wird sich die Kommission mit dem Europäischen Parlament, dem Rat, den Mitgliedstaaten, dem Europäischen Datenschutzausschuss, betroffenen Interessengruppen sowie Bürgerinnen und Bürgern austauschen.