EUROPÄISCHE
KOMMISSION

Brüssel, den 15.1.2024
COM(2024) 7 final

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die erste Überprüfung der Wirkungsweise der Angemessenheitsfeststellungen gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG

{SWD(2024) 3 final}

1. DIE ERSTE ÜBERPRÜFUNG – HINTERGRUND UND KONTEXT

Der vorliegende Bericht enthält die Erkenntnisse der Kommission zur ersten Überprüfung der Angemessenheitsfeststellungen, die auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG[1] (Datenschutzrichtlinie) erlassen wurden.

In den einschlägigen Beschlüssen bzw. Entscheidungen bescheinigte die Kommission elf Ländern bzw. Gebieten ein angemessenes Schutzniveau für aus der Europäischen Union (EU)[2] übermittelte personenbezogene Daten: Andorra[3], Argentinien[4], Kanada (in Bezug auf kommerzielle Betreiber)[5], die Färöer Inseln[6], Guernsey[7], die Insel Man[8], Israel[9], Jersey[10], Neuseeland[11], die Schweiz[12] und Uruguay[13]. Auf dieser Grundlage kann die Datenübermittlung aus der EU in diese Länder bzw. Gebiete ohne zusätzliche Anforderungen erfolgen.

[1] 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.

[2] Da die Datenschutz-Grundverordnung (DSGVO) in das Abkommen über den Europäischen Wirtschaftsraum (EWR) übernommen wurde, gilt sie nun auch für Norwegen, Island und Liechtenstein. Die in diesem Bericht enthaltenen Verweise auf die EU schließen die EWR-Staaten mit ein.

[3] Beschluss 2010/625/EU der Kommission vom 19. Oktober 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Andorra (ABl. L 277 vom 21.10.2010, S. 27).

[4] Entscheidung 2003/490/EG der Kommission vom 30. Juni 2003 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Argentinien (ABl. L 168 vom 5.7.2003, S. 19).

[5] Entscheidung 2002/2/EG der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet (ABl. L 2 vom 4.1.2002, S. 13).

[6] Beschluss 2010/146/EU der Kommission vom 5. März 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus, den das färöische Gesetz über die Verarbeitung personenbezogener Daten bietet (ABl. L 58 vom 9.3.2010, S. 17).

[7] Entscheidung 2003/821/EG der Kommission vom 21. November 2003 über die Angemessenheit des Schutzes personenbezogener Daten in Guernsey (ABl. L 308 vom 25.11.2003, S. 27).

[8] Entscheidung 2004/411/EG der Kommission vom 28. April 2004 über die Angemessenheit des Schutzes personenbezogener Daten auf der Insel Man (ABl. L 151 vom 30.4.2004, S. 48).

[9] Beschluss 2011/61/EU der Kommission vom 31. Januar 2011 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus im Staat Israel im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten (ABl. L 27 vom 1.2.2011, S. 39).

[10] Entscheidung 2008/393/EG der Kommission vom 8. Mai 2008 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Argentinien (ABl. L 138 vom 28.5.2008, S. 21).

[11] Durchführungsbeschluss 2013/65/EU der Kommission vom 19. Dezember 2012 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Neuseeland (ABl. L 28 vom 30.1.2013, S. 12).

[12] Entscheidung 2000/518/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz (ABl. L 215 vom 25.8.2000, S. 1).

[13] Durchführungsbeschluss 2012/484/EU der Kommission vom 21. August 2012 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in der Republik Östlich des Uruguay im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten (ABl. L 227 vom 23.8.2012, S. 11).

Die im Rahmen der Datenschutzrichtlinie erlassenen Angemessenheitsfeststellungen sind auch nach Inkrafttreten der Verordnung (EU) 2016/679[14] (DSGVO) am 25. Mai 2018 weiterhin in Kraft.[15] Gleichzeitig wurde in der DSGVO klargestellt, dass Angemessenheitsfeststellungen „lebende Instrumente" sind und die Kommission fortlaufend die Entwicklungen in Drittländern überwachen muss, die die Wirkungsweise der erlassenen Beschlüsse beeinträchtigen könnten[16]. Darüber hinaus muss die Kommission gemäß Artikel 97 der DSGVO diese Feststellungen alle vier Jahre überprüfen und ermitteln, ob Länder und Gebiete, denen ein angemessenes Schutzniveau bescheinigt worden ist, der Angemessenheitsfeststellung weiterhin gerecht werden.

Diese erste Überprüfung der Angemessenheitsfeststellungen im Rahmen des früheren EU-Datenschutzrahmens wurde als Teil einer umfassenderen Bewertung der Anwendung und Funktionsweise der DSGVO eingeleitet. Die entsprechenden Erkenntnisse legte die Kommission in ihrer Mitteilung „Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung"[17] vor. Schlussfolgerungen zu diesem Aspekt der Überprüfung wurden jedoch vorerst nicht vorgelegt, um das Urteil des Gerichtshofs in der Rechtssache Schrems II[18] berücksichtigen zu können, mit dem der Gerichtshof wichtige Klarstellungen zu Schlüsselelementen der Angemessenheitsfeststellung sowie zu anderen damit zusammenhängenden Entwicklungen vorgenommen hat. Dies wiederum führte zu ausführlichen Beratungen mit den betroffenen Ländern und Gebieten über relevante Aspekte ihres Rechtsrahmens, ihrer Aufsichtsmechanismen und ihres Durchsetzungssystems.[19] In diesem Bericht werden all diese Entwicklungen sowohl in der EU als auch in den betreffenden Drittländern und Gebieten berücksichtigt.

Diese erste Überprüfung findet vor dem Hintergrund der exponentiellen Entwicklung digitaler Technologien statt. In den letzten Jahrzehnten hat die Bedeutung von Angemessenheitsfeststellungen erheblich zugenommen, da Datenströme zu einem integralen Bestandteil des digitalen Wandels der Gesellschaft und der Globalisierung der Wirtschaft geworden sind. Die grenzüberschreitende Übermittlung von Daten gehört zum Betriebsalltag

[14] 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.

[15] Siehe Artikel 45 Absatz 9 der DSGVO, wonach von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen so lange in Kraft bleiben, bis sie durch einen gemäß Artikel 45 Absätze 3 oder 5 erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

[16] Artikel 45 Absatz 4 der DSGVO. Siehe auch Urteil des Gerichtshofs vom 6. Oktober 2015 in der Rechtssache C-362/14, Maximilian Schrems gegen Data Protection Commissioner (Schrems I), ECLI:EU:C:2015:650, Randnummer 76.

[17] Die Mitteilung erschien im Juni 2020 und ist abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020DC0264.

[18] Urteil des Gerichtshofs vom 16. Juli 2020 in der Rechtssache C-311/18, Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems (Schrems II), ECLI:EU:C:2020:559.

[19] Der Angemessenheitsbeschluss betreffend Japan wurde auf der Grundlage der DSGVO erlassen und sieht eine gesonderte regelmäßige Überprüfung vor. Die erste Überprüfung wurde im April 2023 mit dem Bericht der Kommission an das Europäische Parlament und den Rat über die erste Überprüfung der Funktionsweise des Angemessenheitsbeschlusses in Bezug auf Japan abgeschlossen, COM(2023) 275 final, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=COM:2023:275:FIN.

europäischer Unternehmen aller Größen in allen Branchen. Die Achtung der Privatsphäre ist mehr denn je eine Voraussetzung für stabile, sichere und wettbewerbsfähige Handelsströme. Vor diesem Hintergrund spielen Angemessenheitsfeststellungen in vielerlei Hinsicht eine immer wichtigere Rolle. Schutz des Datenverkehrs bedeutet, dass Daten auch nach ihrer Übermittlung geschützt sind und dass die Rechte des Einzelnen im Einklang mit dem auf den Menschen ausgerichteten Ansatz der EU für den digitalen Wandel gewahrt werden. Mit der Angemessenheitsfeststellung wird bescheinigt, dass das Niveau des Datenschutzrahmens eines Drittlandes dem der EU der Sache nach gleichwertig ist, wodurch die Konvergenz der Datenschutzsysteme auf der Grundlage hoher Schutzstandards gefördert wird. Darüber hinaus sind Angemessenheitsfeststellungen, wie in diesem Bericht erläutert, nicht das Ergebnis, sondern vielmehr die Grundlage einer engeren Zusammenarbeit und einer weiteren regulatorischen Konvergenz zwischen der EU und gleichgesinnten Partnern. Die Angemessenheitsfeststellungen haben den freien Verkehr personenbezogener Daten ermöglicht, was zur Öffnung des Handelsverkehrs für die Wirtschaftsbeteiligten in der EU (unter anderem durch die Ergänzung und Verstärkung der Vorteile von Handelsabkommen) und zur Erleichterung der Zusammenarbeit mit ausländischen Partnern in einem breiten Spektrum von Regulierungsbereichen geführt hat. Mit dieser unkomplizierten und umfassenden Lösung für die Übermittlung von Daten, bei der der Datenexporteur weder zusätzliche Garantien vorweisen noch eine Genehmigung einholen muss, wird die Einhaltung der internationalen Übermittlungsanforderungen der DSGVO insbesondere für kleine und mittlere Unternehmen erleichtert. Schließlich werden durch die Europäische Kommission erlassene Angemessenheitsfeststellungen aufgrund ihres „Netzwerkeffekts“ auch über die EU hinaus immer wichtiger, da sie nicht nur den freien Datenverkehr mit den 30 Volkswirtschaften der EU ermöglichen, sondern auch mit vielen anderen Ländern und Gebieten auf der ganzen Welt[20], die in ihren eigenen Datenschutzvorschriften Länder als sichere Zielländer anerkennen, deren Schutzniveau von der EU als angemessen eingestuft wurde.

Aus all diesen Gründen sind Angemessenheitsfeststellungen zu einem strategischen Bestandteil der allgemeinen Beziehungen der EU zu diesen Partnerländern geworden und werden als wesentliche Voraussetzung für die Vertiefung der Zusammenarbeit in einem breiten Spektrum von Bereichen anerkannt. Dies wurde auch im Rahmen des dieser Überprüfung vorausgegangenen intensiven und konstruktiven Dialogs mit den betreffenden Drittländern/Gebieten bekräftigt. Es ist deshalb besonders wichtig, dass Angemessenheitsfeststellungen auf Dauer Bestand haben und neuen Entwicklungen und Herausforderungen gerecht werden.

2. GEGENSTAND UND METHODE DER ÜBERPRÜFUNG

Die Angemessenheitsfeststellungen, die Gegenstand dieser Überprüfung sind, werden im Rahmen des EU-Datenschutzrahmens erlassen, der der DSGVO vorausging. Die jüngsten Feststellungen liegen rund zehn Jahre zurück (z. B. die beiden 2012 angenommenen Beschlüsse zu Neuseeland und Uruguay), andere sind bereits seit über zwanzig Jahren in Kraft (z. B. die Entscheidungen betreffend Kanada von 2001 und die Schweiz von 2000). Seitdem haben sich

[20] Dazu gehören beispielsweise Argentinien, Kolumbien, Israel, Marokko, die Schweiz und Uruguay.

die Datenschutzrahmen in allen elf Ländern und Gebieten weiterentwickelt, beispielsweise durch Gesetzesreformen oder Reformen des ordnungspolitischen Umfelds, Entwicklungen in der Durchsetzungspraxis der Datenschutzbehörden oder die Rechtsprechung.

Bei der Durchführung ihrer Bewertung konzentrierte sich die Kommission deshalb auf die Entwicklungen der Datenschutzrahmen der betreffenden Länder und Gebiete seit der jeweiligen Angemessenheitsfeststellung. Sie bewertete, wie diese Entwicklungen die Datenschutzlandschaft des betreffenden Landes oder Gebiets verändert haben und ob die verschiedenen Regelungen angesichts dieser Entwicklungen weiterhin ein angemessenes Schutzniveau gewährleisten.

Dabei wurde die Entwicklung der Datenschutzvorschriften der EU, insbesondere das Inkrafttreten der DSGVO, umfassend berücksichtigt. Seit der Annahme der Angemessenheitsfeststellungen wurden der für solche Beschlüsse geltende rechtliche Maßstab sowie die Elemente, die für die Feststellung eines angemessenen Schutzniveaus ausländischer Systeme relevant sind, durch die Rechtsprechung des Gerichtshofs und die Leitlinien der Artikel-29-Datenschutzgruppe und ihres Nachfolgers, des Europäischen Datenschutzausschusses[21] (EDSA), weiter präzisiert.

Gemäß dem Urteil des Gerichtshofs vom 6. Oktober 2015 in der Rechtssache Schrems I kann nicht verlangt werden, dass ein Drittland ein dem in der Unionsrechtsordnung garantiertes identisches Schutzniveau gewährleistet. Vielmehr ist unter angemessenem Schutzniveau die Gewährleistung eines Schutzniveaus zu verstehen, das dem in der Union garantierten Niveau der „Sache nach gleichwertig" ist[22]. Der Gerichtshof stellte ferner klar, dass sich die Mittel, auf die das Drittland zur Gewährleistung des Schutzes personenbezogener Daten zurückgreift, durchaus von jenen der Union unterscheiden können, solange sie sich in der Praxis gleichwohl als wirksam erweisen, um einen Schutz zu gewährleisten, der dem in der Union garantierten Schutz der Sache nach gleichwertig ist[23]. Die Angemessenheitsprüfung erfordert deshalb eine umfassende Bewertung des gesamten Systems des Drittlandes, einschließlich der Maßnahmen zum Schutz der Privatsphäre sowie ihrer wirksamen Umsetzung und Durchsetzung.

Darüber hinaus führte der Gerichtshof aus, dass sich die Bewertung durch die Kommission nicht auf den allgemeinen Datenschutzrahmen des Drittlandes beschränken, sondern auch die Vorschriften für den Zugang von Behörden zu personenbezogenen Daten, insbesondere zu Zwecken der Strafverfolgung und der nationalen Sicherheit, umfassen sollte.[24] Unter Bezugnahme auf die Charta der Grundrechte als Maßstab formulierte der Gerichtshof mehrere Anforderungen, die diese Vorschriften erfüllen sollten, um dem Standard der Gleichwertigkeit der Sache nach zu entsprechen. So sollten Regelungen in diesem Bereich klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren personenbezogene Daten

[21] Der Europäische Datenschutzausschuss setzt sich aus den Datenschutzaufsichtsbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten zusammen.
[22] Rechtssache Schrems I, Randnummern 73, 74 und 96. Siehe auch Erwägungsgrund 104 der Verordnung (EU) 2016/679 betreffend die Gleichwertigkeit der Sache nach.
[23] Rechtssache Schrems I, Randnummer 74.
[24] Rechtssache Schrems I, Randnummer 90.

betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen.[25] Desgleichen sollten die Bürger die Möglichkeit haben, mittels eines Rechtsbehelfs Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken.[26]

Die DSGVO stützt sich auf die Ausführungen des Gerichtshofs und enthält eine ausführliche Auflistung von Aspekten, die die Kommission bei der Prüfung der Angemessenheit berücksichtigen muss.[27] Darüber hinaus hat sich der Gerichtshof in seinem Urteil vom 16. Juli 2020 (Schrems II) näher zum Grundsatz der Gleichwertigkeit der Sache nach geäußert, insbesondere in Bezug auf die Vorschriften über den Zugang von Behörden zu personenbezogenen Daten zu Zwecken der Strafverfolgung und der nationalen Sicherheit. Der Grundsatz der Gleichwertigkeit der Sache nach bedeutet, so der Gerichtshof, dass die einschlägigen für die Behörden in den betreffenden Drittländern und Gebieten geltenden Rechtsrahmen Mindesterfordernisse enthalten, die gewährleisten, dass diese Behörden beim Zugang zu Daten nicht über das zur Erreichung legitimer Ziele erforderliche und verhältnismäßige Maß hinausgehen und dass die betroffenen Personen, deren Daten übermittelt werden, über wirksame und durchsetzbare Rechte gegenüber diesen Behörden verfügen.[28]

Die Weiterentwicklung der Angemessenheitsfeststellung spiegelt sich auch in den Leitlinien wider, die ursprünglich von der Artikel-29-Datenschutzgruppe angenommen und anschließend vom EDSA gebilligt wurden.[29] In diesen Leitlinien und insbesondere in der so genannten Referenzgrundlage für Angemessenheit wird präzisiert, welche Aspekte die Kommission bei der Durchführung einer Angemessenheitsbewertung berücksichtigen muss. Dazu gehört u. a. die Bereitstellung eines Überblicks über die wesentlichen Garantien hinsichtlich des Zugangs von Behörden zu personenbezogenen Daten. Die Referenzgrundlage stützt sich insbesondere auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und wurde vom EDSA aktualisiert, um den Ausführungen des Gerichtshofs im Urteil zur Rechtssache Schrems II Rechnung zu tragen.[30] In der Referenzgrundlage für Angemessenheit wird ferner betont, dass es bei der Gleichwertigkeit der Sache nach nicht darum geht, dass die europäischen Vorschriften Punkt für Punkt kopiert werden, da die Mittel zur Gewährleistung eines gleichwertigen Schutzniveaus je nach Datenschutzsystem unterschiedlich sein können und häufig unterschiedliche Rechtstraditionen widerspiegeln.

Um also festzustellen, ob die elf Angemessenheitsbeschlüsse bzw. -entscheidungen, die nach den früheren Vorschriften erlassen wurden, weiterhin den in der DSGVO festgelegten Auflagen entsprechen, hat die Kommission nicht nur die Entwicklung der Datenschutzrahmen in den

[25] Rechtssache Schrems I, Randnummer 91.
[26] Rechtssache Schrems I, Randnummer 95.
[27] Artikel 45 Absatz 2 der DSGVO.
[28] Rechtssache Schrems II, Randnummern 180 bis 182.
[29] Referenzgrundlage für Angemessenheit, WP 254/rev. 01 vom 6.2.2018 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).
[30] Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen (https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_de).

betreffenden Ländern und Gebieten berücksichtigt, sondern auch die Entwicklung bei der Auslegung der Angemessenheitsfeststellung im Rahmen des EU-Rechts. Dazu gehört auch eine Bewertung des Rechtsrahmens für den Zugang zu und die Nutzung von aus der EU übermittelten personenbezogenen Daten durch Behörden der Länder oder Gebiete, die auf der Grundlage von Artikel 25 Absatz 6 der Datenschutzrichtlinie einen angemessenen Schutz bieten.

3. ÜBERPRÜFUNGSVERFAHREN

Wie oben beschrieben, erstreckt sich die Bewertung der erlassenen Angemessenheitsfeststellungen für jedes der betroffenen Länder bzw. Gebiete auf den Datenschutzrahmen und alle Entwicklungen in Bezug auf diesen Rechtsrahmen seit der Annahme der Angemessenheitsfeststellung sowie auf die Vorschriften für den Zugang von Behörden zu Daten, insbesondere für Zwecke der Strafverfolgung und der nationalen Sicherheit. In den vergangenen Jahren haben die Kommissionsdienststellen Schritte unternommen, um die Bewertung in enger Zusammenarbeit mit jedem der betreffenden Länder bzw. Gebiete durchzuführen.

Um die Kommission bei der Erfüllung ihrer Überwachungspflichten zu unterstützen, hat jedes der elf Länder bzw. Gebiete der Kommission umfassende Informationen über die Entwicklung seiner bzw. ihrer Datenschutzregelung seit dem Erlass der Angemessenheitsfeststellung zur Verfügung gestellt. Darüber hinaus holte die Kommission von jedem der elf Länder bzw. Gebiete detaillierte Informationen über die in dem betreffenden Land bzw. Gebiet geltenden Vorschriften für den Zugang von Behörden zu personenbezogenen Daten, insbesondere für Zwecke der Strafverfolgung und der nationalen Sicherheit, ein. Ebenso holte die Kommission Informationen von öffentlichen Quellen, Aufsichts- und Durchsetzungsbehörden sowie von lokalen Sachverständigen über die Funktionsweise der Beschlüsse und über einschlägige Entwicklungen im Recht und in der Praxis der einzelnen betroffenen Länder und Gebiete ein, und zwar sowohl in Bezug auf die für private Betreiber geltenden Datenschutzvorschriften als auch in Bezug auf den Zugang von Behörden. Schließlich wurden gegebenenfalls die internationalen Verpflichtungen, die diese Länder bzw. Gebiete im Rahmen regionaler oder universeller Instrumente eingegangen sind, in angemessener Weise berücksichtigt.

Auf dieser Grundlage hat die Kommission einen intensiven Dialog mit jedem der betroffenen Länder und Gebiete geführt. Im Rahmen dieses Dialogs haben viele dieser Länder und Gebiete ihre Rechtsvorschriften zum Datenschutz durch umfassende oder partielle Reformen modernisiert und gestärkt (z. B. Andorra, Kanada, die Färöer, Schweiz, Neuseeland), was unter anderem der Notwendigkeit geschuldet war, die Kontinuität der Angemessenheitsfeststellungen sicherzustellen. Einige dieser Länder haben Verordnungen und/oder Leitlinien ihrer Datenschutzbehörde erlassen, um neue Datenschutzanforderungen einzuführen (z. B. Israel, Uruguay) oder bestimmte Datenschutzvorschriften zu präzisieren (z. B. Argentinien, Kanada, Guernsey, Jersey, Insel Man, Israel, Neuseeland), die auf der Durchsetzungspraxis oder der Rechtsprechung aufbauen. Wenn dies zur Gewährleistung der Kontinuität der Angemessenheitsfeststellung erforderlich war, wurden darüber hinaus mit einigen der betroffenen Länder und Gebiete zusätzliche Garantien für aus Europa übermittelte

personenbezogene Daten ausgehandelt und vereinbart, um relevante Unterschiede bezüglich des Schutzniveaus anzugehen. So weitete die kanadische Regierung beispielsweise das Recht auf Auskunft und Berichtigung in Bezug auf personenbezogene Daten, die von Behörden verarbeitet werden, auf alle Personen unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnsitz aus (während in der Vergangenheit nur kanadische Staatsbürger sowie Personen mit ständigem Wohnsitz oder in Kanada aufhältige Personen in den Genuss dieser Rechte kamen).[31] Ein weiteres Beispiel: Die israelische Regierung führte spezifische Garantien ein, um den Schutz personenbezogener Daten, die aus dem Europäischen Wirtschaftsraum übermittelt werden, zu stärken, wodurch insbesondere neue Verpflichtungen im Bereich der Datengenauigkeit und Vorratsdatenspeicherung eingeführt, das Recht auf Information und Löschung gestärkt und zusätzliche Kategorien sensibler Daten eingeführt wurden.[32]

Parallel dazu holten die Kommissionsdienststellen die Ansichten des Europäischen Parlaments (Ausschuss für bürgerliche Freiheiten, Justiz und Inneres)[33], des Rates (über die Arbeitsgruppe Datenschutz)[34], des EDSA[35] und der Multi-Stakeholder-Expertengruppe zur DSGVO[36] (der Vertreter der Zivilgesellschaft, der Industrie und der Wissenschaft sowie Angehörige der Rechtsberufe angehören) ein und setzten sie regelmäßig über die Fortschritte bei der Bewertung in Kenntnis.

Dieser Bericht und die begleitende Arbeitsunterlage der Kommissionsdienststellen sind das Ergebnis einer engen Zusammenarbeit mit den einzelnen betroffenen Ländern und Gebieten sowie der Konsultation der einschlägigen Organe und Einrichtungen der EU und deren Rückmeldungen. Sie stützen sich auf eine Vielzahl von Quellen, darunter Rechtsvorschriften, Rechtsakte, Rechtsprechung, Entscheidungen und Leitlinien der Datenschutzbehörden, Berichte (unabhängiger) Aufsichtsgremien und Beiträge von Interessenträgern. Vor der Annahme dieses Berichts wurde allen oben genannten Ländern und Gebieten Gelegenheit gegeben, die sachliche Richtigkeit der Angaben zu ihrem System in der Arbeitsunterlage der Kommissionsdienststellen zu überprüfen.

4. WICHTIGSTE ERGEBNISSE UND SCHLUSSFOLGERUNGEN

Die erste Überprüfung hat gezeigt, dass sich die in jedem der elf Länder bzw. Gebiete geltenden Datenschutzrahmen seit der Annahme der Angemessenheitsfeststellungen weiter an den

[31] Section 12 des „Privacy Act, Privacy Act Extension Order, No. 1“ und „Privacy Act Extension Order, No. 2“.
[32] Datenschutzverordnungen (Anweisungen betreffend Daten, die aus dem Europäischen Wirtschaftsraum an Israel übermittelt wurden), 5783-2023, veröffentlicht im israelischen Amtsblatt (Reshumut) vom 7. Mai 2023.
[33] Siehe z. B. die Entschließung des Europäischen Parlaments vom 25. März 2021 zu dem Bewertungsbericht der Kommission über die Durchführung der Datenschutz-Grundverordnung zwei Jahre nach Beginn ihrer Anwendung (2020/2717(RSP)), abrufbar unter https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_DE.html.
[34] Siehe z. B. Standpunkt und Feststellungen des Rates zur Anwendung der Datenschutz-Grundverordnung (DSGVO) vom 19. Dezember 2019, abrufbar unter https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/de/pdf.
[35] Siehe z. B.“Contribution of the EDPB to the evaluation of the GDPR under Article 97“ vom 18. Februar 2020, abrufbar unter https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.
[36] Siehe z. B. „Report from the Multistakeholder Expert Group on the GDPR evaluation“, abrufbar unter https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=de&do=groupDetail.groupMeeting&meetingId=21356.

Rahmen der EU angeglichen haben. Darüber hinaus hat die erste Überprüfung ergeben, dass das Recht dieser Länder bzw. Gebiete angemessene Garantien und Beschränkungen sowie Aufsichts- und Rechtsbehelfsmechanismen im Bereich des Zugangs von Behörden zu personenbezogenen Daten vorsieht.

Die detaillierten Feststellungen zu jedem der elf Länder bzw. Gebiete sind in der Arbeitsunterlage der Kommissionsdienststellen dargelegt, die diesem Bericht beigefügt ist. Auf der Grundlage dieser Feststellungen kommt die Kommission zu dem Schluss, dass jedes der elf Länder bzw. Gebiete weiterhin ein angemessenes Schutzniveau für aus der Europäischen Union übermittelte personenbezogene Daten im Sinne der DSGVO in der Auslegung durch den Gerichtshof gewährleistet. Die Ergebnisse für jedes der Länder bzw. Gebiete sind nachstehend zusammengefasst.

4.1. Andorra

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen von Andorra seit der Annahme des Angemessenheitsbeschlusses, einschließlich der Gesetzesänderungen und der Tätigkeit der Aufsichtsgremien. Insbesondere die Verabschiedung des qualifizierten Gesetzes 29/2021 über den Schutz personenbezogener Daten, das im Mai 2022 in Kraft trat, hat zu einem höheren Datenschutzniveau beigetragen, da das Gesetz in seiner Struktur und seinen Hauptbestandteilen eng an die DSGVO angelehnt ist.

Für den Zugang von Behörden zu personenbezogenen Daten gelten in Andorra klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen und internationalen Verpflichtungen, insbesondere aus der Verfassung Andorras, der Europäischen Menschenrechtskonvention (EMRK) und dem Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108 und dem Änderungsprotokoll, d. h. der aktualisierten Konvention 108+), sowie aus spezifischen Datenschutzvorschriften für die Verarbeitung personenbezogener Daten im Rahmen der Strafverfolgung, mit denen im Wesentlichen die Kernelemente der Richtlinie (EU) 2016/680[37] übernommen werden. Darüber hinaus sind im andorranischen Recht für den Zugang zu personenbezogenen Daten und ihre Verwendung durch staatliche Stellen eine Reihe besonderer Bedingungen und Beschränkungen sowie entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass Andorra weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt.

[37] 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.

In Bezug auf die spezifischen Datenschutzvorschriften, die derzeit für die Datenverarbeitung durch Strafverfolgungsbehörden gelten, begrüßt die Kommission die Absicht des andorranischen Gesetzgebers, diese Vorschriften durch eine umfassendere Regelung zu ersetzen, die noch näher an die in der EU geltenden Vorschriften angelehnt sein wird. Die Kommission wird hier die künftigen Entwicklungen aufmerksam verfolgen.

4.2. Argentinien

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen Argentiniens seit der Annahme der Angemessenheitsentscheidung, einschließlich der Gesetzesänderungen, der Rechtsprechung und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere wurde die Unabhängigkeit der argentinischen Datenschutzaufsichtsbehörde durch das Dekret Nr. 746/17, mit dem die „Agencia de Acceso a la Información Pública“ (AAIP) mit der Überwachung der Einhaltung des Datenschutzgesetzes betraut wurde, erheblich gestärkt. Darüber hinaus gab die AAIP eine Reihe verbindlicher Verordnungen und Stellungnahmen ab, in denen präzisiert wird, wie der Datenschutzrahmen in der Praxis auszulegen und anzuwenden ist, und die somit dazu beitragen, das Datenschutzgesetz auf dem neuesten Stand zu halten. Zudem hat Argentinien seine internationalen Verpflichtungen im Bereich des Datenschutzes gestärkt, indem es 2019 dem Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dessen Zusatzprotokoll beigetreten ist und das Änderungsprotokoll, das heißt die der aktualisierte Konvention Nr. 108+, im Jahr 2023 ratifiziert hat.

Für den Zugang von Behörden zu personenbezogenen Daten gelten in Argentinien klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen und internationalen Verpflichtungen, insbesondere aus der argentinischen Verfassung, der Amerikanischen Menschenrechtskonvention, den Konventionen 108 und 108+ sowie aus den argentinischen Datenschutzvorschriften (Gesetz 25.326 über den Schutz personenbezogener Daten vom 4. Oktober 2000), die auch für die Verarbeitung personenbezogener Daten durch staatliche Stellen in Argentinien, einschließlich zum Zweck der Strafverfolgung und der nationalen Sicherheit, gelten. Im argentinischen Recht sind für den Zugang zu personenbezogenen Daten und ihre Verwendung zu Zwecken der Strafverfolgung und der nationalen Sicherheit darüber hinaus eine Reihe besonderer Bedingungen und Beschränkungen sowie entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass Argentinien weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt.

Gleichzeitig empfiehlt die Kommission, die auf nachgeordneter Ebene entwickelten Schutzmaßnahmen gesetzlich zu verankern, um die Rechtssicherheit zu erhöhen und diese

Anforderungen zu konsolidieren. Der Entwurf eines Datenschutzgesetzes, der kürzlich im argentinischen Kongress vorgelegt wurde, könnte die Möglichkeit bieten, diese Entwicklungen festzuschreiben und damit den argentinischen Datenschutzrahmen weiter zu festigen. Die Kommission wird hier die künftigen Entwicklungen aufmerksam verfolgen.

4.3. Kanada

Die Kommission begrüßt die Entwicklungen im kanadischen Rechtsrahmen seit der Annahme der Angemessenheitsentscheidung, einschließlich verschiedener Gesetzesänderungen, der Rechtsprechung und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere wurde das Gesetz über den Schutz personenbezogener Informationen und elektronische Dokumente (Personal Information Protection and Electronic Documents Act – PIPEDA) durch verschiedene Änderungen (z. B. in Bezug auf die Bedingungen für eine gültige Einwilligung und die Meldung von Datenschutzverletzungen) weiter gestärkt, während zentrale Datenschutzanforderungen (z. B. in Bezug auf die Verarbeitung sensibler Daten) durch die Rechtsprechung sowie durch Leitlinien der kanadischen Bundesdatenschutzbehörde (Office of the Privacy Commissioner) weiter präzisiert wurden. Gleichzeitig empfiehlt die Kommission, einige der auf nachgeordneter Ebene entwickelten Schutzmaßnahmen gesetzlich zu verankern, um die Rechtssicherheit zu erhöhen und diese Anforderungen zu konsolidieren. Die laufende Gesetzesreform des PIPEDA könnte insbesondere die Möglichkeit bieten, solche Entwicklungen festzuschreiben und damit den kanadischen Datenschutzrahmen weiter zu festigen. Die Kommission wird hier die künftigen Entwicklungen aufmerksam verfolgen.

Für den Zugang von Behörden zu personenbezogenen Daten gelten in Kanada klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten verfassungsrechtlichen Rahmen (Kanadische Charta der Rechte und Freiheiten), der Rechtsprechung, spezifischen Rechtsvorschriften über den Zugang zu Daten sowie Datenschutzvorschriften (d. h. dem Privacy Act und vergleichbaren Gesetzen auf Provinzebene), die auch für die Verarbeitung personenbezogener Daten durch staatliche Stellen in Kanada, einschließlich zum Zweck der Strafverfolgung und der nationalen Sicherheit, gelten. Darüber hinaus bietet das kanadische Rechtssystem wirksame Aufsichts- und Rechtsbehelfsmechanismen in diesem Bereich, unter anderem durch die kürzlich erfolgte Ausweitung der Rechte betroffener Personen und der Rechtsbehelfe für nichtkanadische Staatsangehörige oder Gebietsansässige.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass Kanada weiterhin ein angemessenes Schutzniveau für personenbezogene Daten sicherstellt, die die EU an dem PIPEDA unterliegende Empfänger übermittelt. Wie bereits erwähnt, ist das PIPEDA derzeit Gegenstand einer Gesetzesreform, die den Schutz der Privatsphäre weiter festigen könnte, auch in Bereichen, die für die Angemessenheitsfeststellung relevant sind.

4.4. Die Färöer

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen der Färöer seit der Annahme des Angemessenheitsbeschlusses, einschließlich der Gesetzesänderungen, der Rechtsprechung und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere haben die Färöer ihren Datenschutzrahmen durch den Erlass des 2021 in Kraft getretenen Datenschutzgesetzes erheblich modernisiert, mit dem die Bestimmungen der Färöer eng an die DSGVO angelehnt wurden.

Für den Zugang von Behörden zu personenbezogenen Daten gelten auf den Färöern klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen und internationalen Verpflichtungen, insbesondere dem Verfassungsrahmen und der EMRK, sowie aus spezifischen Gesetzen über den Zugriff von Behörden auf Daten und aus Datenschutzvorschriften, die für die Verarbeitung personenbezogener Daten für die Strafverfolgung (das Gesetz über die Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden, das auf den Färöern 2022 in Kraft trat und mit dem die von Dänemark zur Umsetzung der Richtlinie (EU) 2016/680 auf den Färöern erlassenen Rechtsvorschriften umgesetzt wurden) und für Zwecke der nationalen Sicherheit (gemäß dem Gesetz über den Sicherheits- und Nachrichtendienst) gelten. Darüber hinaus stehen in diesem Bereich wirksame Aufsichts- und Rechtsbehelfsmechanismen zur Verfügung.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass die Färöer weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellen.

4.5. Guernsey

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen Guernseys seit der Annahme der Angemessenheitsentscheidung, einschließlich der Gesetzesänderungen und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere hat Guernsey durch den Erlass des 2019 in Kraft getretenen Datenschutzgesetzes „The Data Protection (Bailiwick of Guernsey) Law, 2017“, mit dem die Bestimmungen Guernseys eng an die Datenschutz-Grundverordnung angelehnt wurden, seinen Datenschutzrahmen umfassend aktualisiert.

Für den Zugang von Behörden zu personenbezogenen Daten gelten in Guernsey klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen und internationalen Verpflichtungen, insbesondere der EMRK und dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108), sowie aus den Datenschutzbestimmungen von Guernsey, einschließlich der besonderen Bestimmungen für die Verarbeitung personenbezogener Daten im Rahmen der Strafverfolgung,

die in der Datenschutzverordnung „The Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018“, festgelegt sind. Darüber hinaus sind im Recht Guernseys für den Zugang zu personenbezogenen Daten und ihre Verwendung zu Zwecken der Strafverfolgung und der nationalen Sicherheit eine Reihe besonderer Bedingungen und Beschränkungen sowie entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass Guernsey weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt.

4.6. Insel Man

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen der Insel Man seit der Annahme der Angemessenheitsentscheidung, einschließlich der Gesetzesänderungen und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere hat die Insel Man 2018 neue Gesetze erlassen (Datenschutzgesetz „Data Protection Act 2018“, ergänzt durch die Datenschutzverfügung „Data Protection (Application of GDPR) Order 2018“), mit denen der Großteil der Bestimmungen des EU-Datenschutzrahmens in die Rechtsordnung der Insel Man übernommen wurden, wobei nur bei bestimmten Aspekten geringfügige Anpassungen vorgenommen wurden, die vor allem der Angleichung des Rahmens an die lokalen Gegebenheiten dienten.

Für den Zugang von Behörden zu personenbezogenen Daten gelten auf der Insel Man klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen und internationalen Verpflichtungen, insbesondere der EMRK und dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108), sowie aus den Datenschutzbestimmungen der Insel Man, einschließlich der besonderen Bestimmungen für die Verarbeitung personenbezogener Daten im Rahmen der Strafverfolgung, die in der Datenschutzverfügung „Data Protection (Application of LED) Order 2018“ und den Durchführungsbestimmungen „GDPR and LED Implementing Regulations 2018“, festgelegt sind. Darüber hinaus sind im Recht der Insel Man für den Zugang zu personenbezogenen Daten und ihre Verwendung zu Zwecken der Strafverfolgung und der nationalen Sicherheit eine Reihe besonderer Beschränkungen sowie entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass die Insel Man weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt.

4.7. Israel

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen Israels seit der Annahme des Angemessenheitsbeschlusses, einschließlich der Gesetzesänderungen, der Rechtsprechung und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere hat Israel mit der Annahme der Datenschutzbestimmungen „Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023“, besondere Garantien für einen stärkeren Schutz der aus dem Europäischen Wirtschaftsraum übermittelten personenbezogenen Daten geschaffen. Durch die Annahme der Datenschutzbestimmungen „Protection of Privacy Regulations (Data Security), 5777-2017“ hat Israel darüber hinaus die Anforderungen an die Datensicherheit verschärft und die Unabhängigkeit seiner Datenschutzaufsichtsbehörde durch einen verbindlichen Regierungsbeschluss gestärkt.

Für den Zugang von Behörden zu personenbezogenen Daten gelten in Israel klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Einschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen, insbesondere dem israelischen Grundgesetz sowie dem Gesetz über den Schutz der Privatsphäre „Protection of Privacy Law, 5741-1981“ und den auf dessen Grundlage erlassenen Verordnungen, die für die Verarbeitung personenbezogener Daten durch israelische Behörden, auch für Zwecke der Strafverfolgung und der nationalen Sicherheit, zugrunde gelegt werden. Darüber hinaus sind im Recht Israels für den Zugang zu personenbezogenen Daten und ihre Verwendung zu Zwecken der Strafverfolgung und der nationalen Sicherheit eine Reihe besonderer Beschränkungen sowie entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass Israel weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt.

Gleichzeitig empfiehlt die Kommission, die auf nachgeordneter Ebene und im Rahmen der Rechtsprechung entwickelten Schutzmaßnahmen gesetzlich zu verankern, um die Rechtssicherheit zu erhöhen und sie auf eine solidere Basis zu stellen. Das kürzlich in das israelische Parlament eingebrachte Gesetz über den Schutz der Privatsphäre „Privacy Protection Bill (Amendment No. 14), 5722-2022“ bietet eine gute Gelegenheit, diese Entwicklungen zu konsolidieren und festzuschreiben und damit den Datenschutzrahmen in Israel weiter zu festigen. Die Kommission wird hier die künftigen Entwicklungen aufmerksam verfolgen.

4.8. Jersey

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen Jerseys seit der Annahme der Angemessenheitsentscheidung, einschließlich der Gesetzesänderungen, der Rechtsprechung und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere hat Jersey durch den Erlass der 2018 in Kraft getretenen Gesetze über den

Datenschutz „Data Protection (Jersey) Law, 2018“ und über eine Datenschutzbehörde „Data Protection Authority (Jersey) Law 2018“, mit denen die Bestimmungen Jerseys eng an die Datenschutz-Grundverordnung angelehnt wurden, seinen Datenschutzrahmen umfassend aktualisiert.

Für den staatlichen Zugang zu personenbezogenen Daten gelten in Jersey klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen und internationalen Verpflichtungen, insbesondere der EMRK und dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108), sowie aus den Datenschutzbestimmungen Jerseys, einschließlich der besonderen Bestimmungen für die Verarbeitung personenbezogener Daten im Rahmen der Strafverfolgung, die in dem Datenschutzgesetz „Data Protection (Jersey) Law 2018“ in der Fassung gemäß Anhang „Schedule 1“ dieses Gesetzes, festgelegt sind. Darüber hinaus sind im Recht Jerseys für den Zugang zu personenbezogenen Daten und ihre Verwendung zu Zwecken der Strafverfolgung und der nationalen Sicherheit eine Reihe besonderer Beschränkungen sowie entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass Jersey weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt.

4.9. Neuseeland

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen Neuseelands seit der Annahme des Angemessenheitsbeschlusses, einschließlich der Gesetzesänderungen, der Rechtsprechung und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere wurde die Datenschutzregelung mit der Annahme des Datenschutzgesetzes „Privacy Act 2020“, mit der die Abstimmung mit dem Datenschutzrahmen der EU weiter verstärkt wurde, grundlegend aktualisiert, vor allem in Bezug auf die Bestimmungen für die internationale Übermittlung personenbezogener Daten und die Befugnisse der Datenschutzbehörde (Amt des Datenschutzbeauftragten).

Für den Zugang von Behörden zu personenbezogenen Daten gelten in Neuseeland klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten verfassungsrechtlichen Rahmen (z. B. „Bill of Rights Act“) und der Rechtsprechung sowie aus besonderen Gesetzen zur Regelung des staatlichen Zugriffs auf Daten und den Bestimmungen des „Privacy Act“, die auch für die Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden und nationale Sicherheitsbehörden gelten. Darüber hinaus sind im neuseeländischen Recht verschiedene entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass Neuseeland weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt. Die Kommission begrüßt ferner, dass die neuseeländische Regierung kürzlich einen Gesetzentwurf zur Änderung des „Privacy Act 2020“ ins Parlament eingebracht hat, mit dem die bestehenden Transparenzanforderungen weiter gestärkt werden sollen. Die Kommission wird hier die künftigen Entwicklungen aufmerksam verfolgen.

4.10. Schweiz

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen der Schweiz seit der Annahme des Angemessenheitsbeschlusses, einschließlich der Gesetzesänderungen, der Rechtsprechung und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben, insbesondere das aktualisierte Bundesdatenschutzgesetz, das die Konvergenz mit dem EU-Datenschutzrahmen weiter erhöht hat, vor allem im Hinblick auf den Schutz sensibler Daten und die Regeln für die internationale Datenübermittlung. Darüber hinaus hat die Schweiz durch die Ratifizierung des modernisierten Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108+) im September 2023 auch ihre internationalen Verpflichtungen im Bereich des Datenschutzes gestärkt.

Für den Zugang von Behörden zu personenbezogenen Daten gelten in der Schweiz klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen und internationalen Verpflichtungen, insbesondere aus der Bundesverfassung der Schweizerischen Eidgenossenschaft, der EMRK und der Konvention 108+, sowie aus den Datenschutzbestimmungen der Schweiz, einschließlich des Bundesgesetzes über den Datenschutz, und besonderen Datenschutzvorschriften für die Strafverfolgung (z. B. Strafprozessordnung) und nationale Sicherheitsbehörden (z. B. Nachrichtendienstgesetz). Darüber hinaus sind im Recht der Schweiz für den Zugang zu personenbezogenen Daten und ihre Verwendung zu Zwecken der Strafverfolgung und der nationalen Sicherheit eine Reihe besonderer Beschränkungen sowie entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die in der Arbeitsunterlage der Kommissionsdienststellen insgesamt getroffen werden, kommt die Kommission zu dem Schluss, dass die Schweiz weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt.

4.11. Uruguay

Die Kommission begrüßt die Entwicklungen im Rechtsrahmen Uruguays seit der Annahme des Angemessenheitsbeschlusses, einschließlich verschiedener Gesetzesänderungen, der Rechtsprechung und der Tätigkeit der Aufsichtsgremien, die zu einem höheren Datenschutzniveau beigetragen haben. Insbesondere hat Uruguay sein Gesetz 18.331 über den

Schutz personenbezogener Daten „Ley de proteccion de datos personales y acción de habeas data“ aus dem Jahr 2008 durch Gesetzesänderungen in den Jahren 2018 und 2020 aktualisiert und verschärft. Mit diesen Änderungen wurde der territoriale Geltungsbereich des Datenschutzrechtes erweitert, und es wurden neue Anforderungen an die Rechenschaftspflicht (wie Folgenabschätzungen, Datenschutz durch Technikgestaltung und durch Voreinstellungen, Benachrichtigung über Datenschutzverletzungen und die Ernennung von Datenschutzbeauftragten) sowie zusätzliche Schutzmaßnahmen für biometrische Daten eingeführt. Uruguay hat darüber hinaus durch den Beitritt zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) im Jahr 2019 und durch die Ratifizierung der modernisierten Fassung des Übereinkommens (Konvention 108+) im Jahr 2021 seine internationalen Verpflichtungen im Bereich des Datenschutzes gestärkt.

Für den Zugang von Behörden zu personenbezogenen Daten gelten in Uruguay klare, eindeutige und zugängliche Regeln, nach denen staatliche Stellen für Ziele des öffentlichen Interesses, insbesondere für die Strafverfolgung und die nationale Sicherheit, auf aus der EU übermittelte Daten zugreifen und diese Daten nutzen können. Diese Beschränkungen und Garantien ergeben sich aus dem übergeordneten Rechtsrahmen und internationalen Verpflichtungen, insbesondere aus der uruguayischen Verfassung, der Amerikanischen Menschenrechtskonvention, den Konventionen 108 und 108+ sowie aus den Datenschutzvorschriften des Gesetzes 18.331 über den Schutz personenbezogener Daten und dem „Habeas-data“-Rechtsbehelf, die für die Verarbeitung personenbezogener Daten durch staatliche Stellen in Uruguay, insbesondere zum Zweck der Strafverfolgung und der nationalen Sicherheit, gelten. Darüber hinaus sind im Recht Uruguays für den Zugang zu personenbezogenen Daten und ihre Verwendung durch staatliche Stellen eine Reihe besonderer Bedingungen und Beschränkungen sowie entsprechende Aufsichtsmechanismen und Rechtsbehelfe vorgesehen.

Ausgehend von den Feststellungen, die im Rahmen dieser ersten Einschätzung insgesamt getroffen wurden, kommt die Kommission zu dem Schluss, dass Uruguay weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten sicherstellt.

5. KÜNFTIGE ÜBERWACHUNG UND ZUSAMMENARBEIT

Die Kommission nimmt die ausgezeichnete Zusammenarbeit mit den zuständigen Behörden der jeweiligen Länder und Gebiete bei der Durchführung dieser Überprüfung zur Kenntnis und weiß sie in hohem Maße zu würdigen. Die Kommission wird weiterhin genau verfolgen, wie sich die Datenschutzrahmen und die tatsächliche Praxis in den jeweiligen Ländern und Gebieten weiterentwickeln. Sollten in einem Land bzw. Gebiet mit einem angemessenen Schutzniveau Entwicklungen mit negativen Auswirkungen auf das bisher für angemessen befundene Datenschutzniveau stattfinden, wird die Kommission erforderlichenfalls von ihren Befugnissen gemäß Artikel 45 Absatz 5 DSGVO Gebrauch machen und eine Angemessenheitsfeststellung aussetzen, ändern oder widerrufen.

Diese Überprüfung zeigt erneut, dass es sich bei dem Beschluss der Angemessenheit nicht um eine endgültige Feststellung handelt, sondern um eine Gelegenheit, den Dialog über

Datenströme und, allgemeiner, digitale Angelegenheiten sowie die entsprechende Zusammenarbeit mit gleichgesinnten internationalen Partnern weiter zu vertiefen. In diesem Zusammenhang sieht die Kommission dem künftigen Austausch mit den zuständigen Behörden zur weiteren Stärkung der Zusammenarbeit auf internationaler Ebene im Sinne eines sicheren und freien Datenverkehrs, auch durch eine intensivere Kooperation bei der Strafverfolgung, zuversichtlich entgegen. Zur Vertiefung dieses Dialogs und zur Förderung des Informations- und Erfahrungsaustauschs beabsichtigt die Kommission, im Jahr 2024 für die EU und alle Länder, die von einer Angemessenheitsfeststellung profitieren, ein hochrangiges Treffen durchzuführen.