Stellungnahme 15/2021 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Richtlinie (EU) 2016/680 über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich

Angenommen am 13. April 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versionsverlauf

Fassung 1.1	6. Juli 2021	Formatänderungen
Fassung 1.0	13. April 2021	Annahme der Stellungnahme

INHALTSVERZEICHNIS

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 51 Absatz 1 Buchstabe g der 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[1] (im Folgenden „Richtlinie zum Datenschutz bei der Strafverfolgung"),

gestützt auf die Artikel 12 und 22 seiner Geschäftsordnung –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG

1. Die Europäische Kommission hat am 19. Februar 2021 ihren Entwurf eines Durchführungsbeschlusses über die Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (im Folgenden „Entwurf des Angemessenheitsbeschlusses") gebilligt.[2] Anschließend hat die Europäische Kommission das Verfahren für seine förmliche Annahme eingeleitet.

2. Am gleichen Tag ersuchte die Europäische Kommission den Europäischen Datenschutzausschuss (EDSA) um eine Stellungnahme.[3] Der EDSA stützte seine Bewertung der Angemessenheit des durch das Vereinigte Königreich gewährleisteten Schutzniveaus auf eine Prüfung des Entwurfs des Angemessenheitsbeschlusses sowie auf die Auswertung der von der Kommission bereitgestellten Unterlagen.

3. Die Hauptbezugspunkte für die Arbeit des EDSA bildeten die am 2. Februar 2021 angenommene Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung[4] sowie die einschlägige Rechtsprechung, auf die in den Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen[5] eingegangen wird.

4. Das wichtigste Ziel des EDSA besteht darin, der Europäischen Kommission eine Stellungnahme zur Angemessenheit des Schutzniveaus für natürliche Personen im Vereinigten Königreich an die Hand zu geben. Natürlich erwartet der EDSA nicht, dass der Rechtsrahmen des Vereinigten Königreichs das europäische Datenschutzrecht nachbildet.

5. Der EDSA weist jedoch darauf hin, dass Artikel 36 der Richtlinie zum Datenschutz bei der Strafverfolgung und die Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden

[1] ABl. L 119 vom 4.5.2016, S. 89.
[2] Siehe die Pressemitteilung der Europäischen Kommission „Datenschutz: Europäische Kommission leitet Verfahren zu Übermittlungen personenbezogener Daten in das Vereinigte Königreich ein" vom 19. Februar 2021, https://ec.europa.eu/commission/presscorner/detail/de/ip_21_661.
[3] Ebenda.
[4] Siehe die Empfehlungen 01/2021 des EDSA zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung, angenommen am 2. Februar 2021, https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_de.pdf.
[5] Siehe die Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, angenommen am 10. November 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf.

„EuGH“) vorsehen, dass die Rechtsvorschriften des Drittlandes an den Wesensgehalt der in der Richtlinie zum Datenschutz bei der Strafverfolgung verankerten Grundsätze angeglichen sein müssen, damit davon ausgegangen werden kann, dass sie ein angemessenes Schutzniveau bieten. Im Bereich Datenschutz stellt der EDSA fest, dass es eine starke Angleichung zwischen dem Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung und dem Rechtsrahmen des Vereinigten Königreichs in Bezug auf bestimmte Kernbestimmungen gibt, unter anderem in Bezug auf Begriffe (z. B. „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“ und „Verantwortlicher“), die Gründe für die rechtmäßige und faire Verarbeitung für legitime Zwecke, die Zweckbindung, die Datenqualität und die Verhältnismäßigkeit, die Datenspeicherung, die Sicherheit und die Vertraulichkeit, die Transparenz, besondere Datenkategorien, die automatisierte Entscheidungsfindung und das Profiling.

6. Der EDSA empfiehlt der Europäischen Kommission, dass sie ihre Analyse durch Informationen darüber ergänzt, ob ein Mechanismus existiert, mit dem die Behörden des Vereinigten Königreichs die zuständigen Behörden des jeweiligen Mitgliedstaats über die Weiterverarbeitung oder Offenlegung der an sie übermittelten personenbezogenen Daten unterrichten können, und dass sie die Wirksamkeit dieses Mechanismus im Rahmen der Rechtsordnung des Vereinigten Königreichs feststellt.

7. Der EDSA ist der Ansicht, dass die Bestimmungen in Teil 3 Kapitel 5 des vom Vereinigten Königreich erlassenen Data Protection Act 2018 (im Folgenden „Datenschutzgesetz von 2018“) grundsätzlich ein Schutzniveau bieten, das dem nach Unionsrecht gewährleisteten Schutzniveau der Sache nach gleichwertig ist, wenn es um die Übermittlung personenbezogener Daten von einer Strafverfolgungsbehörde des Vereinigten Königreichs an ein Drittland geht.

8. Der EDSA erkennt zwar an, dass das Vereinigte Königreich innerhalb seines rechtlichen Rahmens Gebieten in Anbetracht des Datenschutzrahmens ein angemessenes Datenschutzniveau bescheinigen kann, doch möchte der EDSA darauf hinweisen, dass dies zu Risiken in Bezug auf den Schutz personenbezogener Daten, die aus der EU übermittelt werden, führen könnte, insbesondere wenn der Datenschutzrahmen des Vereinigten Königreichs in Zukunft vom Besitzstand der Union abweicht. **In den oben genannten Situationen sollte die Europäische Kommission daher ihre Überwachungsfunktion erfüllen. Sollte das der Sache nach gleichwertige Schutzniveau der von der EU übermittelten personenbezogenen Daten nicht aufrechterhalten werden, sollte die Europäische Kommission erwägen, den Angemessenheitsbeschluss zu ändern, um spezifische Garantien für Daten einzuführen, die aus der EU übermittelt werden, und/oder den Angemessenheitsbeschluss auszusetzen.**

9. **In Bezug auf die zwischen dem Vereinigten Königreich und Drittländern geschlossenen internationalen Abkommen** wird die Europäische Kommission gebeten, das Zusammenspiel zwischen dem Datenschutzrahmen des Vereinigten Königreichs und seinen internationalen Verpflichtungen zu prüfen, um besonders dann die Kontinuität des Schutzniveaus zu gewährleisten, wenn personenbezogene Daten auf der Grundlage des Angemessenheitsbeschlusses zum Vereinigten Königreich von der EU in das Vereinigte Königreich und dann in andere Drittländer weiterübermittelt werden. Für den Fall, dass der Abschluss internationaler Abkommen zwischen dem Vereinigten Königreich und Drittländern das Risiko birgt, dass das in der EU gewährleistete Schutzniveau für personenbezogene Daten untergraben wird, sollte die Europäische Kommission für eine kontinuierliche Überwachung sorgen und erforderlichenfalls Maßnahmen ergreifen.

10. In diesem Zusammenhang weist der EDSA darauf hin, dass das Inkrafttreten des Abkommens zwischen dem Vereinigten Königreich und den USA über den Zugang zu elektronischen Daten für den Zweck der

Bekämpfung schwerer Straftaten (im Folgenden „US Cloud Act“)[6] Auswirkungen auf die Weiterübermittlung durch Strafverfolgungsbehörden im Vereinigten Königreich haben kann, insbesondere in Bezug auf die Ausstellung und Übermittlung von Anordnungen gemäß Artikel 5 des US Cloud Act.

11. Der EDSA empfiehlt außerdem, dass die Europäische Kommission fortlaufend überwacht, ob der Abschluss künftiger Abkommen mit Drittländern zum Zwecke der Zusammenarbeit bei der Strafverfolgung, die eine Rechtsgrundlage für die Übermittlung personenbezogener Daten in diese Länder bieten, die Bedingungen für die Weitergabe der erhobenen Informationen beeinflussen könnte, insbesondere ob die Bestimmungen dieser internationalen Abkommen die Anwendung des Datenschutzrechts des Vereinigten Königreichs beeinträchtigen und weitere Beschränkungen oder Ausnahmen in Bezug auf die Weiterverwendung und Offenlegung von zu Strafverfolgungszwecken erhobenen Informationen im Ausland vorsehen könnten. Der EDSA ist der Ansicht, dass solche Informationen und Bewertungen unerlässlich sind, um eine umfassende Überprüfung des Schutzniveaus zu ermöglichen, das durch den Rechtsrahmen des Vereinigten Königreichs und die Vorgehensweisen in Bezug auf die Offenlegung gegenüber dem Ausland gewährleistet wird.

2 EINLEITUNG

2.1 Datenschutzrahmen des Vereinigten Königreichs

12. Da das Vereinigte Königreich bis zum 31. Januar 2020 ein Mitgliedstaat der EU war, basiert sein Datenschutzrahmen weitgehend auf dem Datenschutzrahmen der EU (insbesondere auf der Richtlinie zum Datenschutz bei der Strafverfolgung und der 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 (im Folgenden „DSGVO“). Darüber hinaus wird mit den Bestimmungen in Teil 3 des Datenschutzgesetzes von 2018, das am 23. Mai 2018 in Kraft trat und mit dem das Datenschutzgesetz des Vereinigten Königreichs aus dem Jahr 1998 aufgehoben wurde, die DSGVO umgesetzt. Auch wird darin die Anwendung der DSGVO innerhalb des Rechtsrahmens des Vereinigten Königreichs näher spezifiziert, und es werden die Befugnisse und Pflichten der nationalen Datenschutzaufsichtsbehörde des Vereinigten Königreichs (Information Commissioner's Office, im Folgenden „ICO“) präzisiert.

13. Wie in Erwägungsgrund 12 des Entwurfs des Angemessenheitsbeschlusses erwähnt, hat die Regierung des Vereinigten Königreichs das Gesetz von 2018 über den Austritt aus der Europäischen Union (European Union (Withdrawal) Act) erlassen, mit dem unmittelbar anzuwendendes Unionsrecht in das Recht des Vereinigten Königreichs übernommen wird. Nach diesem Gesetz haben die Minister des Vereinigten Königreichs die Befugnis, über gesetzliche Instrumente eine Sekundärgesetzgebung einzuführen, um nach dem Austritt des Vereinigten Königreichs aus der EU die notwendigen Änderungen am beibehaltenen Unionsrecht vorzunehmen, damit es in den nationalen Kontext passt.

[6] Siehe das Abkommen zwischen der Regierung des Vereinigten Königreichs von Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugang zu elektronischen Daten für den Zweck der Bekämpfung schwerer Straftaten, Washington DC, USA, 3. Oktober 2019.

14. Folglich umfasst der einschlägige Rechtsrahmen, der im Vereinigten Königreich nach dem Ende des Übergangszeitraums[7] gilt, folgende Kernpunkte:

- die Datenschutzgrundverordnung des Vereinigten Königreichs, wie sie im Rahmen des European Union (Withdrawal) Act 2018 in das Recht des Vereinigten Königreichs aufgenommen wurde, in der Fassung der sogenannten DPPEC-Verordnungen von 2019 (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019),
- das Datenschutzgesetz von 2018, geändert durch die DPPEC-Verordnungen von 2019, und die Verordnungen von 2020 zu Datenschutz und elektronischer Kommunikation (Änderungen usw.) sowie
- das Gesetz über Ermittlungsbefugnisse von 2016 (Investigatory Powers Act 2016).

(gemeinsam im Folgenden „Datenschutzrahmen des Vereinigten Königreichs").

2.2 Umfang der Bewertung durch den EDSA

15. Der Entwurf des Angemessenheitsbeschlusses der Europäischen Kommission ist das Ergebnis einer Bewertung des Datenschutzrahmens des Vereinigten Königreichs, auf die Erörterungen mit der Regierung des Vereinigten Königreichs folgten. Gemäß Artikel 51 Absatz 1 Buchstabe g der Richtlinie zum Datenschutz bei der Strafverfolgung wird vom EDSA erwartet, dass er eine unabhängige Stellungnahme zu den Feststellungen der Europäischen Kommission abgibt, etwaige Unzulänglichkeiten im Angemessenheitsrahmen feststellt und gegebenenfalls Änderungen vorschlägt, um diese zu beheben.

16. Wie es in der Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung des EDSA heißt, sollten „die von der Europäischen Kommission bereitgestellten Informationen umfassend sein" und es dem EDSA ermöglichen, das Datenschutzniveau im betreffenden Drittland selbst zu beurteilen.[8]

17. Dazu ist anzumerken, dass der EDSA nur einen Teil der für die Prüfung des Rechtsrahmens des Vereinigten Königreichs relevanten Dokumente rechtzeitig erhalten hat. Der EDSA erhielt den größten Teil der Rechtsvorschriften des Vereinigten Königreichs, auf die im Entwurf des Angemessenheitsbeschlusses Bezug genommen wurde, über darin enthaltene Links. Die Europäische Kommission war nicht in der Lage, dem EDSA schriftliche Erklärungen und Zusagen des Vereinigten Königreichs in Bezug auf den für diese Aufgabe relevanten Austausch zwischen den Behörden des Vereinigten Königreichs und der Europäischen Kommission zu übermitteln.[9]

[7] Das Ende des Übergangszeitraums wurde mit dem 31. Dezember 2020 festgelegt. Nach diesem Datum gilt das Unionsrecht im Vereinigten Königreich nicht mehr. Die „Überbrückungsfrist" gilt bis höchstens 30. Juni 2021 und entspricht dem Zeitraum, in dem die Übertragung personenbezogener Daten aus der EU in das Vereinigte Königreich noch nicht als Übermittlung gilt.

[8] Siehe die Empfehlungen 01/2021 zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung, Ziffer 15, S. 6.

[9] Dabei handelt es sich um die Elemente, bei denen die Europäische Kommission in ihrem Entwurf des Angemessenheitsbeschlusses auf Erklärungen der Behörden des Vereinigten Königreichs verweist, ohne schriftliche Unterlagen vorzulegen, die die Erklärungen beispielsweise in Bezug auf folgende Punkte untermauern würden: die Auswirkungen der Übergangsbestimmungen und das Fehlen einer Verfallsklausel (Erwägungsgrund 87), Beispiele einer Einwilligung als angemessene Grundlage für die Verarbeitung (Fußnote 68), den Begriff „ungenau" für „unrichtige oder irreführende" personenbezogene Daten (Fußnote 79), den Aufgabenbereich des Ausschusses für Nachrichtenwesen und Sicherheit (Intelligence and Security

18. Unter Berücksichtigung der obigen Ausführungen und aufgrund des begrenzten Zeitrahmens (zwei Monate), der dem EDSA für die Annahme dieser Stellungnahme zur Verfügung steht, hat sich der EDSA dafür entschieden, sich auf einige bestimmte Punkte des Entwurfs des Angemessenheitsbeschlusses zu konzentrieren und seine Analyse und Stellungnahme dazu abzugeben. Bei der Analyse des Rechts und der Praxis eines Drittlandes, das bis vor Kurzem noch ein Mitgliedstaat der EU war, ist es naheliegend, dass der EDSA viele Aspekte als der Sache nach gleichwertig erkannt hat. Angesichts seiner Rolle im Verfahren zur Annahme eines Angemessenheitsbeschlusses und des Umfangs der zu analysierenden Rechtsvorschriften und Praktiken hat der EDSA seine Aufmerksamkeit auf die Aspekte gerichtet, bei denen er den größten Bedarf für eine genauere Betrachtung sah.

19. Der EDSA hat den geltenden europäischen Datenschutzrahmen berücksichtigt, darunter die Artikel 7, 8 und 47 der Charta der Grundrechte der Europäischen Union (im Folgenden „EU-Charta“), die das Recht auf Privat- und Familienleben, das Recht auf den Schutz personenbezogener Daten und das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren schützen, sowie Artikel 8 der Europäischen Menschenrechtskonvention (im Folgenden „EMRK“), der das Recht auf Privat- und Familienleben schützt. Darüber hinaus hat der EDSA die Anforderungen der Richtlinie zum Datenschutz bei der Strafverfolgung berücksichtigt und sich mit der einschlägigen Rechtsprechung befasst.

20. Ziel dieses Verfahrens ist es, der Europäischen Kommission eine Stellungnahme für die Bewertung der Angemessenheit des Schutzniveaus im Vereinigten Königreich vorzulegen. Der Begriff „angemessenes Schutzniveau“, der bereits im Rahmen der Richtlinie 95/46/EG existierte, wurde vom EuGH weiterentwickelt. Es sei an den Standard erinnert, der vom EuGH in der Rechtssache „Schrems I“ festgelegt wurde und der besagt, dass das „Schutzniveau“ im Drittland zwar „der Sache nach gleichwertig“ mit dem in der EU gewährleisteten Schutzniveau sein muss, doch „die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, [können sich] von denen unterscheiden (…), die in der Union herangezogen werden“.[10] Ziel ist es also nicht, die europäischen Vorschriften Punkt für Punkt wiederzugeben, sondern es geht vielmehr darum, die wesentlichen Kernanforderungen der zu prüfenden Vorschriften festzulegen. Angemessenheit kann durch eine Kombination von gegenüber den Betroffenen eingeräumten Rechten, bestimmten Pflichten für die Stellen, bei denen die Daten verarbeitet werden oder in deren Zuständigkeit die Verarbeitung der Daten fällt, und die Aufsicht durch unabhängige Behörden erreicht werden. Datenschutzvorschriften sind allerdings nur dann wirksam, wenn sie durchsetzbar sind und in der Praxis eingehalten werden. Daher gilt es nicht nur den Inhalt der geltenden Vorschriften für die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation zu beachten, sondern auch das System, mit dem die Wirksamkeit der Regeln sichergestellt werden soll. Effiziente Durchsetzungsmechanismen sind für die Wirksamkeit von Datenschutzvorschriften von wesentlicher Bedeutung.[11]

Committee, ISC) (Fußnote 245), die geringen Hürden für die Einreichung einer Beschwerde beim Gericht für Ermittlungsbefugnisse (Investigatory Powers Tribunal, IPT) und die Tatsache, dass es nicht ungewöhnlich ist, dass dieses Gericht feststellt, dass der Beschwerdeführer tatsächlich nie Gegenstand einer Untersuchung durch eine Behörde war (Fußnote 263), die Kombination von Befugnissen, die sich aus der Gesetzgebung und dem Common Law ergeben (Fußnote 52), die von der Regierung ausgeübten Vorrechte (Fußnote 62) sowie die Tatsache, dass es anderen Organisationen freisteht, die Grundsätze der Verwaltung von polizeilichen Informationen (Management of Police Information, MoPI) zu befolgen, wenn sie dies wünschen (Fußnote 86).

[10] Siehe Urteil des Gerichtshofs vom 6. Oktober 2015, Maximilian Schrems/Datenschutzbeauftragter, C-362/14, ECLI:EU:C:2015:650, Rn. 73 und 74 (im Folgenden „Schrems I“).

[11] Siehe die Empfehlungen 01/2021 des EDSA zu der Referenzgrundlage für den Begriff „Angemessenheit“ in der Richtlinie zum Datenschutz bei der Strafverfolgung, Ziffer 14, S. 5.

2.3 Allgemeine Bemerkungen und Bedenken

2.3.1 Vom Vereinigten Königreich eingegangene internationale Verpflichtungen

21. Gemäß Artikel 36 Absatz 2 Buchstabe c der Richtlinie zum Datenschutz bei der Strafverfolgung und der Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung[12] berücksichtigt die Europäische Kommission bei der Bewertung der Angemessenheit des Schutzniveaus eines Drittlands unter anderem die von dem betreffenden Drittland eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten sowie die Umsetzung derartiger Verpflichtungen. Außerdem sollte der Beitritt des Drittlands zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (im Folgenden „Übereinkommen Nr. 108“)[13] und dessen Zusatzprotokoll[14] berücksichtigt werden.

22. **Diesbezüglich begrüßt der EDSA, dass das Vereinigte Königreich der EMRK beigetreten ist und der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) unterliegt. Darüber hinaus ist das Vereinigte Königreich auch dem Übereinkommen Nr. 108 und dessen Zusatzprotokoll beigetreten, hat das Übereinkommen Nr. 108+[15] im Jahr 2018 unterzeichnet und arbeitet derzeit an dessen Ratifizierung.**

2.3.2 Mögliche zukünftige Divergenz des Datenschutzrahmens des Vereinigten Königreichs

23. Wie in Erwägungsgrund 171 des Entwurfs des Angemessenheitsbeschlusses erwähnt, muss die Europäische Kommission berücksichtigen, dass das Vereinigte Königreich mit dem Ende des im Austrittsabkommen[16] vorgesehenen Übergangszeitraums seine eigene Datenschutzregelung erlässt, anwendet und durchsetzt, und sobald die Überbrückungsregelung[17] gemäß Artikel FINPROV.10A des Handels- und Kooperationsabkommens zwischen der EU und dem Vereinigten Königreich[18] nicht mehr gilt, kann dies insbesondere Änderungen oder Ergänzungen des im Entwurf des Angemessenheitsbeschlusses bewerteten Datenschutzrahmens sowie andere relevante Entwicklungen nach sich ziehen.

---

[12] Siehe die Empfehlungen 01/2021 des EDSA zu der Referenzgrundlage für den Begriff „Angemessenheit“ in der Richtlinie zum Datenschutz bei der Strafverfolgung, Ziffer 24, S. 8.

[13] Siehe das Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) vom 28. Januar 1981.

[14] Siehe das am 8. November 2001 zur Unterzeichnung aufgelegte Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr.

[15] Siehe das Protokoll zur Änderung des Übereinkommens zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (im Folgenden „Übereinkommen Nr. 108+“) vom 18. Mai 2018.

[16] Abkommen über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft (ABl. L 29 vom 31.1.2020, S. 7).

[17] Das Ende des Übergangszeitraums wurde mit dem 31. Dezember 2020 festgelegt. Nach diesem Datum gilt das Unionsrecht im Vereinigten Königreich nicht mehr. Die „Überbrückungsfrist“ gilt bis höchstens 30. Juni 2021 und entspricht dem Zeitraum, in dem die Übertragung personenbezogener Daten aus der EU in das Vereinigte Königreich noch nicht als Übermittlung gilt.

[18] Siehe das Handels- und Kooperationsabkommen zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits (ABl. L 444 vom 31.12.2020, S. 14).

24. Die Europäische Kommission hat daher beschlossen, eine Verfallsklausel in ihren Entwurf des Angemessenheitsbeschlusses[19] aufzunehmen, nach der der angenommene Beschluss vier Jahre nach seinem Inkrafttreten seine Gültigkeit verliert.

25. Es sei darauf hingewiesen, dass der Datenschutzrahmen des Vereinigten Königreichs in Zukunft erheblich von dem der EU abweichen kann, sollten die Minister und der Secretary of State des Vereinigten Königreichs von der Möglichkeit Gebrauch machen, nach dem Ende der Überbrückungsfrist sekundäre Rechtsvorschriften einzuführen.

26. Schließlich ist das Vereinigte Königreich seit dem Ende des Übergangszeitraums nicht mehr an die Rechtsprechung des EuGH gebunden und muss sich auch nicht mehr an die bereits angenommenen Urteile des EuGH, die im Rechtsrahmen des Vereinigten Königreichs als beibehaltene Rechtsprechung betrachtet werden, halten, da das Vereinigte Königreich die Möglichkeit hat, beibehaltenes Unionsrecht nach Ablauf der Überbrückungsfrist zu ändern, und sein Oberster Gerichtshof nicht an eine beibehaltene EU-Rechtsprechung gebunden ist.[20]

27. **In Anbetracht der Risiken, die durch eine mögliche Abweichung des Datenschutzrahmens des Vereinigten Königreichs vom EU-Besitzstand nach dem Ende der Überbrückungsfrist entstehen könnten, begrüßt der EDSA die Entscheidung der Europäischen Kommission, in den Entwurf des Angemessenheitsbeschlusses eine Klausel über dessen Verfall nach vier Jahren aufzunehmen. Der EDSA möchte in diesem Zusammenhang allerdings die Bedeutung der Überwachungsfunktion der Europäischen Kommission hervorheben.**[21] Die Europäische Kommission sollte alle relevanten Entwicklungen im Vereinigten Königreich, die sich auf die wesentliche Gleichwertigkeit des Schutzniveaus der personenbezogenen Daten auswirken könnten, die seit dem Inkrafttreten des Angemessenheitsbeschlusses zum Vereinigten Königreich übermittelt wurden, kontinuierlich und dauerhaft überwachen. **Darüber hinaus sollte die Europäische Kommission geeignete Maßnahmen ergreifen, um den Angemessenheitsbeschluss entsprechend den vorliegenden Umständen auszusetzen, zu ändern oder aufzuheben, wenn es nach Erlass des Angemessenheitsbeschlusses Hinweise darauf gibt, dass ein angemessenes Schutzniveau im Vereinigten Königreich nicht mehr gewährleistet ist.**

28. Der EDSA wird seinerseits nach besten Kräften die Europäische Kommission über alle einschlägigen Maßnahmen der Datenschutzaufsichtsbehörden der Mitgliedstaaten informieren, insbesondere in Bezug auf Beschwerden von betroffenen Personen in der EU über die Übermittlung personenbezogener Daten aus der EU in das Vereinigte Königreich.

3 VORSCHRIFTEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN DURCH DIE ZUSTÄNDIGEN BEHÖRDEN ZU STRAFVERFOLGUNGSZWECKEN

3.1 Sachlicher Anwendungsbereich

29. In Bezug auf die Erwägungsgründe 24 ff des Entwurfs des Angemessenheitsbeschlusses merkt der EDSA an, dass der Entwurf des Angemessenheitsbeschlusses kaum Einzelheiten zu den Tätigkeiten und

[19] Siehe Artikel 4 des Entwurf des Angemessenheitsbeschlusses. Siehe auch Erwägungsgrund 172 des Entwurfs des Angemessenheitsbeschlusses.
[20] Siehe Paragraf 6 Absätze 3 bis 6 des European Union (Withdrawal) Act 2018.
[21] Siehe Artikel 36 Absatz 4 der Richtlinie zum Datenschutz bei der Strafverfolgung.

dem Rechtsrahmen enthält, die für andere mit Strafverfolgungsaufgaben befasste Stellen als die Polizei gelten.

30. Im erklärenden Rahmen für Angemessenheitsdiskussionen des Vereinigten Königreichs (UK Explanatory Framework for Adequacy Discussions) wird beispielsweise in Abschnitt F zum Thema Strafverfolgung[22] auf Seite 11 darauf hingewiesen, dass die **National Crime Agency** (NCA) eine Strafverfolgungsbehörde von besonderer Bedeutung sein könnte, die unter anderem eine umfassendere Funktion in Bezug auf Informationen zur Strafverfolgung hat. Der NCA zufolge besteht ihre Aufgabe darin, aus einer Reihe von Quellen (darunter die technische Überwachung von Kommunikationsvorgängen, Strafverfolgungspartner im Vereinigten Königreich und im Ausland sowie Sicherheits- und Nachrichtendienste) Informationen zusammenzuführen, um die Analysen, die Bewertungen und die taktischen Möglichkeiten zu maximieren.[23] Die NCA ist auch einer der Hauptgesprächspartner für die internationalen Partner in der Strafverfolgung und spielt beim Austausch von Informationen zur Strafverfolgung eine wichtige Rolle.[24]

31. Der EDSA nimmt ferner zur Kenntnis, dass die Regierungsbehörde Government Communications Headquarters (im Folgenden „GCHQ“), deren Tätigkeiten normalerweise in den Anwendungsbereich von Teil 4 des Datenschutzgesetzes von 2018 (d. h. in den Bereich der nationalen Sicherheit) fallen, auch eine aktive Rolle dabei spielt, den gesellschaftlichen und finanziellen Schaden zu verringern, der im Vereinigten Königreich durch schwere und organisierte Kriminalität verursacht wird. Dabei arbeitet sie eng mit dem Innenministerium, der NCA, der Steuer und Zollbehörde (HM Revenue and Customs, HMRC) und anderen Regierungsabteilungen zusammen.[25] Ihre Tätigkeiten beziehen sich auf die Bekämpfung des sexuellen Missbrauchs von Kindern sowie von Betrug, anderen Arten von Wirtschaftskriminalität einschließlich Geldwäsche, kriminellem Einsatz von Technologie,

[22] Siehe den erklärenden Rahmen für Angemessenheitsdiskussionen des Vereinigten Königreichs (UK Explanatory Framework for Adequacy Discussions), Abschnitt F zum Thema Strafverfolgung, 13. März 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[23] Siehe die Website der National Crime Agency unter „Intelligence: enhancing the picture of serious organised crime affecting the UK“, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[24] Zwar handelt es sich nicht bei allen von der NCA verarbeiteten Informationen um personenbezogene Daten, aber ein erheblicher Teil könnte aus personenbezogenen Informationen bestehen, und die hier beschriebenen Tätigkeiten unterscheiden sich von denen der klassischen Polizeiarbeit, sodass eine Bewertung des Zugangs zu personenbezogenen Daten durch Strafverfolgungsbehörden im Vereinigten Königreich ohne eine gründliche Bewertung der Tätigkeiten der NCA unvollständig wäre. Es erscheint sinnvoll, dafür zu sorgen, dass den Datenschutzgrundsätzen in allen relevanten Strafverfolgungsbehörden die gleiche Bedeutung beigemessen wird, und daher das Augenmerk auf eine besonders datengesteuerte Behörde wie die NCA zu werfen. Darüber hinaus heißt es unter dem Zwischentitel „Blick auf die Zukunft“ weiter: „Wir suchen laufend nach neuen Möglichkeiten, traditionelle Fähigkeiten zu bündeln, zu entwickeln und zu verbessern, um die Quantität und Qualität der zur Nutzung sowohl im Vereinigten Königreich als auch im Ausland bereitstehenden Informationen zu erhöhen. Im Rahmen dessen entwickeln wir eine neue nationale Datenverwertungskapazität (National Data Exploitation Capability), die die Befugnisse nutzt, die der Behörde durch den Crime and Courts Act übertragen wurden, um Daten, die in allen Regierungsstellen vorhanden sind, miteinander zu verbinden, darauf zuzugreifen und sie zu verwerten. […] All dies wird unsere Agilität und Flexibilität erhöhen, mit der wir auf neue Bedrohungen reagieren und proaktiv agieren können und mit der wir Informationen und Erkenntnisse über aufkommende Bedrohungen sammeln und analysieren können, um Maßnahmen zu ergreifen, bevor Bedrohungen in die Tat umgesetzt werden.“

[25] Siehe die Website der GCHQ unter „Mission“ und „Serious and Organised Crime“, https://www.gchq.gov.uk/section/mission/serious-crime.

Cyberkriminalität, organisierter Schleuserkriminalität einschließlich Menschenhandel sowie von Schmuggel mit Drogen, Schusswaffen und anderen illegalen Waren.

32. **Der EDSA empfiehlt der Europäischen Kommission, ihre Analyse durch eine Analyse der im Bereich der Strafverfolgung tätigen Agenturen (und insbesondere der NCA) zu ergänzen, die den Schwerpunkt ihrer täglichen Arbeit offenbar auf das Sammeln und Analysieren von Daten, einschließlich personenbezogener Daten, legen. Darüber hinaus rät der EDSA der Kommission, Agenturen wie die GCHQ, deren Tätigkeiten sowohl in den Bereich der Strafverfolgung als auch in den Bereich der nationalen Sicherheit fallen, und den für sie geltenden Rechtsrahmen für die Verarbeitung personenbezogener Daten genauer zu untersuchen.**

3.2 Garantien, Rechte und Pflichten

3.2.1 Verarbeitung auf der Grundlage einer „Einwilligung" der betroffenen Person

33. Der EDSA nimmt zur Kenntnis, dass die Europäische Kommission in den Erwägungsgründen 37 und 38 des Entwurfs des Angemessenheitsbeschlusses erklärt, dass die **Berufung auf die Einwilligung** in einem Angemessenheitsszenario nicht als relevant angesehen wird, da Daten in Übermittlungssituationen nicht direkt durch eine Strafverfolgungsbehörde des Vereinigten Königreichs von einer betroffenen Person auf der Grundlage einer Einwilligung erhoben werden.

34. In diesem Zusammenhang erinnert der EDSA daran, dass nach Artikel 36 Absatz 2 Buchstabe a der Richtlinie zum Datenschutz bei der Strafverfolgung eine Reihe von Elementen zu bewerten ist, die nicht auf die Übermittlungssituation beschränkt sind, darunter „die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die (…) geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, auch in Bezug auf (…) das Strafrecht".

35. In einem Strafverfolgungskontext kann die Einwilligung als Rechtsgrundlage für die Datenverarbeitung, als zusätzliche Garantie oder ganz allgemein als Grundlage für die Ausübung von Ermittlungsbefugnissen, die zur Erfassung personenbezogener Daten führen, relevant sein. Dies gilt beispielsweise für die Einwilligung einer dritten Person zur Durchsuchung ihrer Räumlichkeiten oder zur Beschlagnahme von Datenspeichern.

36. Diesbezüglich möchte der EDSA (auch auf der Grundlage der von der Europäischen Kommission in Erwägungsgrund 38 des Entwurfs des Angemessenheitsbeschlusses erteilten Informationen) anmerken, dass die Verwendung der Einwilligung, wie sie in der Regelung des Vereinigten Königreichs enthalten ist, immer eine Rechtsgrundlage erfordern würde. Das bedeutet, dass selbst wenn die Polizei gesetzlich befugt ist, die Daten zum Zweck einer strafrechtlichen Ermittlung zu verarbeiten, sie es unter bestimmten Umständen (z. B. zur Entnahme einer DNA-Probe) für angemessen halten kann, die Einwilligung der betroffenen Person einzuholen.

37. Der EDSA empfiehlt der Europäischen Kommission, bei der Beurteilung der Angemessenheit eines Drittlandes im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung generell die mögliche Verwendung der Einwilligung in einem Strafverfolgungskontext zu analysieren.

3.2.2 Rechte des Einzelnen

3.2.2.1 Nationale Sicherheitsbescheinigungen („National Security Certificates")

38. Gemäß Paragraf 79 des Datenschutzgesetzes von 2018 können die für die Verarbeitung Verantwortlichen nationale Sicherheitsbescheinigungen beantragen, die von einem Minister, einem Mitglied des Kabinetts, dem Generalstaatsanwalt oder dem Generalanwalt für Schottland ausgestellt

werden und in denen bescheinigt wird, dass die in Teil 3 Kapitel 3 und 4 des Datenschutzgesetzes von 2018 verankerten Einschränkungen von Pflichten und Rechten eine notwendige und verhältnismäßige Maßnahme zum Schutz der nationalen Sicherheit darstellen.

39. Diese Bescheinigungen sollen den Verantwortlichen mehr Rechtssicherheit geben und ein unwiderlegbarer Beweis für die Tatsache sein, dass bei der Verarbeitung personenbezogener Daten der Aspekt der nationalen Sicherheit Anwendung findet. Es sollte jedoch erwähnt werden, dass diese Bescheinigungen kein Erfordernis bei Einschränkungen, die unter Berufung auf die Notwendigkeit der Wahrung der nationalen Sicherheit erfolgen, sind, sondern vielmehr eine Transparenzmaßnahme darstellen.[26]

40. Der EDSA entnimmt dem Anhang 20 Paragrafen 17 und 18 des Datenschutzgesetzes von 2018, dass eine nach dem Datenschutzgesetz von 1998 ausgestellte nationale Sicherheitsbescheinigung (im Folgenden „alte Bescheinigung“) nach dem Datenschutzgesetz von 2018 eine verlängerte Wirkung für die Verarbeitung personenbezogener Daten bis zum 25. Mai 2019 besaß. Bis zu diesem Datum wurden die alten Bescheinigungen, sofern sie nicht ersetzt oder widerrufen wurden, so behandelt, als wären sie gemäß dem Datenschutzgesetz von 2018 ausgestellt worden. Wenn es jedoch kein ausdrückliches Ablaufdatum auf einer nationalen Sicherheitsbescheinigung gibt, die gemäß dem Datenschutzgesetz von 1998 ausgestellt wurde, geht der EDSA davon aus, dass eine solche Bescheinigung sich weiterhin auf die Verarbeitung gemäß dem Datenschutzgesetz von 1998 auswirkt, sofern diese Bescheinigung nicht widerrufen oder aufgehoben wird.[27] Der durch diese alten Bescheinigungen gewährte Schutz ist auf die Verarbeitung personenbezogener Daten nach dem Datenschutzgesetz von 1998 beschränkt. Gleichwohl stellt der EDSA fest, dass für personenbezogene Daten, die gemäß dem Datenschutzgesetz von 1998 verarbeitet wurden, neue nationale Sicherheitsbescheinigungen nach dem Datenschutzgesetz von 1998 ausgestellt werden können.[28]

41. **Der EDSA empfiehlt der Europäischen Kommission, in ihrem Entwurf des Angemessenheitsbeschlusses der Vollständigkeit halber klarzustellen, dass nationale Sicherheitsbescheinigungen weiterhin nach dem Datenschutzgesetz von 1998 ausgestellt werden können. Darüber hinaus rät der EDSA der Europäischen Kommission, in ihrem Entwurf des Angemessenheitsbeschlusses die Rechtsbehelfs- und Aufsichtsmechanismen für die gemäß dem Datenschutzgesetz von 1998 ausgestellten Bescheinigungen zu beschreiben. Ferner empfiehlt der EDSA der Europäischen Kommission, in ihren Entwurf des Angemessenheitsbeschlusses die Zahl der bestehenden gemäß dem Datenschutzgesetz von 1998 ausgestellten Bescheinigungen aufzunehmen und diesen Aspekt aufmerksam zu überwachen.**

3.2.2.2 Automatisierte Entscheidungsfindung nach der Richtlinie zum Datenschutz bei der Strafverfolgung

42. Der EDSA betont, dass nach Artikel 11 Absatz 3 der Richtlinie zum Datenschutz bei der Strafverfolgung jedes Profiling verboten ist, das zur Folge hat, dass natürliche Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden. Der EDSA stellt jedoch fest,

[26] Siehe Innenministerium des Vereinigten Königreichs, Datenschutzgesetz von 2018, Hinweise zu den „National Security Certificates“, August 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf, S. 4.

[27] Siehe Innenministerium des Vereinigten Königreichs, Datenschutzgesetz von 2018, Hinweise zu den „National Security Certificates“, August 2020, S. 5.

[28] Siehe Innenministerium des Vereinigten Königreichs, Datenschutzgesetz von 2018, Hinweise zu den „National Security Certificates“, August 2020, S. 5.

dass in Paragraf 50 des Datenschutzgesetzes von 2018, in dem die spezifischen Regeln für die automatisierte Entscheidungsfindung festgelegt sind, kein solches Verbot vorgesehen ist.

43. **Der EDSA ersucht die Europäische Kommission daher, diesen Punkt zu überprüfen und ihre Ergebnisse in ihrem Angemessenheitsbeschluss ausdrücklich zu vermerken. Darüber hinaus empfiehlt der EDSA der Europäischen Kommission, Fälle im Zusammenhang mit automatisierter Entscheidungsfindung und Profiling genau zu überwachen.**

44. In der Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung heißt es: „Im Recht des Drittlandes sollten in jedem Fall die erforderlichen Garantien für die Rechte und Freiheiten der betroffenen Person vorgesehen sein. In dieser Hinsicht sollte zudem berücksichtigt werden, ob ein Mechanismus existiert, mit dem die zuständigen Behörden des jeweiligen Mitgliedstaats über jede Weiterverarbeitung der übermittelten Daten – beispielsweise für ein umfangreiches Profiling – unterrichtet werden können."[29]

45. **Der EDSA ersucht die Kommission, dieses Element im Lichte der in der Referenzgrundlage des EDSA gegebenen Hinweise zu bewerten.**

3.2.3 Weiterübermittlungen

46. Gemäß der Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung darf die Weiterübermittlung personenbezogener Daten durch den ursprünglichen Empfänger an ein anderes Drittland oder eine andere internationale Organisation das in der Union gebotene Schutzniveau für natürliche Personen, deren Daten übermittelt werden, nicht untergraben. Daher sollte eine Weiterübermittlung von Daten nur dann zulässig sein, wenn der Fortbestand des nach Unionsrecht gebotenen Schutzniveaus gewährleistet ist. Der EDSA ist der Ansicht, dass – wie von der Europäischen Kommission in ihrer Bewertung hervorgehoben – die Bestimmungen in Teil 3 Kapitel 5 des Datenschutzgesetzes von 2018 und insbesondere in Paragraf 73 im Prinzip ein Schutzniveau bieten, das dem nach Unionsrecht garantierten Schutzniveau der Sache nach gleichwertig ist, wenn es um die Übermittlung personenbezogener Daten von einer Strafverfolgungsbehörde des Vereinigten Königreichs in ein Drittland geht.

47. Erstens sieht Paragraf 73 Absatz 1 Buchstabe b des Datenschutzgesetzes von 2018 ausdrücklich vor, dass ein Verantwortlicher personenbezogene Daten nicht an ein Drittland oder eine internationale Organisation übermitteln darf, es sei denn, die personenbezogenen Daten wurden dem Verantwortlichen oder einer anderen zuständigen Behörde ursprünglich von einem anderen Mitgliedstaat als dem Vereinigten Königreich übermittelt oder auf andere Weise zur Verfügung gestellt und dieser Mitgliedstaat oder eine in diesem Mitgliedstaat ansässige Person, die für die Zwecke der Richtlinie zum Datenschutz bei der Strafverfolgung eine zuständige Behörde ist, hat die Übermittlung im Einklang mit den Rechtsvorschriften des Mitgliedstaats genehmigt. Diese Bestimmungen scheinen im Einklang mit der Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung zu stehen, welche vorsieht, dass auch zu berücksichtigen ist, ob ein Mechanismus existiert, mit dem die zuständigen Behörden des jeweiligen Mitgliedstaats über eine solche Weiterübermittlung von Daten unterrichtet werden und diese genehmigen. Der ursprüngliche Empfänger der aus der EU übermittelten Daten sollte dafür haften und in der Lage sein, nachzuweisen, dass die zuständige Behörde des Mitgliedstaats die Weiterübermittlung genehmigt hat und dass in Ermangelung eines Angemessenheitsbeschlusses in Bezug auf das Drittland, in das die Daten weiterübermittelt werden sollen, angemessene Garantien für die Weiterübermittlung von Daten

[29] Siehe die Empfehlungen 01/2021 des EDSA zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung, Ziffern 59–61.

vorgesehen sind. „In diesem Zusammenhang sollte berücksichtigt werden, ob eine Pflicht oder eine Selbstverpflichtung zur Anwendung einschlägiger, von den Behörden der übertragenden Mitgliedstaaten festgelegter Bearbeitungskodizes besteht."[30]

48. **Der EDSA empfiehlt der Kommission, dieses Element im Lichte der vom EDSA in dessen Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung gegebenen Hinweise zu bewerten.**

49. Zweitens ist der Secretary of State des Vereinigten Königreichs, wie in Erwägungsgrund 81 des Entwurfs des Angemessenheitsbeschlusses erläutert, befugt, einem Drittland (oder einem Gebiet oder einem Sektor innerhalb eines Drittlands), einer internationalen Organisation oder einer Beschreibung eines solchen Landes, Gebiets, Sektors oder einer solchen Organisation nach Konsultation des ICO ein angemessenes Schutzniveau für personenbezogene Daten zu bescheinigen.[31] Bei der Prüfung der Angemessenheit des Schutzniveaus muss der Secretary of State des Vereinigten Königreichs dieselben Elemente berücksichtigen, die die Europäische Kommission gemäß Artikel 36 Absatz 2 Buchstaben a bis c der Richtlinie zum Datenschutz bei der Strafverfolgung – in Verbindung mit Erwägungsgrund 67 der Richtlinie zum Datenschutz bei der Strafverfolgung und der beibehaltenen EU-Rechtsprechung – zu prüfen hat. Maßgeblicher Standard bei der Prüfung des Schutzniveaus eines Drittlandes auf dessen Angemessenheit wird mithin sein, ob das betreffende Drittland ein Schutzniveau gewährleistet, das dem im Vereinigten Königreich gewährleisteten Schutzniveau „der Sache nach gleichwertig" ist. Der EDSA nimmt zur Kenntnis, dass das Vereinigte Königreich im Rahmen des Datenschutzgesetzes von 2018 Gebieten ein angemessenes Schutzniveau im Sinne des Datenschutzrahmens des Vereinigten Königreichs bescheinigen kann, möchte jedoch hervorheben, dass diese Gebiete möglicherweise noch nicht von einem Angemessenheitsbeschluss der Europäischen Kommission erfasst sind, mit dem ein Schutzniveau anerkannt wird, das dem in der EU garantierten Schutzniveau „der Sache nach gleichwertig" ist. Dies könnte zu Risiken beim Schutz der aus der EU übermittelten personenbezogenen Daten führen, insbesondere wenn der Datenschutzrahmen des Vereinigten Königreichs in Zukunft vom Besitzstand der Union abweichen sollte. Es sei angemerkt, dass das richtungsweisende „Schrems II"-Urteil des EuGH vom Juli 2020[32] zur Ungültigkeit der US-Privacy Shield-Beschlusses geführt hat, da der US-Rechtsrahmen nach Ansicht des EuGH kein dem Unionsrecht der Sache nach gleichwertiges Schutzniveau bietet. Das Vereinigte Königreich muss sich nicht mehr an die bereits angenommenen Urteile des EuGH, die im Rechtsrahmen des Vereinigten Königreichs als beibehaltene Rechtsprechung betrachtet werden, halten, da das Vereinigte Königreich die Möglichkeit hat, beibehaltenes Unionsrecht nach Ablauf der Überbrückungsfrist zu ändern, und sein Oberster Gerichtshof nicht an eine beibehaltene EU-Rechtsprechung gebunden ist.[33]

50. **Der EDSA empfiehlt der Europäischen Kommission daher, das Verfahren der Angemessenheitsbewertung und die Kriterien der Behörden des Vereinigten Königreichs in Bezug auf andere Drittländer genau zu überwachen, insbesondere in Bezug auf Drittländer, die von der EU im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung nicht als angemessen anerkannt werden.**

[30] Siehe die Empfehlungen 01/2021 des EDSA zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung, Ziffern 55-56.

[31] Siehe Paragraf 182 Absatz 2 des Datenschutzgesetzes von 2018. Siehe auch die Absichtserklärung über die Rolle des ICO in Bezug auf neue Bewertungen der Angemessenheit zum Vereinigten Königreich, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

[32] Siehe Urteil des Gerichtshofs vom 16. Juli 2020, Datenschutzbeauftragter/Facebook Ireland Ltd. und Maximilian Schrems, C-311/18, ECLI:EU:C:2020:559 (im Folgenden „Schrems II").

[33] Siehe Paragraf 6 Absätze 3 bis 6 des European Union (Withdrawal) Act 2018.

51. Für Fälle, in denen die Europäische Kommission zu dem Schluss gelangt, dass das vom Vereinigten Königreich für angemessen befundene Drittland gemäß Artikel 36 der Richtlinie zum Datenschutz bei der Strafverfolgung kein Schutzniveau bietet, das dem in der EU gewährleisteten der Sache nach gleichwertig ist, **empfiehlt der EDSA der Europäischen Kommission, alle erforderlichen Schritte zu unternehmen, beispielsweise die Änderung des Angemessenheitsbeschlusses zum Vereinigten Königreich, um spezifische Garantien für personenbezogene Daten, die aus der EU stammen, einzuführen, und/oder die Aussetzung des Angemessenheitsbeschlusses des Vereinigten Königreichs in Erwägung zu ziehen, wenn personenbezogene Daten, die aus der EU in das Vereinigte Königreich übermittelt werden, auf der Grundlage einer Angemessenheitsregelung des Vereinigten Königreichs in das betreffende Drittland weitergegeben werden.**

52. **Schließlich empfiehlt der EDSA in Bezug auf die internationalen Abkommen, die das Vereinigte Königreich abgeschlossen hat oder in Zukunft abschließen wird, und den möglichen Zugang von Behörden aus Drittländern, die Vertragsparteien solcher Abkommen sind, zu aus der EU stammenden personenbezogenen Daten, dass die Europäische Kommission das Zusammenspiel zwischen dem Datenschutzrahmen des Vereinigten Königreichs und dessen internationalen Verpflichtungen prüft, um insbesondere die Kontinuität des Schutzniveaus bei der Weiterübermittlung von personenbezogenen Daten, die aus der EU in das Vereinigte Königreich übermittelt wurden, auf der Grundlage eines Angemessenheitsbeschlusses des Vereinigten Königreichs in andere Drittländer sicherzustellen. In Bezug auf den Abschluss internationaler Abkommen zwischen dem Vereinigten Königreich und Drittländern, die das in der EU gebotene Schutzniveau für personenbezogene Daten zu untergraben drohen, sollte die Europäische Kommission für eine kontinuierliche Überwachung sorgen und erforderlichenfalls geeignete Maßnahmen ergreifen.** Die Europäische Kommission hat zwar beispielsweise auf die Tatsache verwiesen, dass sich der US Cloud Act[34] auf Weiterübermittlungen von Dienstleistern im Vereinigten Königreich in die USA auswirken kann, **doch möchte der EDSA hervorheben, dass sich das Inkrafttreten dieses Abkommens auch auf von Strafverfolgungsbehörden im Vereinigten Königreich vorgenommene Weiterübermittlungen auswirken kann, insbesondere in Bezug auf die Ausstellung und Übermittlung von Anordnungen gemäß Artikel 5 des US Cloud Act.**

53. Der EDSA ist außerdem der Ansicht, dass der Abschluss künftiger Abkommen mit Drittländern zum Zweck der Zusammenarbeit bei der Strafverfolgung, die eine Rechtsgrundlage für die Übermittlung personenbezogener Daten an diese Länder bieten, ebenfalls erhebliche Auswirkungen auf die Bedingungen für die Weitergabe der erhobenen Informationen haben kann, da sich solche Abkommen auf den Rechtsrahmen des Vereinigten Königreichs für den Datenschutz, wie er bewertet wurde, auswirken könnten.

54. **Der EDSA empfiehlt daher, dass die Europäische Kommission fortlaufend überwacht, ob sich der Abschluss künftiger Abkommen zwischen dem Vereinigten Königreich und Drittländern auf die Anwendung des Datenschutzrechts des Vereinigten Königreichs auswirken könnte, und dass sie weitere Beschränkungen oder Ausnahmen in Bezug auf die Weitergabe und die Weiterverwendung und Offenlegung von zu Strafverfolgungszwecken erhobenen Informationen gegenüber dem Ausland vorsieht. Der EDSA ist der Ansicht, dass solche Informationen und Bewertungen unerlässlich sind, um eine umfassende Überprüfung des Schutzniveaus zu ermöglichen, das durch den**

[34] Siehe das Abkommen zwischen der Regierung des Vereinigten Königreichs von Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugang zu elektronischen Daten für den Zweck der Bekämpfung schwerer Straftaten, Washington DC, USA, 3. Oktober 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

Rechtsrahmen des Vereinigten Königreichs und die Vorgehensweisen in Bezug auf die Offenlegung gegenüber dem Ausland gewährleistet wird.

55. Schließlich nimmt der EDSA zur Kenntnis, dass gemäß Paragraf 76 Absatz 4 Buchstabe b des Datenschutzgesetzes von 2018 (zum Thema Übermittlungen unter besonderen Umständen) Strafverfolgungsbehörden im Vereinigten Königreich personenbezogene Daten an ein Drittland oder eine internationale Organisation übermitteln können, wenn die Übermittlung „für die Einholung von Rechtsberatung in Bezug auf einen der Strafverfolgungszwecke erforderlich" ist. **Der EDSA betont, dass Artikel 38 der Richtlinie zum Datenschutz bei der Strafverfolgung keine entsprechende Bestimmung enthält. Er empfiehlt der Europäischen Kommission daher, klarzustellen, was unter Rechtsberatung zu verstehen ist und welche Arten von personenbezogenen Daten in solchen Fällen ausgetauscht werden.**

3.2.4 Weiterverarbeitung einschließlich Weitergabe für Zwecke der nationalen Sicherheit

56. In seiner Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung hatte der EDSA darauf hingewiesen, dass die Weiterverarbeitung oder Offenlegung von aus der EU übermittelten Daten zu anderen Zwecken als zu Strafverfolgungszwecken, z. B. zu Zwecken der nationalen Sicherheit, ebenfalls gesetzlich geregelt, erforderlich und verhältnismäßig sein sollte. Die Europäische Kommission gelangt bei ihrer Bewertung in ihrem Entwurf des Angemessenheitsbeschlusses zu dem Ergebnis, dass Paragraf 36 Absatz 3 des Datenschutzgesetzes von 2018 sowie das Gesetz von 2017 über die digitale Wirtschaft (Digital Economy Act), das Gesetz von 2013 über Straftaten und Gerichte (Crime and Courts Act) und das Gesetz von 2017 über schwere Straftaten (Serious Crime Act) einen klaren Rechtsrahmen bilden, der die Weitergabe von Daten unter der Voraussetzung ermöglicht, dass eine solche Weitergabe im Einklang mit den im Datenschutzgesetz von 2018 festgelegten Regeln erfolgt.

57. Der EDSA stellt diesbezüglich fest, dass im Zusammenhang mit aus der EU übermittelten personenbezogenen Daten, die zu anderen Zwecken weiterverarbeitet werden, von der Europäischen Kommission nicht bewertet wurde, ob etwaige Mechanismen existieren, mit denen die Strafverfolgungsbehörden des Vereinigten Königreichs die zuständigen Behörden des jeweiligen Mitgliedstaats über eine mögliche Weiterverarbeitung von Daten unterrichten können. In der Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung wird dies jedoch als ein Element betrachtet, das berücksichtigt werden muss.[35] Darüber hinaus wird auch die Existenz eines solchen Mechanismus zur Unterrichtung der zuständigen Behörden des jeweiligen Mitgliedstaats über die Weiterverarbeitung von Daten zu Strafverfolgungszwecken als ein Element betrachtet, das gemäß der Referenzgrundlage zur Angemessenheit nach der Richtlinie zum Datenschutz bei der Strafverfolgung zu berücksichtigen ist.[36]

58. **Der EDSA ersucht die Europäische Kommission daher, ihre Analyse um Informationen über die Existenz etwaiger Mechanismen, mit denen die Strafverfolgungsbehörden des Vereinigten Königreichs die zuständigen Behörden der jeweiligen Mitgliedstaaten über eine mögliche Weiterverarbeitung von aus der EU übermittelten Daten unterrichten können, zu ergänzen.**

59. Maßgebliche Rechtsgrundlage, die die Weitergabe von Daten, die von einer Strafverfolgungsbehörde erhoben wurden, an einen Nachrichtendienst für die Zwecke der nationalen Sicherheit erlaubt, ist das Gesetz von 2008 zur Terrorismusbekämpfung (Counter-terrorism Act). In diesem Zusammenhang stellt

[35] Siehe die Empfehlungen 01/2021 des EDSA zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung, Ziffer 41 und Fußnote 39.
[36] Siehe die Empfehlungen 01/2021 des EDSA zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung, Ziffer 40.

der EDSA fest, dass der Anwendungsbereich und die Bestimmungen von Paragraf 19 des Counter-terrorism Act 2008 in der Bewertung der Europäischen Kommission nicht vollständig behandelt werden. Diese implizieren nämlich möglicherweise eine breiter gefasste Weiterverwendung, insbesondere im Hinblick auf Paragraf 19 Absatz 2 des Counter-terrorism Act 2008, wonach Informationen, die einer der Nachrichtendienste in Ausübung einer seiner Aufgaben erlangt hat, von diesem Dienst bei der Ausübung einer seiner anderen Aufgaben verwendet werden können. Diesbezüglich betont der EDSA, dass für die Daten bei der Weiterverarbeitung oder Offenlegung das gleiche Schutzniveau gelten muss wie bei ihrer ursprünglichen Verarbeitung durch die empfangende zuständige Behörde.

3.3 Aufsicht und Durchsetzung

60. Der EDSA stellt fest, dass die Aufsicht über die Strafverfolgungsbehörden neben dem ICO durch eine Kombination verschiedener Beauftragter (Commissioners) gewährleistet wird. Im Entwurf des Angemessenheitsbeschlusses werden der Beauftragte für Untersuchungsbefugnisse (Investigatory Powers Commissioner, im Folgenden „IPC“), der Beauftragte für die Speicherung und Verwendung von biometrischem Material sowie der Beauftragte für Überwachungskameras erwähnt. In diesem Zusammenhang sei darauf hingewiesen, dass der EuGH wiederholt betont hat, dass die Aufsicht unabhängig sein muss. Der IPC ist im Falle des Zugangs zu personenbezogenen Daten, die in das Vereinigte Königreich übermittelt werden, von besonderer Bedeutung. Nach dem Verständnis des EDSA handelt es sich bei dem IPC um einen der sogenannten Justizbeauftragten (Judicial Commissioners), auf die im Zusammenhang mit dem Kapitel über die nationale Sicherheit Bezug genommen wird und die auch bei ihrer Tätigkeit als Beauftragte richterliche Unabhängigkeit genießen. Was das Amt des IPC betrifft, so erklärt die Europäische Kommission in Erwägungsgrund 245 des Entwurfs des Angemessenheitsbeschlusses, dass der IPC unabhängig als „arm's length body“ tätig ist, aber vom Innenministerium finanziert wird.

61. Darüber hinaus ist der IPC auch für die Ex-post-Beaufsichtigung von Überwachungsmaßnahmen zuständig. Es scheint jedoch, dass die Rolle des IPC in dieser Funktion darin besteht, bei Verstößen Empfehlungen auszusprechen und die betroffene Person zu benachrichtigen, wenn es sich um einen schwerwiegenden Fehler handelt und es im öffentlichen Interesse liegt, dass die Person informiert wird.

62. Der EDSA hat in dem Entwurf des Angemessenheitsbeschlusses keine weiteren Anhaltspunkte für die Bewertung der Unabhängigkeit des Beauftragten für die Speicherung und Verwendung von biometrischem Material sowie des Beauftragten für Überwachungskameras gefunden.

63. **Die Europäische Kommission wird ersucht, die Unabhängigkeit der Justizbeauftragten weiter zu bewerten, auch in Bezug auf Fälle, in denen der Beauftragte nicht (mehr) als Richter tätig ist, und die Unabhängigkeit des Beauftragten für die Speicherung und Verwendung von biometrischem Material sowie des Beauftragten für Überwachungskameras zu bewerten.**