Stellungnahme 14/2021 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich

Angenommen am 13. April 2021

INHALTSVERZEICHNIS

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 70 Absatz 1 Buchstabe s 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 und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden „DSGVO“ oder „EU-DSGVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum (im Folgenden „EWR“), insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung,[1]

gestützt auf die Artikel 12 und Artikel 22 seiner Geschäftsordnung –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. ZUSAMMENFASSUNG

1. Die Europäische Kommission billigte ihren Entwurf eines Durchführungsbeschlusses (im Folgenden „Beschlussentwurf“) über die Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich gemäß der DSGVO am 19. Februar 2021.[2] Daraufhin leitete die Europäische Kommission das Verfahren für seine förmliche Annahme ein.

2. Am selben Tag ersuchte die Europäische Kommission den Europäischen Datenschutzausschuss (im Folgenden „EDSA“) um eine Stellungnahme.[3] Der EDSA stützte seine Bewertung der Angemessenheit des im Vereinigten Königreich gewährten Schutzniveaus auf eine Prüfung des Beschlussentwurfs selbst sowie auf eine Auswertung der von der Europäischen Kommission bereitgestellten Unterlagen.

3. In den Mittelpunkt seiner Bewertung stellte der EDSA sowohl die allgemeinen auf die DSGVO bezogenen Aspekte des Beschlussentwurfs als auch den Zugriff von Behörden auf personenbezogene Daten, die aus dem EWR für Zwecke der Strafverfolgung und der nationalen Sicherheit übermittelt werden, einschließlich der Rechtsbehelfe, die Personen im EWR zur Verfügung stehen. Der EDSA prüfte auch, ob die im Rechtsrahmen des Vereinigten Königreichs vorgesehenen Garantien tatsächlich vorhanden und wirksam sind.

4. Als Maßstab für diese Prüfungsarbeit hat der EDSA seine im Februar 2018 angenommene Referenzgrundlage für Angemessenheit im Sinne der DSGVO[4] sowie die Empfehlungen 02/2020 des

[1] Soweit in dieser Stellungnahme von Mitgliedstaaten die Rede ist, sind damit die Mitgliedstaaten des EWR gemeint.
[2] Siehe Pressemitteilung der Europäischen Kommission, Datenschutz: Europäische Kommission leitet Verfahren zu Übermittlungen personenbezogener Daten in das Vereinigte Königreich ein, 19. Februar 2021, https://ec.europa.eu/commission/presscorner/detail/de/ip_21_661.
[3] Ebd.
[4] Siehe die von der Artikel-29-Datenschutzgruppe veröffentlichte Referenzgrundlage für Angemessenheit, angenommen am 28. November 2017, zuletzt überarbeitet und angenommen am 6. Februar 2018, WP 254/rev.01 (vom EDSA gebilligt, siehe https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines; im Folgenden „Referenzgrundlage für Angemessenheit im Sinne der DSGVO“).

EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen[5] verwendet.

1.1 Konvergenzbereiche

5. Die zentrale Zielsetzung des EDSA besteht darin, der Europäischen Kommission eine Stellungnahme zur Angemessenheit des Schutzniveaus, das natürlichen Personen im Vereinigten Königreich gewährt wird, vorzulegen. Der EDSA erwartet ausdrücklich nicht, dass der Rechtsrahmen des Vereinigten Königreichs das europäische Datenschutzrecht nachbildet.

6. Der EDSA weist jedoch darauf hin, dass nach Artikel 45 DSGVO und nach der Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „EuGH“) die Rechtsvorschriften des Drittlandes an die in der DSGVO verankerten Grundsätze im Wesentlichen angeglichen sein müssen, damit davon ausgegangen werden kann, dass sie ein angemessenes Schutzniveau bieten. Der Datenschutzrahmen des Vereinigten Königreichs basiert weitgehend auf dem Datenschutzrahmen der EU (insbesondere auf der DSGVO und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates im Bereich von Justiz und Inneres, im Folgenden „JI-RL“), was darauf zurückzuführen ist, dass das Vereinigte Königreich bis zum 31. Januar 2020 Mitgliedstaat der EU war. Darüber hinaus wird mit dem britischen Data Protection Act von 2018 (Datenschutzgesetz), der am 23. Mai 2018 in Kraft getreten ist und mit dem der Data Protection Act von 1998 aufgehoben wurde, nicht nur die JI-RL umgesetzt, sondern auch die Anwendung der DSGVO im Recht des Vereinigten Königreichs näher spezifiziert; zudem werden der nationalen britischen Datenschutzaufsichtsbehörde – dem Information Commissioner's Office (im Folgenden „ICO“) – Befugnisse übertragen und Pflichten auferlegt. Daher erkennt der EDSA an, dass der Datenschutzrahmen im Vereinigten Königreich der DSGVO größtenteils entspricht.

7. **Bei der Analyse des Rechts und der Rechtspraxis eines Drittlands, das bis vor Kurzem Mitgliedstaat der EU gewesen ist, hat der EDSA erwartungsgemäß festgestellt, dass zahlreiche Aspekte der Sache nach gleichwertig sind.**

8. Im Bereich des Datenschutzes stellt der EDSA fest, dass es bei bestimmten Kernbestimmungen starke Angleichungen zwischen dem Rahmen der DSGVO und dem Rechtsrahmen des Vereinigten Königreichs gibt, beispielsweise in Bezug auf Begriffe (z. B. „personenbezogene Daten“, „Verarbeitung personenbezogener Daten”, „Verantwortlicher“), Gründe für die rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung für legitime Zwecke, Zweckbindung, Datenqualität und Verhältnismäßigkeit, Datenspeicherung, Sicherheit und Vertraulichkeit, Transparenz, besondere Kategorien personenbezogener Daten, Direktwerbung sowie automatisierte Entscheidungen und Profiling.

1.2 Herausforderungen

9. Da das Vereinigte Königreich bis vor Kurzem Mitgliedstaat der EU war, hat der EDSA bei der Analyse des Rechts und der Rechtspraxis des Landes festgestellt, dass viele Aspekte der Sache nach gleichwertig sind. Gleichzeitig hat der EDSA aufgrund seiner Funktion im Verfahren zur Annahme einer Angemessenheitsentscheidung, aber auch angesichts der Zeitknappheit beschlossen, sich auf

[5] Siehe EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, angenommen am 10. November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_de.

diejenigen Aspekte zu konzentrieren, bei denen er eine genauere Untersuchung und eine eingehendere Prüfung für erforderlich hält.

10. Dennoch gibt es nach wie vor Herausforderungen, und der EDSA ist der Auffassung, dass die nachfolgenden Punkte einer weiteren Bewertung bedürfen, um sicherzustellen, dass ein der Sache nach gleichwertiges Schutzniveau erreicht wird, und die Europäische Kommission diese Punkte im Vereinigten Königreich genau überwachen muss.

1.2.1 Allgemeines

11. Die erste Herausforderung ist allgemeiner Art und betrifft die Überwachung der Entwicklung des britischen Datenschutzrechts insgesamt. Die Regierung des Vereinigten Königreichs hat ihre Absicht bekundet, im Bereich des Datenschutzes separate und unabhängige Strategien zu entwickeln, um dabei möglicherweise vom Datenschutzrecht der EU abzuweichen. Zwar haben sich derartige politische Erklärungen bisher im Rechtsrahmen des Vereinigten Königreichs noch nicht niedergeschlagen, dennoch **könnte diese mögliche Abweichung in Zukunft die Aufrechterhaltung des Schutzniveaus für personenbezogene Daten, die aus der EU übermittelt werden, gefährden**. **Daher wird angeregt, dass die Europäische Kommission ab dem Inkrafttreten ihres Angemessenheitsbeschlusses diese Entwicklungen genau verfolgt und die erforderlichen Maßnahmen ergreift, einschließlich der Änderung und/oder der Aussetzung des Beschlusses.**

1.2.2 Allgemeine Aspekte des Datenschutzes

12. Zum einen ist die sogenannte **Ausnahmeregelung für den Bereich der Einwanderung** in **Anhang 2 Teil 1 Nummer 4 des Data Protection Act von 2018** weit gefasst. Sie gilt nämlich auch für den Fall, dass personenbezogene Daten nicht für den Zweck der Einwanderungskontrolle von einem Verantwortlichen erhoben werden, sondern von diesem einem anderen Verantwortlichen zur Verfügung gestellt werden, der die personenbezogenen Daten dann für den Zweck der Einwanderungskontrolle verarbeitet.

13. Der EDSA ersucht die Europäische Kommission, den Sachstand des Verfahrens Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) zu überprüfen und, da dieses Urteil nicht rechtskräftig (res judicata) ist, zu prüfen, ob es durch das Berufungsurteil bestätigt oder abgeändert wird, wobei alle etwaigen Aktualisierungen zu berücksichtigen sind, und es in dem Beschluss anzugeben. **Der EDSA ersucht die Kommission zudem, im Angemessenheitsbeschluss weitere Informationen über die Ausnahmeregelung für den Bereich der Einwanderung bereitzustellen[6], vor allem in Bezug auf die Erforderlichkeit und Verhältnismäßigkeit einer solch weit gefassten Ausnahmeregelung im Recht des Vereinigten Königreichs, insbesondere angesichts des weiten persönlichen Anwendungsbereichs.** Gleichzeitig empfiehlt der EDSA der Europäischen Kommission, noch weiter zu prüfen, ob zusätzliche Garantien im Rechtsrahmen des Vereinigten Königreichs vorgesehen sind oder in Erwägung gezogen werden könnten, beispielsweise durch rechtsverbindliche Instrumente, die die Ausnahmeregelung für den Bereich der Einwanderung ergänzen würden, indem deren Vorhersehbarkeit und die Garantien für die betroffenen Personen gestärkt würden, was auch eine

[6] Auch als Ergebnis der fortlaufenden Überprüfung der Anwendung der Ausnahmeregelung für den Bereich der Einwanderung, siehe Seite 5 der Veröffentlichung der Regierung des Vereinigten Königreichs *Explanatory Framework for Adequacy Discussions, Section E3: Schedule 2, Restrictions* vom 13. März 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

bessere und raschere Bewertung und Überwachung der Voraussetzungen der Erforderlichkeit und Verhältnismäßigkeit ermöglichen würde.

14. Zweitens erkennt der EDSA zwar an, dass das Vereinigte Königreich Kapitel V der DSGVO größtenteils in seinen eigenen Datenschutzrahmen übernommen hat, doch hat der EDSA festgestellt, dass bestimmte Aspekte des Rechtsrahmens des Vereinigten Königreichs **in Bezug auf die Weiterübermittlung** das Schutzniveau für personenbezogene Daten, die aus dem EWR übermittelt werden, untergraben könnten.

15. Laut Artikel 44 DSGVO[7] dürfen personenbezogene Daten nur übermittelt oder weiterübermittelt werden, wenn das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird. **Das bedeutet, dass die Rechtsvorschriften des Vereinigten Königreichs den EU-Rechtsvorschriften nicht nur in Bezug auf die Verarbeitung von in das Vereinigte Königreich auf Grundlage des künftigen Angemessenheitsbeschlusses übermittelten personenbezogenen Daten „der Sache nach gleichwertig" sein müssen, sondern dass auch durch die im Vereinigten Königreich geltenden Vorschriften für die Weiterübermittlung dieser Daten in Drittländer sichergestellt sein muss, dass ein der Sache nach gleichwertiges Schutzniveau fortlaufend gewährleistet wird.**

16. Zwar stellt der EDSA fest, dass das Vereinigte Königreich gemäß seinem Rechtsrahmen anerkennen kann, dass bestimmte Gebiete im Sinne des Datenschutzrahmens des Vereinigten Königreichs ein angemessenes Datenschutzniveau bieten, doch er weist auch darauf hin, dass für diese Gebiete bislang möglicherweise noch kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, wonach sie ein Schutzniveau gewährleisten würden, das dem im EWR garantierten Schutzniveau „der Sache nach gleichwertig" ist. Dies könnte zu möglichen Risiken beim Schutz personenbezogener Daten führen, die aus dem EWR übermittelt werden, insbesondere wenn der Datenschutzrahmen des Vereinigten Königreichs künftig vom EU-Besitzstand abweicht. Darüber hinaus hat das Vereinigte Königreich die Drittländer, für welche die Europäische Kommission bereits eine Angemessenheitsentscheidung gemäß der Richtlinie 95/46/EG[8] erlassen hat, schon als angemessen anerkannt, obwohl die Europäische Kommission diese Entscheidungen demnächst überprüfen wird und die Ergebnisse dieser Überprüfung noch nicht bekannt sind.

17. **In den oben genannten Fällen sollte die Europäische Kommission ihrer Überwachungsfunktion nachkommen, und falls das der Sache nach gleichwertige Schutzniveau für aus dem EWR übermittelte personenbezogene Daten nicht aufrechterhalten wird, sollte die Europäische Kommission in Erwägung ziehen, den Angemessenheitsbeschluss zu ändern, um besondere Garantien für aus dem EWR übermittelte Daten einzuführen, und/oder den Angemessenheitsbeschluss auszusetzen.**

18. **In Bezug auf internationale Übereinkünfte zwischen dem Vereinigten Königreich und Drittländern** wird die Europäische Kommission ersucht, die Wechselwirkungen zwischen dem

[7] „Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird."

[8] 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).

Datenschutzrahmen des Vereinigten Königreichs und dessen internationalen Verpflichtungen zu untersuchen, und zwar über das zwischen dem Vereinigten Königreich und den Vereinigten Staaten von Amerika (im Folgenden „USA“) geschlossene Abkommen über den Zugriff auf elektronische Daten zur Bekämpfung von schwerer Kriminalität[9] (im Folgenden „CLOUD-Act-Abkommen“) hinaus, um insbesondere den Fortbestand des Schutzniveaus sicherzustellen, wenn personenbezogene Daten auf der Grundlage des Angemessenheitsbeschlusses aus der EU in das Vereinigte Königreich übermittelt und anschließend in andere Drittländer weiterübermittelt werden, und fortlaufend zu überwachen, ob der Abschluss internationaler Übereinkünfte zwischen dem Vereinigten Königreich und Drittländern das in der EU vorgesehene Schutzniveau für personenbezogene Daten untergraben könnte, und erforderlichenfalls entsprechende Maßnahmen zu ergreifen.

19. Darüber hinaus wird die Europäische Kommission ersucht, zu überwachen, ob das CLOUD-Act-Abkommen geeignete zusätzliche Garantien bietet, unter Berücksichtigung des Sensibilitätsgrads der betroffenen Datenkategorien und der einzigen Anforderungen der Übermittlung elektronischer Beweismittel unmittelbar durch Diensteanbieter anstatt zwischen Behörden, und dabei auch zu bewerten, unter welchen Umständen durch eine geeignete Umsetzung der Anpassung des Rahmenabkommens zwischen der EU und den USA[10] Garantien geboten werden können.

20. Des Weiteren stellt der EDSA fest, dass Weiterübermittlungen aus dem Vereinigten Königreich in ein anderes Drittland auch mit **Übermittlungsinstrumenten gemäß den geltenden Datenschutzvorschriften des Vereinigten Königreichs**[11] erfolgen können. In Anbetracht des Urteils in der Rechtssache Schrems II[12] empfiehlt der EDSA der Europäischen Kommission, im Angemessenheitsbeschluss Zusicherungen für die wirksame Einführung notwendiger Garantien zu machen, auch unter Berücksichtigung der Rechtsvorschriften des empfangenden Drittlands.

21. In Bezug auf das Fehlen **von Schutzmaßnahmen gemäß Artikel 48 DSGVO** in den Rechtsvorschriften des Vereinigten Königreichs rät der EDSA der Europäischen Kommission, weitere Zusicherungen und spezifische Verweise auf die Rechtsvorschriften des Vereinigten Königreichs einzufügen, mit denen sichergestellt wird, dass das im Rechtsrahmen des Vereinigten Königreichs gewährleistete Schutzniveau dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist.

22. In Bezug auf **Verfahrens- und Durchsetzungsmechanismen** stellt der EDSA fest, dass das Bestehen und wirksame Funktionieren einer unabhängigen Aufsichtsbehörde und das Vorhandensein eines Systems, das ein hohes Maß an Konformität gewährleistet, sowie eines Systems für den Zugang zu geeigneten Rechtsschutzverfahren, natürlichen Personen im EWR die Möglichkeit bieten, ihre Rechte wahrzunehmen und Rechtsbehelfe einzulegen, ohne dabei auf große administrative und gerichtliche Hürden zu stoßen, Schlüsselelemente sind, die ein Datenschutzrahmen aufweisen muss , um mit dem Datenschutzrahmen der EU im Einklang zu stehen.

---

[9] Siehe das Abkommen zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugriff auf elektronische Daten zur Bekämpfung von schwerer Kriminalität, 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.

[10] Siehe das Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten vom Dezember 2016 (im Folgenden „Rahmenabkommen zwischen der EU und den USA“), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3A3104_8.

[11] Siehe Artikel 46 und 47 UK-DSGVO.

[12] Siehe Schrems II.

23. Der EDSA erkennt an, dass das Vereinigte Königreich die einschlägigen Bestimmungen der EU-DSGVO größtenteils in die DSGVO des Vereinigten Königreichs und in den Data Protection Act von 2018 übernommen hat; gleichwohl wird die Europäische Kommission ersucht, alle Entwicklungen im Rechtsrahmen und in der Praxis des Vereinigten Königreichs, die sich nachteilig auf diese Bereiche auswirken könnten, fortlaufend zu überwachen.

1.2.3 Zugriff von Behörden auf in das Vereinigte Königreich übermittelte Daten

24. Der EDSA nimmt die erheblichen Änderungen des britischen Rechtsrahmens für Sicherheits- und Nachrichtendienste zur Kenntnis, insbesondere in Bezug auf das Abfangen und Sammeln von Kommunikationsdaten. Der EDSA geht davon aus, dass es sich bei diesen Änderungen u. a. um eine Reaktion auf die beim EuGH und beim Europäischen Gerichtshof für Menschenrechte (im Folgenden „EGMR“) eingeleiteten Verfahren und die jüngsten Urteile in diesem Zusammenhang handelt.

25. Insbesondere begrüßt der EDSA, dass das Vereinigte Königreich das Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse, im Folgenden „IPT“) eingerichtet hat. Das IPT entscheidet nicht nur über Fälle betreffend die Ausübung von Ermittlungsbefugnissen durch Strafverfolgungsbehörden, sondern auch über Fälle betreffend die Ausübung von Ermittlungsbefugnissen durch Nachrichtendienste. Nach Auffassung des EDSA fungiert daher das IPT als ordentliches Gericht im Sinne von Artikel 47 der Charta der Grundrechte der Europäischen Union (im Folgenden „EU-Charta“).

26. Darüber hinaus begrüßt der EDSA die Einsetzung von Justizkommissaren durch den Investigatory Powers Act von 2016 (Gesetz über Ermittlungsbefugnisse, im Folgenden „IPA von 2016“) als wesentliche Verbesserung. Er geht davon aus, dass eine wichtige Funktion der Justizkommissare darin besteht, in Einzelfällen vorab unterschiedliche Überwachungsmaßnahmen zu genehmigen, darunter das gezielte Abfangen und das Sammeln von Massenkommunikationsdaten (sogenanntes Double-Lock-Verfahren).

27. Um die Wirksamkeit dieser zusätzlichen Aufsichtsebene bewerten zu können, hält es der EDSA jedoch für erforderlich, noch genauer zu klären, in welchen Szenarien ein rechtmäßiges Abfangen ohne Zustimmung des Investigatory Powers Commissioner (Kommissar mit Ermittlungsbefugnissen, im Folgenden „IPC“) oder der Justizkommissare möglich ist, und er empfiehlt der Europäischen Kommission, eingehender zu bewerten und nachzuweisen, dass der Rechtsrahmen des Vereinigten Königreichs geeignete Garantien bietet, unter anderem durch wirksame Ex-post-Aufsicht und Rechtsbehelfsmöglichkeiten für natürliche Personen, selbst in Fällen, in denen das Double-Lock-Verfahren nicht zur Anwendung kommt, und so ein Schutzniveau gewährleistet, das dem in der EU gebotenen Schutzniveau der Sache nach gleichwertig ist.

28. Darüber hinaus ersucht der EDSA die Europäische Kommission, eingehender zu bewerten, unter welchen Bedingungen Dringlichkeit geltend gemacht werden kann, und Erläuterungen zu den möglichen Wegen für die Ausübung der Rechte der betroffenen Personen und zu den Rechtsbehelfsmöglichkeiten vorzulegen, die diesen im Zusammenhang mit Eingriffen in Geräte offenstehen, insbesondere im Fall einer Ausnahme vom Double-Lock-Verfahren.

29. Darüber hinaus ist der EDSA der Auffassung, dass es einer weitergehenden Klärung und Bewertung des Abfangens von Massendaten bedarf, insbesondere in Bezug auf die Auswahl und Anwendung der Selektoren, um zu klären, inwieweit beim Zugriff auf personenbezogene Daten der vom EuGH festgelegte Mindeststandard eingehalten wird, und welche Garantien zum Schutz der Grundrechte von Personen, deren Daten in diesem Zusammenhang abgefangen werden, bestehen, auch in Bezug auf die Speicherfristen der Daten. Besonders nützlich wäre eine unabhängige Bewertung durch die

zuständigen Aufsichtsbehörden des Vereinigten Königreichs. Der EDSA betont ferner, dass er es für besonders bedenklich hält, dass „mit dem Ausland in Zusammenhang stehende Kommunikationsdaten“ in den Anwendungsbereich von Praktiken des Abfangens von Massendaten fallen, und dies offenbar bedeutet, dass Daten vom Vereinigten Königreich unmittelbar in der EU abgefangen und massenhaft erhoben werden könnten, darunter auch Daten während der Übermittlung zwischen der EU und dem Vereinigten Königreich, die ja ebenfalls in den Anwendungsbereich des Beschlussentwurfs fallen würden. Angesichts der Bedeutung dieses Aspekts ersucht der EDSA die Europäische Kommission, die diesbezüglichen Entwicklungen genau zu verfolgen.

30. Bezüglich des Abfangens von Massendaten verweist der EDSA ferner auf die übereinstimmende Bewertung durch den EGMR und den EuGH und erinnert an die Bedenken, die hinsichtlich Sekundärdaten geäußert wurden, für die aufgrund ihrer Sensibilität besondere Garantien eingeräumt werden sollten. Der EDSA rät der Europäischen Kommission daher, sorgfältig zu prüfen, ob die im Recht des Vereinigten Königreichs für diese Kategorie personenbezogener Daten vorgesehenen Garantien ein Schutzniveau gewährleisten, das dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist.

31. In diesem Zusammenhang ist dem EDSA bekannt, dass der öffentliche Bericht des Intelligence and Security Committee (Ausschuss für Nachrichtendienste und Sicherheit) über die Ausübung von Massenüberwachungsbefugnissen aus dem Jahr 2016[13] Praktiken im Rahmen des vorherigen Rechtsrahmens betrifft, welcher später durch den IPA von 2016 ersetzt wurde. Dennoch hält er eine weitere unabhängige Bewertung und Überwachung des Einsatzes von Instrumenten für die automatisierte Datenverarbeitung durch die zuständigen Aufsichtsbehörden des Vereinigten Königreichs für erforderlich und empfiehlt der Europäischen Kommission, diese Frage und die Garantien, die betroffenen Personen im EWR in diesem Zusammenhang gewährt würden bzw. gewährt werden könnten, eingehender zu bewerten.

32. Der EDSA teilt die Auffassung des IPC, dass eine weitergehende Überprüfung und Überwachung erforderlich ist, um sicherzustellen, dass die Garantien, die in der Praxis von den zuständigen Behörden im Bereich der nationalen Sicherheit und der Nachrichtendienste angewandt werden, um bei Verstößen Abhilfe zu schaffen, aufrechterhalten und fortlaufend verbessert werden. Der EDSA begrüßt ferner, dass der IPC dementsprechend 2019 seinen Ansatz bei der Kontrolle des Abfangens von Massendaten überprüft hat, „unter anderem auch sehr sorgfältig die komplexen technischen Abläufe der Umsetzung des Abfangens von Massendaten“, und sich verpflichtet hat, ab 2020 bei den Kontrollen des Abfangens von Massendaten auch „die Selektoren und Suchkriterien, auf die der EGMR in diesem Zusammenhang aufmerksam gemacht hat, eingehend zu prüfen“. Angesichts der Bedeutung dieses Aspekts ist der EDSA besorgt darüber, dass die eingehende Prüfung der Selektoren und Suchkriterien durch den IPC noch nicht stattgefunden hat, und er ersucht die Europäische Kommission, die diesbezüglichen Entwicklungen genau zu beobachten, zumal das konkrete Format dieser Aufsicht noch geklärt werden muss.

33. Der EDSA weist darauf hin, dass in Bezug auf die Offenlegung von Daten im Ausland die Anwendung der im Recht des Vereinigten Königreichs vorgesehenen Ausnahmeregelung für die nationale

[13] Siehe Bericht des Independent Reviewer of Terrorism Legislation (Unabhängiger Prüfer der Rechtsvorschriften zum Terrorismus) zur Überprüfung von Massenüberwachungsbefugnissen vom August 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

Sicherheit dazu führen kann, dass es keine Garantien gibt, die gewährleisten würden, dass auch im empfangenden Drittland die Grundsätze der Zweckbindung, der Erforderlichkeit und der Verhältnismäßigkeit eingehalten oder Betroffenenrechte, Aufsicht und Rechtsbehelfe in ausreichendem Umfang gewährt werden. Der EDSA empfiehlt der Europäischen Kommission daher, in Bezug auf die Offenlegung von Datenim Ausland die im Recht des Vereinigten Königreichs vorgesehenen allgemeinen Garantien noch weiter zu prüfen, insbesondere im Hinblick auf die Anwendung von Ausnahmeregelungen für die nationale Sicherheit.

34. Schließlich ist der EDSA besorgt über weitere Formen des Austauschs und der Offenlegung von Daten auf der Grundlage weiterer Instrumente, insbesondere der verschiedenen internationalen Übereinkünfte, die das Vereinigte Königreich mit anderen Drittländern geschlossen hat – insbesondere wenn diese Instrumente nicht für die Öffentlichkeit zugänglich sind, wie etwa die Vereinbarung zur Zusammenarbeit der Geheimdienste zwischen dem Vereinigten Königreich und den USA. Eine solche Übereinkunft könnte bewirken, dass die genannten Garantien in Bezug auf den Zugriff auf und die Nutzung von personenbezogenen Daten für Zwecke der nationalen Sicherheit umgangen werden. Der EDSA ist der Auffassung, dass der Abschluss bilateraler oder multilateraler Übereinkünfte mit Drittländern für den Zweck der nachrichtendienstlichen Zusammenarbeit, die eine Rechtsgrundlage für das direkte Abfangen und Sammeln personenbezogener Daten oder für die Übermittlung personenbezogener Daten in diese Länder bieten, sich auch erheblich auf die Bedingungen für die Weiterverwendung der erhobenen Daten auswirken können, da solche Übereinkünfte den bewerteten Datenschutzrechtsrahmen des Vereinigten Königreichs beeinträchtigen dürften.

1.3 Schlussfolgerung

35. Der EDSA ist der Auffassung, dass die Beurteilung der Angemessenheit in Bezug auf das Vereinigte Königreich aufgrund des früheren Status des Vereinigten Königreichs als EU-Mitgliedstaat einzigartig ist. Darüber hinaus wäre dies auch der erste Angemessenheitsbeschluss mit einer Verfallsklausel.

36. Dementsprechend erkennt der EDSA viele Konvergenzbereiche zwischen dem britischen Datenschutzrahmen und dem EU-Datenschutzrahmen. Gleichzeitig hat der EDSA jedoch nach sorgfältiger Prüfung des Beschlussentwurfs der Europäischen Kommission und der Datenschutzvorschriften des Vereinigten Königreichs mehrere Herausforderungen identifiziert, die in der vorliegenden Stellungnahme ausführlich untersucht werden. In diesem Zusammenhang möchte der EDSA die herausragende Rolle der Europäischen Kommission bei der Überwachung aller diesbezüglicher Entwicklungen im Vereinigten Königreich hervorheben.

37. Vor diesem Hintergrund empfiehlt der EDSA der Europäischen Kommission, sich mit den in dieser Stellungnahme genannten Herausforderungen auseinanderzusetzen. Der EDSA ersucht die Europäische Kommission zudem, alle relevanten Entwicklungen im Vereinigten Königreich, die sich auf die der Sache nach vorhandene Gleichwertigkeit des Schutzniveaus für personenbezogene Daten auswirken könnten, genau zu überwachen und erforderlichenfalls zügig geeignete Maßnahmen zu ergreifen.

2. EINLEITUNG

2.1 Datenschutzrahmen des Vereinigten Königreichs

38. Der Datenschutzrahmen des Vereinigten Königreichs basiert weitgehend auf dem Datenschutzrahmen der EU (insbesondere auf der DSGVO und der JI-RL), was darauf zurückzuführen

ist, dass das Vereinigte Königreich bis zum 31. Januar 2020 Mitgliedstaat der EU war. Darüber hinaus wird mit dem britischen Data Protection Act von 2018, der am 23. Mai 2018 in Kraft getreten ist und mit dem der Data Protection Act von 1998 aufgehoben wurde, nicht nur die JI-RL umgesetzt, sondern auch die Anwendung der DSGVO im Recht des Vereinigten Königreichs näher spezifiziert; zudem werden der nationalen britischen Datenschutzaufsichtsbehörde – dem ICO – Befugnisse übertragen und Pflichten auferlegt.

39. Wie in Erwägungsgrund 12 des Beschlussentwurfs der Europäischen Kommission erwähnt, erließ die Regierung des Vereinigten Königreichs den European Union (Withdrawal) Act von 2018 (Gesetz über den Austritt aus der Europäischen Union), mit dem unmittelbar geltende EU-Rechtsvorschriften in das Recht des Vereinigten Königreichs übernommen wurden. Nach diesem Gesetz sind die Minister des Vereinigten Königreichs befugt, durch Rechtsverordnungen Sekundärrecht einzuführen, um das nach dem Austritt des Vereinigten Königreichs aus der EU beibehaltene Unionsrecht an die nationalen Gegebenheiten anzupassen.

40. Folglich besteht der einschlägige Rechtsrahmen, der nach Ablauf des Übergangszeitraums[14] im Vereinigten Königreich anwendbar ist, aus

- der Datenschutz-Grundverordnung des Vereinigten Königreichs (im Folgenden „UK-DSGVO"), wie sie durch den European Union (Withdrawal) Act von 2018 in das Recht des Vereinigten Königreichs übernommen wurde, in der durch die DPPEC-Vorschriften (Data Protection, Privacy and Electronic Communications (Amendment etc.) (EU Exit) – Datenschutz, Schutz personenbezogener Daten und elektronische Kommunikation (Änderungen etc.) (EU-Austritt)) von 2019 geänderten Fassung,
- dem Data Protection Act von 2018 (im Folgenden „DPA von 2018") in der durch die DPPEC-Vorschriften von 2019 und die DPPEC-Vorschriften von 2020 geänderten Fassung sowie
- dem IPA von 2016

(zusammen im Folgenden „der Datenschutzrahmen des Vereinigten Königreichs").

2.2 Umfang der Bewertung durch den EDSA

41. Der Beschlussentwurf der Europäischen Kommission ist das Ergebnis einer Bewertung des Datenschutzrahmens des Vereinigten Königreichs und anschließender Gespräche mit der Regierung des Vereinigten Königreichs. Gemäß Artikel 70 Absatz 1 Buchstabe s DSGVO wird vom EDSA erwartet, dass er eine unabhängige Stellungnahme zu den Feststellungen der Europäischen Kommission abgibt, etwaige Unzulänglichkeiten des Angemessenheitsrahmens ermittelt und entsprechende Vorschläge zu deren Beseitigung unterbreitet.

42. Laut der Referenzgrundlage für Angemessenheit im Sinne der DSGVO „sollten die von der Europäischen Kommission bereitgestellten Informationen umfassend sein und es dem EDSA ermöglichen, das Datenschutzniveau im betreffenden Drittland selbst zu beurteilen"[15].

43. In diesem Zusammenhang sei darauf hingewiesen, dass der EDSA die einschlägigen Dokumente für die Prüfung des Rechtsrahmens des Vereinigten Königreichs nur zum Teil fristgerecht erhalten hat.

[14] Der Übergangszeitraum wurde auf die Zeit bis zum 31. Dezember 2020 festgesetzt; danach gilt im Vereinigten Königreich das Unionsrecht nicht mehr. Der „Brückenzeitraum", der spätestens am 30. Juni 2021 endet, ist der zusätzliche Zeitraum, in dem die Übermittlung personenbezogener Daten aus dem EWR nach Großbritannien nicht als Übermittlung in ein Drittland gilt.
[15] Siehe WP 254/rev.01, S. 4.

Den Großteil der im Beschlussentwurf genannten Rechtsvorschriften des Vereinigten Königreichs erhielt der EDSA über die darin angegebenen Links. Die Europäische Kommission war nicht in der Lage, dem EDSA die für diese Angelegenheit relevanten schriftlichen Erklärungen und Zusagen des Vereinigten Königreichs in Bezug auf den einschlägigen Austausch zwischen den Behörden des Vereinigten Königreichs und der Europäischen Kommission vorzulegen.[16]

44. Vor diesem Hintergrund und aufgrund des dem EDSA für die Annahme dieser Stellungnahme gewährten begrenzten Zeitrahmens von zwei Monaten hat der EDSA beschlossen, sich auf einige spezifische Punkte des Beschlussentwurfs zu konzentrieren und seine Analyse und Stellungnahme zu diesen Punkten abzugeben.

45. Bei der Analyse des Rechts und der Rechtspraxis eines Drittlands, das bis vor Kurzem Mitgliedstaat der EU gewesen ist, hat der EDSA erwartungsgemäß festgestellt, dass zahlreiche Aspekte der Sache nach gleichwertig sind. Angesichts seiner Funktion im Verfahren zur Annahme einer Angemessenheitsentscheidung und des Umfangs der zu analysierenden Rechtsvorschriften und Rechtspraxis hat der EDSA die Entscheidung getroffen, sich auf diejenigen Aspekte zu konzentrieren, bei denen seiner Auffassung nach eine genauere Prüfung vordringlich ist. Darüber hinaus – im Einklang mit der Rechtsprechung des EuGH – umfasst die Analyse zu einem sehr großen Teil den Rechtsrahmen betreffend den mit der nationalen Sicherheit in Zusammenhang stehenden Zugriff auf die in das Vereinigte Königreich übermittelten personenbezogenen Daten und die Praxis des nationalen Sicherheitsapparats im Vereinigten Königreich. Dabei gilt es allerdings zu beachten, dass die nationale Sicherheit ein Bereich des Rechts und der Rechtspraxis ist, in dem die Rechtsvorschriften der Mitgliedstaaten auf EU-Ebene nicht harmonisiert sind und daher unterschiedlich sein können.

46. Der EDSA berücksichtigte den geltenden europäischen Datenschutzrahmen einschließlich der Artikel 7, 8 und 47 EU-Charta, die das Recht auf Achtung des Privat- und Familienlebens, das Recht auf den Schutz personenbezogener Daten und das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht schützen, sowie den Artikel 8 der Europäischen Menschenrechtskonvention (im Folgenden „EMRK“), der das Recht auf Achtung des Privat- und Familienlebens schützt. Darüber

[16] In Bezug auf Artikel 48 DSGVO (Fußnote 78 des Beschlussentwurfs) sowie auf verbesserte Garantien und Sicherheitsmaßnahmen, die von Verantwortlichen bei der Verarbeitung im Bereich der nationalen Sicherheit angewandt werden (Fußnote 64 des Beschlussentwurfs), auf die Pflicht des Verantwortlichen, auf Einzelfallbasis zu prüfen, ob die Ausnahmeregelung auch dann benötigt wird, wenn eine nationale Sicherheitsbescheinigung ausgestellt wurde (Erwägungsgrund 126 und Fußnote 172 des Beschlussentwurfs), auf die Tatsache, dass der Schutz des Rahmenabkommens zwischen der EU und den USA für alle personenbezogenen Daten gilt, die im Rahmen des CLOUD-Act-Abkommens erstellt oder gespeichert werden, unabhängig von der Art der ersuchenden Stelle, unter Berücksichtigung der Einzelheiten der konkreten Umsetzung der Datenschutzgarantien, die noch Gegenstand von Gesprächen zwischen dem Vereinigten Königreich und den USA sind, sowie der Zusicherung, dass die britischen Behörden dieses Abkommen erst in Kraft treten lassen werden, wenn sie sich davon überzeugt haben, dass bei seiner Umsetzung die darin vorgesehenen rechtlichen Pflichten eingehalten werden, einschließlich Klarheit hinsichtlich der Einhaltung der Datenschutzstandards für alle im Rahmen dieses Abkommens angeforderten Daten (Erwägungsgrund 153 des Beschlussentwurfs), auf Situationen, in denen Daten im Anwendungsbereich dieses Beschlussentwurfs aus der EU in das Vereinigte Königreich übermittelt werden, und auf die Tatsache, dass immer eine „Verbindung zu den Britischen Inseln“ bestünde und jeder Eingriff in Geräte, bei dem solche Daten betroffen sind, daher einen obligatorischen Gerichtsbeschluss gemäß Artikel 13 Absatz 1 des IPA von 2016 erfordern würde (Erwägungsgrund 206 des Beschlussentwurfs) sowie auf die angeführten Beispiele für operative Zwecke (Erwägungsgrund 216 und Fußnote 369 des Beschlussentwurfs).

hinaus hat der EDSA die Anforderungen der DSGVO und die einschlägige Rechtsprechung berücksichtigt.

47. Ziel dieser Übung ist es, der Europäischen Kommission eine Stellungnahme zur Bewertung der Angemessenheit des Schutzniveaus im Vereinigten Königreich vorzulegen. Der Begriff des „angemessenen Schutzniveaus", der bereits nach der Richtlinie 95/46/EG existierte, wurde vom EuGH weiterentwickelt. Es ist wichtig, sich den Standard zu vergegenwärtigen, den der EuGH in seinem Urteil in der Rechtssache Schrems I festgelegt hat; dieser besagt, dass das „Schutzniveau" im Drittland zwar „der Sache nach gleichwertig" mit dem in der EU gewährleisteten Schutzniveau sein muss, dass sich aber „die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden können, die in der Union herangezogen werden"[17]. Das Ziel ist also nicht, die europäischen Rechtsvorschriften Punkt für Punkt zu übernehmen, sondern vielmehr, die wesentlichen Kernanforderungen dieser Vorschriften festzulegen. Angemessenheit kann durch eine Kombination aus Rechten für betroffene Personen, Pflichten für Daten verarbeitende oder die Datenverarbeitung kontrollierende Stellen und eine Aufsicht durch unabhängige Gremien erreicht werden. Datenschutzvorschriften sind allerdings nur dann wirksam, wenn sie durchsetzbar sind und in der Praxis eingehalten werden. Daher sind nicht nur der Inhalt der geltenden Vorschriften für die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation zu beachten, sondern auch das bestehende System, mit dem die Wirksamkeit der Regeln gesichert werden soll. Effiziente Durchsetzungsmechanismen sind für die Wirksamkeit von Datenschutzvorschriften von wesentlicher Bedeutung.[18]

2.3 Allgemeine Bemerkungen und Bedenken

2.3.1 Vom Vereinigten Königreich eingegangene internationale Verpflichtungen

48. Gemäß Artikel 45 Absatz 2 Buchstabe c DSGVO und der Referenzgrundlage für Angemessenheit im Sinne der DSGVO[19] 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. Darüber hinaus 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")[20] und dem dazugehörigen Zusatzprotokoll[21] berücksichtigt werden.

49. **In diesem Zusammenhang begrüßt der EDSA, dass das Vereinigte Königreich der EMRK beigetreten ist und der Gerichtsbarkeit des EGMR unterliegt. Darüber hinaus ist das Vereinigte Königreich auch**

[17] Siehe Urteil des EuGH vom 6. Oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (im Folgenden „Schrems I"), Rn. 73-74.
[18] Siehe WP 254/rev.01, S. 3.
[19] Siehe WP 254/rev.01, S. 3.
[20] Siehe das Übereinkommen des Europarats zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten, Übereinkommen Nr. 108 vom 28. Januar 1981.
[21] Siehe das Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, aufgelegt zur Unterzeichnung am 8. November 2001.

dem Übereinkommen Nr. 108 und seinem Zusatzprotokoll beigetreten, hat 2018 das Übereinkommen Nr. 108+[22] unterzeichnet und befasst sich derzeit mit dessen Ratifizierung.

2.3.2 Mögliche künftige Abweichungen des Datenschutzrahmens des Vereinigten Königreichs

50. Wie in Erwägungsgrund 281 des Beschlussentwurfs erwähnt, muss die Europäische Kommission beachten, dass das Vereinigte Königreich mit Ablauf des im Austrittsabkommen[23] vorgesehenen Übergangszeitraums seine eigenen Datenschutzvorschriften verwaltet, anwendet und durchsetzt, und mit Ablauf des Brückenzeitraums gemäß Artikel FINPROV.10A des Handels- und Kooperationsabkommens zwischen der EU und dem Vereinigten Königreich[24] kann dies insbesondere Änderungen des im Beschlussentwurf bewerteten Datenschutzrahmens sowie andere entscheidende Entwicklungen mit sich bringen.

51. Die Europäische Kommission hat daher beschlossen, in ihren Beschlussentwurf eine Verfallsklausel aufzunehmen[25], in der eine Frist von vier Jahren nach Inkrafttreten festgelegt wird.

52. Die Möglichkeit, dass die britischen Minister und der Secretary of State (Kabinettsminister) nach dem Ende des Brückenzeitraums Sekundärrecht einführen können, wird möglicherweise in Zukunft zu einer erheblichen Abweichung des Datenschutzrahmens des Vereinigten Königreichs von dem der EU führen.

53. Die Regierung des Vereinigten Königreichs hat ihre Absicht bekundet, im Bereich des Datenschutzes separate und unabhängige Strategien zu entwickeln; diese könnten zu einer Abweichung vom Datenschutzrecht der EU führen.[26] Diese Absicht umfasst auch die Aufnahme von Aspekten

[22] Siehe das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten („Übereinkommen Nr. 108+“) vom 18. Mai 2018.
[23] Siehe das Abkommen über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft (ABl. L 029 vom 31.1.2020, S. 7).
[24] 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).
[25] Siehe Artikel 4 des Beschlussentwurfs. Siehe auch Erwägungsgrund 282 des Beschlussentwurfs.
[26] Die nationale Datenstrategie des Vereinigten Königreichs (zuletzt aktualisiert am 9. Dezember 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) umfasst u. a. folgende Aufgabe: „Engagement für den internationalen Datenverkehr. Der Datenverkehr über Grenzen hinweg begünstigt weltweite Unternehmensbeziehungen und Lieferketten sowie den globalen Handel und damit das Wachstum auf der ganzen Welt. Doch auch für die Gesellschaft im Allgemeinen ist er von zentraler Bedeutung. Durch die Übermittlung personenbezogener Daten wird sichergestellt, dass Menschen ihre Gehälter ausbezahlt bekommen und dass sie mit ihren Lieben auch über Entfernungen hinweg in Kontakt bleiben können. Und wie die Corona-Pandemie gezeigt hat, begünstigt der Austausch von Gesundheitsdaten die immens wichtige wissenschaftliche Erforschung von Krankheiten und ermöglicht zugleich, dass viele Länder gemeinsam auf globale Notsituationen reagieren können. **Nach dem Austritt aus der Europäischen Union wird sich das Vereinigte Königreich dafür einsetzen, Daten so vorteilhaft wie möglich zu nutzen.** Wir werden bewährte nationale Verfahren unterstützen und mit internationalen Partnern zusammenarbeiten, **um dafür zu sorgen, dass Daten nicht durch nationale Grenzen und fragmentierte Regulierungssysteme in unangemessener Weise eingeschränkt werden**, sondern dass sie in größtmöglichem Umfang genutzt werden können.“ (Hervorhebungen hinzugefügt.)

personenbezogener Daten in Handelsabkommen[27], eine Praxis, die die Gefahr birgt, dass das vom Vereinigten Königreich gewährte Schutzniveau für personenbezogene Daten herabgesetzt wird.[28]

54. Schließlich ist das Vereinigte Königreich nicht nur seit dem Ende des Übergangszeitraums nicht mehr an die Rechtsprechung des EuGH gebunden, sondern auch die bereits erlassenen Urteile des EuGH, die als im Rechtsrahmen des Vereinigten Königreichs beibehaltene Rechtsprechung gelten, sind möglicherweise für das Vereinigte Königreich nicht mehr bindend, insbesondere weil nach Ablauf des Brückenzeitraums das Vereinigte Königreich beibehaltenes Unionsrecht ändern kann und sein Supreme Court (Oberster Gerichtshof) an keinerlei beibehaltene Rechtsprechung der EU mehr gebunden ist.[29]

55. **Angesichts der Risiken im Zusammenhang mit einer möglichen Abweichung des Datenschutzrahmens des Vereinigten Königreichs vom EU-Besitzstand nach Ablauf des Brückenzeitraums begrüßt der EDSA die Entscheidung der Europäischen Kommission, im Beschlussentwurf eine vierjährige Verfallsklausel vorzusehen. Der EDSA möchte jedoch an dieser Stelle die Bedeutung der Überwachungsfunktion der Europäischen Kommission[30] hervorheben. Die Europäische Kommission sollte alle einschlägigen Entwicklungen im Vereinigten Königreich, die sich auf das der Sache nach gleichwertige Schutzniveau für personenbezogene Daten auswirken könnten, die auf der Grundlage des Angemessenheitsbeschlusses in Bezug auf das Vereinigte Königreich übermittelt werden, ab dem Inkrafttreten des Angemessenheitsbeschlusses fortlaufend und dauerhaft überwachen. Darüber hinaus sollte die Europäische Kommission geeignete Maßnahmen ergreifen, indem sie den Angemessenheitsbeschluss unter Berücksichtigung der vorliegenden Umstände aussetzt, ändert oder aufhebt, wenn der Europäischen Kommission nach der Annahme des Angemessenheitsbeschlusses Hinweise darauf vorliegen, dass im Vereinigten Königreich kein angemessenes Schutzniveau mehr gewährleistet ist.**

56. Der EDSA wird sich seinerseits nach Kräften bemühen, die Europäische Kommission über alle einschlägigen Maßnahmen zu informieren, die die Datenschutzaufsichtsbehörden der Mitgliedstaaten im gewerblichen oder öffentlichen Bereich ergreifen, insbesondere in Bezug auf

---

[27] Ebd.: „Erleichterung des grenzüberschreitenden Datenverkehrs: **Wir werden weltweit darauf hinarbeiten, unnötige Hindernisse für den internationalen Datenverkehr zu beseitigen. Wir werden in unseren Handelsgesprächen ehrgeizige Bestimmungen in Bezug auf Daten vereinbaren** und unsere seit Kurzem unabhängige Mitgliedschaft in der Welthandelsorganisation nutzen, um die Handelsbestimmungen für Daten zum Besseren zu wenden. **Wir werden Hindernisse** für wachstums- und innovationsfördernde **internationale Datenübermittlungen beseitigen**, unter anderem durch die Entwicklung einer neuen Kapazität des Vereinigten Königreichs, die neue und innovative Mechanismen für internationale Datenübermittlungen bietet. Wir werden auch gemeinsam mit Partnern in der G20 daran arbeiten, die Interoperabilität zwischen nationalen Datenregelungen herzustellen, um Widerstände bei der Datenübertragung zwischen verschiedenen Ländern so gering wie möglich zu halten." (Hervorhebungen hinzugefügt.)

[28] Siehe die Entschließung des Europäischen Parlaments vom 12. Dezember 2017 zu dem Thema „Auf dem Weg zu einer Strategie für den digitalen Handel" (2017/2065(INI)), Erwägung V, in der festgehalten wird, dass „der Schutz personenbezogener Daten in Handelsabkommen nicht verhandelbar ist", abrufbar unter: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_DE.pdf. Siehe auch 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, Ziffer 28: „[...] befürwortet die Vorgehensweise der Kommission, den Datenschutz und die Übermittlung personenbezogener Daten getrennt von Handelsabkommen zu thematisieren", https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_DE.html.

[29] Siehe Artikel 6 Absätze 3 bis 6 des European Union (Withdrawal) Act von 2018.

[30] Siehe Artikel 45 Absatz 4 DSGVO.

Beschwerden betroffener Personen im EWR im Zusammenhang mit der Übermittlung personenbezogener Daten aus dem EWR in das Vereinigte Königreich.

3. ALLGEMEINE ASPEKTE DES DATENSCHUTZES

3.1 Grundsätze

57. In Kapitel 3 der Referenzgrundlage für Angemessenheit im Sinne der DSGVO geht es um die „inhaltlichen Grundsätze“. Diese müssen im System eines Drittlands enthalten sein, damit dessen Datenschutzniveau dem innerhalb der EU garantierten Schutzniveau als der Sache nach gleichwertig betrachtet werden kann. Der EDSA erkennt an, dass das Vereinigte Königreich keine kodifizierte Verfassung besitzt, da es kein zentrales Dokument gibt, in dem die geltenden Grundregeln des Landes festgelegt sind. Allerdings sind das Recht auf Achtung des Privat- und Familienlebens (und das Recht auf Datenschutz als Teil dieses Rechts) und das Recht auf ein unparteiisches Gericht[31] im Human Rights Act von 1998 (Gesetz über Menschenrechte) enthalten, und der verfassungsmäßige Wert dieses Gesetzes wurde von den Gerichten des Vereinigten Königreichs anerkannt. Tatsächlich enthält der Human Rights Act von 1998 die in der EMRK verankerten Rechte.[32] Zudem heißt es im Human Rights Act von 1998, dass jede Behördenmaßnahme mit der EMRK vereinbar sein muss.[33]

58. Abgesehen von strukturellen und formellen Unterschieden zwischen den Rechtsvorschriften des Vereinigten Königreichs und der EU stellt der EDSA erwartungsgemäß fest, dass der Datenschutzansatz des Vereinigten Königreichs dem der EU ähnelt, da das Vereinigte Königreich bis zum 31. Januar 2020 Mitgliedstaat der EU war. Infolgedessen sind viele inhaltliche Grundsätze an die der DSGVO angeglichen und bieten ein Schutzniveau, das dem von der EU gebotenen Schutzniveau der Sache nach gleichwertig ist. Der EDSA hat beschlossen, die Analyse der inhaltlichen Grundsätze, die an das EU-Recht angeglichen sind, nicht weiter zu vertiefen, und gibt sich mit der Analyse, die die Europäische Kommission dazu in ihrem Beschlussentwurf vorgelegt hat, zufrieden. Diese inhaltlichen Grundsätze beziehen sich beispielsweise auf Begriffe (z. B. „personenbezogene Daten“, „Verarbeitung personenbezogener Daten”, „Verantwortlicher“), Gründe für die rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung für legitime Zwecke, Zweckbindung, Datenqualität und Verhältnismäßigkeit, Datenspeicherung, Sicherheit und Vertraulichkeit, Transparenz, besondere Kategorien personenbezogener Daten, Direktwerbung sowie automatisierte Entscheidungen und Profiling. Der EDSA stellt ferner fest, dass die UK-DSGVO und der DPA von 2018 inhaltliche Grundsätze umfassen, die über das hinausgehen, was nach der Referenzgrundlage für Angemessenheit im Sinne der DSGVO erforderlich ist, und die den Grundsätzen der EU-DSGVO entsprechen; damit wird das im Vereinigten Königreich gewährte Schutzniveau angehoben. Bei diesen inhaltlichen Grundsätzen handelt es sich beispielsweise um die Grundsätze in Bezug auf Meldungen von Verletzungen des Schutzes personenbezogener Daten, auf den Datenschutzbeauftragten, auf Datenschutzfolgenabschätzungen sowie auf Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen.

59. Wie in der Einleitung erwähnt, möchte der EDSA in dieser Stellungnahme jedoch gezielt auf bestimmte Punkte eingehen, zu denen er Bedenken hat und zu denen er die Europäische Kommission gern um Klarstellungen ersuchen möchte.

[31] Siehe die Artikel 6 und 8 der EMRK (Anhang 1 des Human Rights Act von 1998).
[32] Weitere Informationen sind den Erwägungsgründen 8 bis 10 des Beschlussentwurfs zu entnehmen.
[33] Siehe Artikel 6 des Human Rights Act von 1998.

3.1.1 Rechte auf Auskunft, Berichtigung und Löschung personenbezogener Daten sowie Recht auf Widerspruch

60. Die in **Anhang 2 Teil 1** Nummer 4 des **DPA** von **2018** vorgesehene sogenannte Ausnahmeregelung für den Bereich der Einwanderung ermöglicht es den an der Einwanderungskontrolle beteiligten Verantwortlichen, bestimmte im DPA von 2018 verankerte Rechte betroffener Personen nicht anzuwenden, wenn die Ausübung dieser Rechte „die Aufrechterhaltung einer wirksamen Einwanderungskontrolle“ oder „die Untersuchung oder Aufdeckung von Tätigkeiten, die die Aufrechterhaltung einer wirksamen Einwanderungskontrolle untergraben würden“, voraussichtlich beeinträchtigen würde.

61. Wie von der Europäischen Kommission in ihrem Beschlussentwurf festgehalten[34] und in der Stellungnahme des LIBE-Ausschusses des Europäischen Parlaments zum Abschluss des Handels- und Kooperationsabkommens im Namen der Union zwischen der EU und dem Vereinigten Königreich[35] erwähnt wird, ist diese Ausnahme **weit gefasst**. Sie gilt für folgende Rechte: Recht, unterrichtet zu werden, Auskunftsrecht, Recht auf Löschung, Recht auf Einschränkung der Verarbeitung und Widerspruchsrecht.

62. Darüber hinaus ist darauf hinzuweisen, dass diese Ausnahmeregelung auch dann gilt, wenn personenbezogene Daten nicht für die Zwecke der Einwanderungskontrolle von einem Verantwortlichen („Verantwortlicher 1“) erhoben, sondern von diesem einem anderen Verantwortlichen („Verantwortlicher 2“) zur Verfügung gestellt werden, der diese personenbezogenen Daten für den Zweck der Einwanderungskontrolle verarbeitet (z. B. dem britischen Innenministerium).[36]

---

[34] Siehe die Erwägungsgründe 62 bis 65 des Beschlussentwurfs.

[35] Dazu, dass die Ausnahme für den Bereich der Einwanderung **weit gefasst** ist, siehe die Stellungnahme des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres zu dem Abschluss des Handels- und Kooperationsabkommens im Namen der Union zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits und zu dem Abschluss des Abkommens zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien und Nordirland über die Sicherheitsverfahren für den Austausch und den Schutz von Verschlusssachen (2020/0382(NLE)), 5. Februar 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_DE.pdf, Ziffer 10: „verweist diesbezüglich auf seine Entschließungen vom Februar und Juni 2020, in denen darauf hingewiesen wird, dass im britischen Datenschutzgesetz [...] eine **allgemeine und umfassende Ausnahme** vorgesehen ist, wenn es um die Verarbeitung personenbezogener Daten zu Einwanderungszwecken geht;“ und Ziffer 11: „ist der Auffassung, dass die **allgemeine und umfassende** Ausnahme, die im britischen Datenschutzgesetz [...] vorgesehen ist, wenn es um die Verarbeitung personenbezogener Daten zu Einwanderungszwecken geht, geändert werden muss, bevor eine gültige Entscheidung über die Angemessenheit getroffen werden kann;“ (Hervorhebungen hinzugefügt).

[36] Siehe Beispiel in: ICO, Guide to the General Data Protection Regulation (GDPR), 1. Januar 2021, S. 307 (Hervorhebungen hinzugefügt): „Eine private Organisation (Verantwortlicher 1) warnt das Innenministerium (Verantwortlicher 2) vor einem Mitarbeiter, der zur Erlangung einer Stelle mutmaßlich gefälschte Dokumente zum Nachweis seiner Identität und seiner Qualifikationen vorgelegt hat. Der Arbeitgeber stellt dem Innenministerium die einschlägigen Informationen zur Verfügung. Das Recht der betroffenen Person, über die Weitergabe ihrer personenbezogenen Daten an das Innenministerium unterrichtet zu werden, ist insofern eingeschränkt, als seine Wahrung die Untersuchung beeinträchtigen könnte.
Der Arbeitgeber ist daher nicht verpflichtet, die betroffene Person darüber zu unterrichten, dass ihre Daten an das Innenministerium weitergeleitet wurden, und **das Innenministerium** ist seinerseits nicht verpflichtet, der betroffenen Person einen Datenschutzhinweis zu übermitteln, in dem es sie darüber informiert, dass es ihre personenbezogenen Daten verarbeitet. Die Ausnahme gilt für beide Verantwortlichen gleichermaßen.

63. In der Rechtssache Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (3. Oktober 2019) rügten die Kläger die Rechtmäßigkeit der Ausnahmeregelung für den Bereich der Einwanderung mit der Begründung, diese verstoße gegen Artikel 23 DSGVO und sei mit den in den Artikeln 7 und 8 EU-Charta garantierten Rechten auf Schutz der Privatsphäre und Schutz personenbezogener Daten unvereinbar. Der High Court of England and Wales (im Folgenden „High Court") prüfte, ob die in Anhang 2 Teil 1 Nummer 4 des DPA von 2018 vorgesehene Ausnahmeregelung für den Bereich der Einwanderung rechtmäßig ist, und entschied zugunsten ihrer Rechtmäßigkeit.

64. Der High Court vertrat insbesondere die Auffassung, dass

- „[...] die Ausnahmeregelung für den Bereich der Einwanderung eindeutig von ‚erheblichem öffentlichem Interesse' ist und einen legitimen Zweck verfolgt. [...]", Rn. 30
- „die Ausnahmeregelung für den Bereich der Einwanderung die Voraussetzungen für die ‚Rechtmäßigkeit' einer Maßnahme erfüllt. […]", Rn. 38
- „[d]ie Ausnahmeregelung für den Bereich der Einwanderung nur geltend gemacht werden [kann], wenn und soweit die Einhaltung der ‚aufgelisteten Bestimmungen der DSGVO' die Aufrechterhaltung einer wirksamen Einwanderungskontrolle oder die Untersuchung oder Aufdeckung von Tätigkeiten, die die Aufrechterhaltung einer wirksamen Einwanderungskontrolle untergraben würden, **voraussichtlich beeinträchtigen würde**. Im Kontext des Data Protection Act von 1998 (dem Vorläufer des DPA von 2018) wurde die Formulierung ‚voraussichtlich beeinträchtigen würde' dahingehend ausgelegt, dass damit ‚eine sehr große und schwerwiegende Gefahr einer Beeinträchtigung des besonderen öffentlichen Interesses' gemeint sei. Das Risiko muss so hoch sein, dass diese Interessen ‚sehr wahrscheinlich' beeinträchtigt würden, auch wenn das Risiko selbst nicht sehr wahrscheinlich ist [...].", Rn. 39 (Hervorhebung hinzugefügt)

65. Es sei darauf hingewiesen, dass dieses Urteil nach Kenntnis des EDSA nicht rechtskräftig ist und Berufung dagegen eingelegt wurde.

66. In den Leitlinien des EDSA zu Beschränkungen gemäß Artikel 23 DSGVO („Leitlinien zu Artikel 23 DSGVO")[37] heißt es, „[...] Beschränkungen [müssen] in einem DSGVO-Kontext **im Wege von Gesetzgebungsmaßnahmen vorgesehen** werden, dürfen nur eine **begrenzte Zahl der** in Artikel 23 DSGVO aufgeführten **Rechte betroffener Personen und/oder Pflichten des Verantwortlichen** betreffen, müssen **den Wesensgehalt** der betreffenden Grundrechte und Grundfreiheiten **wahren**,

---

Der Mitarbeiter verlangt jedoch vom Innenministerium eine Kopie seiner personenbezogenen Daten, die gerade dort untersucht werden. Das **Innenministerium kann sich auf die Ausnahmeregelung berufen** und einen Teil der Daten zurückhalten, wenn die Offenlegung die Untersuchung voraussichtlich beeinträchtigen würde. Würde der Arbeitnehmer einen ähnlichen Antrag an seinen Arbeitgeber richten, wäre auch dieser berechtigt, gleichermaßen **von der Ausnahmeregelung Gebrauch zu machen**."
Auf S. 300 wird dies noch einmal klargestellt: „In den meisten Fällen wird der Verantwortliche, der die Ausnahmeregelung in Anspruch nimmt, das Innenministerium oder eine seiner Behörden oder Auftragnehmer sein. Es muss allerdings darauf hingewiesen werden, dass die Anwendung dieser Ausnahmeregelung nicht auf das Innenministerium beschränkt ist. Sie kann auch für andere Verantwortliche sachdienlich sein, etwa für Arbeitgeber, Universitäten und Polizeibehörden, die in Einwanderungsangelegenheiten mit dem Innenministerium zusammenarbeiten."

[37] Siehe EDSA, Guidelines 10/2020 on restrictions under Article 23 GDPR (Leitlinien 10/2020 zu Beschränkungen gemäß Artikel 23 DSGVO), Version 1.0, angenommen am 15. Dezember 2020, die nach Konsultation der Öffentlichkeit derzeit fertiggestellt werden, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_de.

in einer demokratischen Gesellschaft eine **erforderliche und verhältnismäßige Maßnahme** darstellen und einen der in Artikel 23 Absatz 1 DSGVO genannten Gründe [...] sicherstellen."[38]

67. Der EDSA weist ferner darauf hin, dass es in Erwägungsgrund 41 DSGVO heißt: „Wenn in dieser Verordnung auf **eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme** Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt; davon unberührt bleiben Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats. Die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme sollte jedoch **klar und präzise sein und ihre Anwendung sollte für die Rechtsunterworfenen** gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union […] und des Europäischen Gerichtshofs für Menschenrechte **vorhersehbar sein**." (Hervorhebungen hinzugefügt).

68. Der EGMR hat zwar ausgeführt, dass „[i]n Bezug auf die in den Artikeln 8 bis 11 der Konvention enthaltenen Formulierungen ‚gemäß dem Gesetz' und ‚gesetzlich vorgesehen' [...] der [EMRK] [feststellt], dass er den Begriff ‚Gesetz' stets im ‚materiellen' und nicht im ‚formellen' Sinn verstanden hat; er umfasst sowohl das ‚geschriebene Recht', das den Erlass von Gesetzen mit niedrigerem Rang und Regulierungsmaßnahmen einschließt, die von professionellen Regulierungsstellen im Rahmen unabhängiger, vom Parlament übertragener Befugnisse zur Rechtsetzung ergriffen werden, als auch ungeschriebenes Recht. Der Begriff ‚Gesetz' ist dahin auszulegen, dass er sowohl Gesetzesrecht **als auch ‚Richterrecht'** beinhaltet"[39], doch wird in den Leitlinien zu Artikel 23 DSGVO darauf hingewiesen, dass „gemäß der Rechtsprechung des EuGH jede auf der Grundlage von Artikel 23 Absatz 1 DSGVO erlassene **Gesetzgebungsmaßnahme** insbesondere **den spezifischen Anforderungen von Artikel 23 Absatz 2 DSGVO entsprechen muss**. In Artikel 23 Absatz 2 DSGVO heißt es, dass Gesetzgebungsmaßnahmen, mit denen die Rechte betroffener Personen und die Pflichten von Verantwortlichen beschränkt werden, gegebenenfalls **spezifische Vorschriften in Bezug auf verschiedene nachfolgend aufgeführte Kriterien** enthalten müssen. Grundsätzlich sollten alle nachfolgend aufgeführten Anforderungen **in die Gesetzgebungsmaßnahme aufgenommen werden**, mit der Beschränkungen im Sinne von Artikel 23 DSGVO erlassen werden."[40]

[38] Siehe Leitlinien zu Artikel 23 DSGVO, Ziffer 9, S. 5.

[39] Siehe EGMR, Sanoma Uitgevers B.V./Niederlande, 14. September 2010, EC:ECHR:2010:0914JUD003822403, Rn. 83 (Hervorhebungen hinzugefügt).

[40] Siehe Leitlinien zu Artikel 23 DSGVO, Ziffern 45 und 46, S. 11. Artikel 52 Absatz 3 der EU-Charta lautet: „So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt." In Bezug auf den in Artikel 52 Absatz 1 der EU-Charta verwendeten Begriff „**gesetzlich vorgesehen**" sollten die vom EGMR entwickelten Kriterien angewandt werden, wie in mehreren Schlussanträgen des Generalanwalts des EuGH vorgeschlagen, siehe z. B. die Schlussanträge des Generalanwalts in der Rechtssache Tele2 Sverige AB, C-203/15 und C-698/15, ECLI:EU:C:2016:572, Rn. 137–154, und in Scarlet Extended SA, C-70/10, ECLI:EU:C:2011:255, Rn. 88–114. Daher kann u. a. auf das Urteil des EGMR in der Rechtssache Weber und Saravia/Deutschland, R. 84 verwiesen werden: „Der Gerichtshof weist erneut darauf hin, dass der Ausdruck ‚**gesetzlich vorgesehen**' nach Artikel 8 Abs. 2 [der EMRK] zunächst bedeutet, dass die gerügte Maßnahme eine gewisse **innerstaatliche Rechtsgrundlage** haben muss; er betrifft auch die **Qualität des** in Rede gestellten **Gesetzes** und setzt voraus, dass die betroffene Person Zugang zu dem Gesetz hat und darüber hinaus erkennen kann, welche Folgen es für sie hat; außerdem muss das Gesetz rechtsstaatlichen Anforderungen genügen [...]." (Hervorhebungen hinzugefügt).
Siehe auch Erwägungsgrund 41 DSGVO: „Die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme sollte [...] **klar** und **präzise** sein und ihre Anwendung sollte **für die Rechtsunterworfenen** gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union [...] und des Europäischen Gerichtshofs für Menschenrechte **vorhersehbar sein**." (Hervorhebungen hinzugefügt).

69. In diesem Zusammenhang ist festzustellen, dass in **der Ausnahmeregelung für den Bereich der Einwanderung folgende in Artikel 23 Absatz 2 DSGVO genannten Elemente nicht angegeben sind**:

- „die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung“ (Buchstabe d),
- „die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen“ (Buchstabe e)[41]
- „die Risiken für die Rechte und Freiheiten der betroffenen Personen“ (Buchstabe g),
- „das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist“ (Buchstabe h).

70. Die Veröffentlichung *Guide to the General Data Protection Regulation (GDPR)*[42] des ICO, die ein Kapitel über die Ausnahmeregelung für den Bereich der Einwanderung umfasst, enthält zwar Erläuterungen zu der Ausnahmeregelung, sie kann aber per se **keine** verbindlichen Vorschriften zu deren Ergänzung vorgeben. Darüber hinaus ist die Frage nach der „Qualität des Gesetzes“ angesichts der Bedeutung der beschränkten Rechte und des Umfangs der Ausnahmeregelung besonders relevant.[43]

---

[41] Siehe das vorstehend genannte Urteil des High Court, Rn. 54: „Meiner Auffassung nach ist es nicht rechtswidrig, dass die Ausnahmeregelung für den Bereich der Einwanderung **für alle Verantwortlichen**, die Daten für die angegebenen Zwecke verarbeiten, verfügbar ist. Die Beklagten weisen darauf hin, dass die Ausnahmeregelung für den Bereich der Einwanderung ohne Nummer 4 Punkte 3 und 4 in Fällen unwirksam werden würde, in denen Daten von Dritten (wie beispielsweise einer lokalen Behörde oder der Finanz- und Zollbehörde des Vereinigten Königreichs) für Zwecke der Aufrechterhaltung einer wirksamen Einwanderungskontrolle abgerufen werden" (Hervorhebung hinzugefügt), wodurch die **verallgemeinerte** Anwendung der Beschränkungen bestätigt wird.

[42] ICO, Guide to the General Data Protection Regulation (GDPR), 1. Januar 2021, S. 299–307.

[43] Siehe Rn. 57 des vorstehend genannten Urteils des High Court: „Herr Knight teilt mir mit, dass die Datenschutzbeauftragte derzeit Leitlinien für die Ausnahmeregelung fertigstellt, dass diese aber nur in dem Sinne den Status von ‚Gesetzesrecht‘ haben werden, dass sie kraft der Befugnisse der Datenschutzbeauftragten gemäß Artikel 57 Absatz 1 DSGVO erlassen werden. Sie werden keinen Rechtsstatus nach dem DPA von 2018 besitzen.“
Die Begründung für die Einführung rechtsverbindlicher Leitlinien, die vom ICO unterstützt werden, wird insbesondere in Rn. 56-60 des Urteils gegeben:
„56. Schließlich komme ich zu dem Vorbringen der Datenschutzbeauftragten, dass die Ausnahmeregelung für den Bereich der Einwanderung ohne flankierende gesetzliche Leitlinien, mit denen sowohl die Bedeutung als auch die Anwendung der Ausnahmeregelung abgesichert wird, keine verhältnismäßige Umsetzung von Artikel 23 Absatz 1 DSGVO darstellen würde. Herr Knight erklärt, dass die Bestimmung, wenn sie durch solche Leitlinien ergänzt wird, verhältnismäßig sei.
57. Herr Knight teilt mir mit, dass die Datenschutzbeauftragte derzeit Leitlinien für die Ausnahmeregelung fertigstellt, dass diese aber nur in dem Sinne den Status von ‚Gesetzesrecht‘ haben werden, dass sie kraft der Befugnisse der Datenschutzbeauftragte gemäß Artikel 57 Absatz 1 DSGVO erlassen werden. Sie werden keinen Rechtsstatus nach dem DPA von 2018 besitzen. Darüber hinaus nehme ich zur Kenntnis, dass das Innenministerium zu der Ausnahmeregelung für den Bereich der Einwanderung einen Entwurf für interne Leitlinien für Mitarbeiter erstellt hat (siehe Rn. 22 dieses Urteils). In der Praxis sind Leitlinien, die von der Datenschutzbeauftragten herausgegeben werden, unabhängig von ihrer Rechtsgrundlage richtungsweisend. Die Datenschutzbeauftragte ist jedoch nicht befugt, ‚verbindliche‘ Leitlinien zu erlassen, wie sie der Supreme Court in der Rechtssache Christian Institute (siehe Rn. 101 und 107) im Sinn hatte. Es scheint, dass Primärrecht erforderlich wäre, wenn es für notwendig erachtet würde, dass zu der Ausnahmeregelung für den Bereich der

71. Es wird auch nicht dargelegt, welche Garantien bei einer „**vermuteten Beeinträchtigung**“ beispielsweise vom Innenministerium umzusetzen sind, um Missbrauch oder unrechtmäßigen Zugriff oder unrechtmäßige Übermittlung zu verhindern.

72. Im Lichte all dieser Erwägungen merkt der EDSA an, dass weitere Erläuterungen zur Anwendung der Ausnahmeregelung für den Bereich der Einwanderung erforderlich sind.

73. Darüber hinaus weist der EDSA darauf hin, dass es kein rechtsverbindliches Instrument gibt, das hinsichtlich der Ausnahmeregelung für den Bereich der Einwanderung Klarheit schafft, um beurteilen zu können, ob diese der Sache nach gleichwertig mit Artikel 23 DSGVO und den Artikeln 7 und 8 EU-Charta ist. Gleichzeitig ist der EDSA der Auffassung, dass die Erforderlichkeit und Verhältnismäßigkeit des weiten persönlichen Anwendungsbereichs der Ausnahmeregelung für den Bereich der Einwanderung von der Europäischen Kommission noch weiter nachgewiesen und durch Beweise belegt werden muss.

74. **Dementsprechend bittet der EDSA die Europäische Kommission, den Sachstand des vorstehend genannten Verfahrens Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) zu überprüfen und, da dieses Urteil nicht**

Einwanderung Leitlinien mit demselben Status wie die derzeit in den Artikeln 121–124 des DPA von 2018 vorgesehenen Verhaltensregeln vorhanden sind.

58. In seiner Argumentation für gesetzliche Leitlinien bringt Herr Knight vor, dass in einer Situation, in der sich die Inanspruchnahme der Ausnahmeregelung für den Bereich der Einwanderung ergeben würde, unweigerlich die Bedenken hinsichtlich der Erforderlichkeit und der Verhältnismäßigkeit der Existenz und der Anwendung dieser Regelung zum Tragen kämen. Er weist auf zwei Punkte hin, die insbesondere den rechtlichen Kontext betreffen. Erstens ist es wahrscheinlich, dass personenbezogene Daten, auf die die Ausnahmeregelung für den Bereich der Einwanderung Anwendung findet, Daten besonderer Kategorien im Sinne von Artikel 9 Absatz 1 DSGVO umfassen (d. h. Daten, ‚aus denen die rassische und ethnische Herkunft [...] hervorgehen'). Solche Daten werden in der DSGVO genannt, da sie ein höheres Schutzniveau erfordern (Stellungnahme 1/15 [2019] 3 C.M.L.R.25, Rn. 141). Zweitens ist es ein Grundsatz des Datenschutzrechts, dass insbesondere das Auskunftsrecht von zentraler Bedeutung ist, weil es der Ausgangspunkt für die Ausübung der anderen Rechte ist, die betroffenen Personen gewährt werden, (siehe YS/Minister voor Immigratie, Integratie en Asiel, C-141/12, EU:C:2014:2081,[2015] 1 C.M.L.R.18, Rn. 44).

59. Herr Knight nennt vier praxisbezogene Aspekte. Erstens: Wenn Verantwortliche betroffenen Personen weder erläutern, dass sie sich auf eine gesetzliche Ausnahmeregelung berufen haben, noch eine umfassende Zusammenfassung der entsprechenden Gründe geben, weiß die betroffene Person nicht, dass die Ausnahmeregelung angewandt wurde, und kann sie folglich nicht wirksam anfechten. Zweitens sind betroffene Personen besonders darauf angewiesen, dass Verantwortliche die Ausnahmeregelung sorgfältig und nur im erforderlichen Maß anwenden. Zwar hat jede betroffene Person das Recht, sich bei der Datenschutzbeauftragten über die Anwendung der Ausnahmeregelung zu beschweren oder dagegen zu klagen, doch ist davon auszugehen, dass die betroffene Person ihre Rechte nicht kennt und nicht über die Mittel verfügt, um in einer Situation, in der Datenschutzrechte unverzüglich und genau eingehalten werden müssen, rechtliche Schritte zu unternehmen. Drittens ist die betroffene Person als Einwanderer wahrscheinlich besonders gefährdet. Viertens handelt es sich angesichts der Beweismittel der Beklagten in Bezug auf die Inanspruchnahme der Ausnahmeregelung für den Bereich der Einwanderung nicht um eine abstrakte Frage (siehe Rn. 4 dieses Urteils).

60. Herr Knight weist auf eine deutliche Parallele zwischen der vorliegenden Anfechtung der Ausnahmeregelung für den Bereich der Einwanderung und der Urteilsbegründung in der Rechtssache Christian Institute [2016] UKSC 51 hin. Er führt an, dass ebenso wie in der Rechtssache Christian Institute die Ausnahmeregelung für den Bereich der Einwanderung weit gefasst sei, dass darin ungenaue Begriffe verwendet würden und die Schwelle für ihre Anwendung niedrig sei, dass sie Kontrollen unterliege, die aus der Bestimmung nicht klar hervorgehen, und dass sie auf ein sehr breites Spektrum von Zusammenhängen und Rechten anwendbar sei. Anders als in der Rechtssache Christian Institute gibt es zur Ausnahmeregelung für den Bereich der Einwanderung keine öffentlich zugänglichen Leitlinien, geschweige denn einen gesetzesrechtlichen Status, der berücksichtigt werden müsste.“

rechtskräftig (res judicata) ist, zu prüfen, ob es durch das Berufungsurteil bestätigt oder abgeändert wird, alle etwaigen Aktualisierungen zu berücksichtigen und es im Angemessenheitsbeschluss anzugeben. Der EDSA ersucht die Europäische Kommission zudem, weitere Informationen über die Erforderlichkeit und Verhältnismäßigkeit der Ausnahmeregelung für den Bereich der Einwanderung bereitzustellen, insbesondere im Hinblick auf den weiten persönlichen Anwendungsbereich.

75. **Gleichzeitig bittet der EDSA die Europäische Kommission, noch weiter zu prüfen, ob zusätzliche Garantien im Rechtsrahmen des Vereinigten Königreichs vorgesehen sind oder in Erwägung gezogen werden könnten, beispielsweise durch rechtsverbindliche Instrumente, die die Ausnahmeregelung für den Bereich der Einwanderung ergänzen würden, indem deren Vorhersehbarkeit und die Garantien für betroffene Personen gestärkt würden, was auch eine bessere und raschere Bewertung und Überwachung der Voraussetzungen der Erforderlichkeit und Verhältnismäßigkeit ermöglichen würde.**

3.1.2 Einschränkungen bei der Weiterübermittlung von Daten

76. Laut Artikel 44 DSGVO dürfen personenbezogene Daten nur übermittelt oder weiterübermittelt werden, wenn das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird. Daher müssen personenbezogene Daten, die auf der Grundlage des Angemessenheitsbeschlusses aus dem EWR in das Vereinigte Königreich übermittelt werden, ein der Sache nach gleichwertiges Schutzniveau wie das des EU-Datenschutzrahmens genießen. **Das bedeutet, dass die Rechtsvorschriften des Vereinigten Königreichs den EU-Rechtsvorschriften nicht nur in Bezug auf die Verarbeitung von in das Vereinigte Königreich auf Grundlage des Beschlussentwurfs übermittelten personenbezogenen Daten „der Sache nach gleichwertig" sein müssen, sondern dass auch durch die im Vereinigten Königreich geltenden Vorschriften für die Weiterübermittlung dieser Daten in Drittländer sichergestellt sein muss, dass ein der Sache nach gleichwertiges Schutzniveau fortlaufend gewährleistet wird.**

77. Daher muss jede Weiterübermittlung personenbezogener Daten aus dem EWR, die aus dem Vereinigten Königreich in ein anderes Drittland erfolgt, durch geeignete Garantien geschützt sein oder im Einklang mit den Ausnahmeregelungen[44] stehen, um den Fortbestand des durch die EU-Rechtsvorschriften gewährten Schutzes sicherzustellen. **Wenn ein solcher Schutz nicht geboten werden kann, sollten personenbezogene Daten aus dem EWR nicht weiterübermittelt werden.**

78. Der EDSA erkennt an, dass das Vereinigte Königreich Kapitel V der EU-DSGVO größtenteils in die UK-DSGVO (Artikel 44–49) und in den DPA von 2018[45] übernommen hat. **Dennoch hat der EDSA festgestellt, dass bestimmte Aspekte des Rechtsrahmens des Vereinigten Königreichs in Bezug auf die Weiterübermittlung das Schutzniveau für personenbezogene Daten, die aus dem EWR übermittelt werden, untergraben könnten.**

79. **Die erste Herausforderung**, die der EDSA festgestellt hat, betrifft die Anerkennung von Drittländern, internationalen Organisationen oder Gebieten[46] als Empfänger mit einem angemessenen Schutzniveau durch das Vereinigte Königreich nach dem im DPA von 2018 festgelegten Verfahren. Es ist nämlich möglich, dass personenbezogene Daten aus dem EWR auf der Grundlage einer künftigen

[44] Siehe Artikel 49 UK-DSGVO.
[45] Siehe die Artikel 17A, 17B, 17C und 18 des DPA von 2018.
[46] Siehe Artikel 17A des DPA von 2018.

möglichen Angemessenheitsregelung des Vereinigten Königreichs[47] aus dem Vereinigten Königreich in andere Drittländer weiterübermittelt werden.

80. Wie in Erwägungsgrund 77 des Beschlussentwurfs erläutert, ist der Secretary of State befugt, nach Konsultation des ICO[48] anzuerkennen, dass ein Drittland (oder ein Gebiet oder ein Sektor in diesem Drittland), eine internationale Organisation oder eine Beschreibung eines solchen Landes, eines solchen Gebiets, eines solchen Sektors oder einer solchen Organisation ein angemessenes Schutzniveau für personenbezogene Daten bietet. Bei der Beurteilung der Angemessenheit des Schutzniveaus muss der Secretary of State dieselben Elemente berücksichtigen, die die Europäische Kommission nach Artikel 45 Absatz 2 Buchstaben a bis c DSGVO in Verbindung mit Erwägungsgrund 104 DSGVO und der beibehaltenen EU-Rechtsprechung prüfen muss. Dies bedeutet, dass bei der Beurteilung des angemessenen Schutzniveaus eines Drittlands maßgeblich sein muss, ob dieses Drittland ein Schutzniveau bietet, das dem im Vereinigten Königreich garantierten Schutzniveau „der Sache nach gleichwertig" ist. Zwar stellt der EDSA fest, dass das Vereinigte Königreich gemäß der UK-DSGVO anerkennen kann, dass bestimmte Gebiete im Sinne des Datenschutzrahmens des Vereinigten Königreichs ein angemessenes Schutzniveau bieten, doch er weist auch darauf hin, dass für diese Gebiete bislang möglicherweise noch kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, in dem ein Schutzniveau anerkannt wird, das dem in der EU garantierten Schutzniveau „der Sache nach gleichwertig" ist. Dies könnte zu möglichen Risiken beim Schutz personenbezogener Daten führen, die aus dem EWR übermittelt werden, vor allem wenn der Datenschutzrahmen des Vereinigten Königreichs künftig vom EU-Besitzstand abweichen sollte. Es sei darauf hingewiesen, dass im Juli 2020 in dem richtungweisenden Urteil des EuGH in der Rechtssache Schrems II[49] der Beschluss über den EU-US-Datenschutzschild für ungültig erklärt wurde, da nach Auffassung des EuGH der Rechtsrahmen der USA nicht als der Sache nach gleichwertig mit dem der EU angesehen werden konnte. Allerdings sind die bereits erlassenen EuGH-Urteile, die als im Rechtsrahmen des Vereinigten Königreichs beibehaltene Rechtsprechung betrachtet werden, möglicherweise für das Vereinigte Königreich nicht mehr bindend, insbesondere weil nach Ablauf des Brückenzeitraums das Vereinigte Königreich beibehaltenes Unionsrecht ändern kann und sein Supreme Court an keinerlei beibehaltene Rechtsprechung der EU mehr gebunden ist.[50]

81. **Der EDSA bittet die Europäische Kommission, das Verfahren und die Kriterien für die Angemessenheitsbewertung anderer Drittländer durch die Behörden des Vereinigten Königreichs genau zu überwachen, insbesondere in Bezug auf Drittländer, die von der EU nicht als angemessen im Sinne der DSGVO anerkannt wurden. Er regt ferner an, dass die Europäische Kommission in Fällen, in denen sie feststellt, dass ein Drittland, das vom Vereinigten Königreich für angemessen befunden wurde, kein dem in der EU gewährleisteten Schutzniveau der Sache nach gleichwertiges Schutzniveau sicherstellt, alle erforderlichen Schritte (wie eine Änderung des Angemessenheitsbeschlusses in Bezug auf das Vereinigte Königreich) unternimmt, um spezifische Garantien für aus dem EWR stammende personenbezogene Daten einzuführen, und/oder die Aussetzung des Angemessenheitsbeschlusses in Bezug auf das Vereinigte Königreich in Erwägung zieht, wenn personenbezogene Daten, die aus dem EWR in das Vereinigte Königreich übermittelt**

[47] Das Äquivalent des Vereinigten Königreichs zu einem Angemessenheitsbeschluss gemäß der DSGVO.
[48] Siehe Artikel 182 Absatz 2 des DPA von 2018. Siehe auch die Vereinbarung über die Funktion des ICO bezüglich neuer Angemessenheitsbewertungen des Vereinigten Königreichs, 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/.
[49] Siehe Schrems II.
[50] Siehe Artikel 6 Absätze 3 bis 6 des European Union (Withdrawal) Act von 2018.

werden, auf der Grundlage einer Angemessenheitsregelung des Vereinigten Königreichs in das betreffende Drittland weiterübermittelt werden.

82. **Die zweite Herausforderung** betrifft die bevorstehende Überprüfung der bereits bestehenden durch die Europäische Kommission gemäß der Richtlinie 95/46/EG erlassenen Angemessenheitsbeschlüsse. Durch diese Überprüfung könnte die Europäische Kommission zu der Entscheidung kommen, dass bestimmte Länder, die bis jetzt von einem Angemessenheitsbeschluss profitiert haben, angesichts der geltenden EU-Rechtsvorschriften und der jüngsten Rechtsprechung kein der Sache nach gleichwertiges Schutzniveau mehr bieten. Wie aus Anhang 21 Nummer 4 des DPA von 2018 hervorgeht, hat das Vereinigte Königreich jedoch bereits anerkannt, dass diese Länder ein angemessenes Schutzniveau bieten. Obwohl der Secretary of State innerhalb von vier Jahren eine Überprüfung dieser Angemessenheitsfeststellungen vornehmen muss, stellt die Europäische Kommission in ihrem Beschlussentwurf fest, dass diese Angemessenheitsfeststellungen nicht automatisch nichtig werden, wenn der Secretary of State die erforderliche Überprüfung nicht innerhalb der festgelegten Vierjahresfrist vornimmt.[51]

83. **Der EDSA ersucht die Europäische Kommission, zu überwachen, ob nach Abschluss der Überprüfung der bereits bestehenden Angemessenheitsbeschlüsse durch die EU ein Land, für das festgestellt wurde, dass es kein angemessenes Schutzniveau mehr bietet, vom Vereinigten Königreich noch immer als solches betrachtet wird. Sollte dies der Fall sein, empfiehlt der EDSA der Europäischen Kommission auf der Grundlage der Erwägungsgründe 277 bis 280 des Beschlussentwurfs, geeignete Abhilfemaßnahmen zu ergreifen (beispielsweise durch Änderung des Angemessenheitsbeschlusses), um spezifische Anforderungen für personenbezogene Daten, die aus dem EWR stammen, hinzuzufügen, und/oder durch Aussetzung des Angemessenheitsbeschlusses, wenn personenbezogene Daten, die aus dem EWR in das Vereinigte Königreich übermittelt werden, in das betreffende Drittland weiterübermittelt werden. Der EDSA empfiehlt der Europäischen Kommission, diese Überwachung während der Geltungsdauer des Angemessenheitsbeschlusses fortzusetzen.**

84. **Die dritte Herausforderung** betrifft die Weiterübermittlung personenbezogener Daten aus dem EWR in Länder ohne angemessenes Schutzniveau auf der Grundlage der in den Artikeln 46 und 47 UK-DSGVO vorgesehenen Übermittlungsinstrumente. Obwohl in der UK-DSGVO dieselben Übermittlungsinstrumente vorgesehen sind wie in der EU-DSGVO, betont der EDSA, dass sichergestellt werden muss, dass die darin enthaltenen Garantien einen wirksamen Schutz im Drittland bieten, insbesondere vor dem Hintergrund des Schrems-II-Urteils.

85. Nach der Entscheidung in der Rechtssache Schrems II, in welcher der EuGH daran erinnert, dass der in der EU geltende Schutz für personenbezogene Daten auch überall dort gewährleistet sein muss, wohin die Daten übermittelt werden, hat der EDSA bereits erste Empfehlungen für zusätzliche Maßnahmen[52] angenommen, um Exporteure gegebenenfalls dabei zu unterstützen, sicherzustellen, dass betroffenen Personen ein Schutzniveau gewährt wird, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

[51] Siehe Erwägungsgrund 82 des Beschlussentwurfs.

[52] Siehe Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 10. November 2020, die nach Konsultation der Öffentlichkeit derzeit fertiggestellt werden, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf.

86. Dem EuGH zufolge obliegt es Datenexporteuren, in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Datenimporteur im Drittland – zu prüfen, ob das Recht oder die Praxis des Drittlands die Wirksamkeit der Garantien, die in den in Artikel 46 DSGVO genannten Übermittlungsinstrumenten enthalten sind, beeinträchtigt.[53] In diesem Fall sollten die Datenexporteure zusätzliche Maßnahmen ergreifen, um die Rechtsschutzlücken zu schließen und die Einhaltung des unionsrechtlichen Schutzniveaus zu gewährleisten.

87. **Der EDSA rät der Kommission, zwecks Gewährleistung des Fortbestands des Schutzes in den Beschlussentwurf Zusicherungen dafür aufzunehmen, dass Datenexporteure im Vereinigten Königreich bei jedem Rückgriff auf die in den Artikeln 46 und 47 UK-DSGVO vorgesehenen Übermittlungsinstrumente für die Weiterübermittlung von Daten aus dem EWR in andere Drittländer in jedem Einzelfall den Datenschutzrahmen des Drittlandes bewerten und erforderlichenfalls geeignete Maßnahmen ergreifen, um die wirksame Einhaltung der in dem gewählten Übermittlungsinstrument enthaltenen Garantien sicherzustellen, um ein Schutzniveau zu gewährleisten, das dem Schutzniveau in der EU der Sache nach gleichwertig ist. Der EDSA hebt hervor, dass ohne diese Zusicherungen die Gefahr besteht, dass das Schutzniveau, das der Sache nach dem innerhalb der EU gewährleisteten Schutzniveau gleichwertig sein muss, durch Weiterübermittlungen aus dem Vereinigten Königreich verwässert wird.**

88. **Die vierte Herausforderung** in Bezug auf die Weiterübermittlung betrifft die vom Vereinigten Königreich geschlossenen oder künftig zu schließenden internationalen Übereinkünfte und den möglichen direkten Zugriff von Behörden aus Drittländern, die Vertragsparteien dieser Übereinkünfte sind, auf personenbezogene Daten aus dem EWR. Der EDSA hat in dieser Hinsicht große Bedenken wegen des bereits geschlossenen CLOUD-Act-Abkommens, und die Europäische Kommission räumt ein, dass dieses eine Herausforderung darstellt, indem sie betont, dass „ein mögliches Inkrafttreten des Abkommens sich auf das in diesem Beschluss bewertete Schutzniveau auswirken kann“[54]. Nach diesem Abkommen würden ab dem Zeitpunkt seines Inkrafttretens personenbezogene Daten, die auf Grundlage des Beschlussentwurfs aus dem EWR in das Vereinigte Königreich übermittelt werden, den Bestimmungen dieses Abkommens unterliegen, die einen direkten Zugriff der US-Behörden vorsehen, was sich auf den Datenschutzrahmen des Vereinigten Königreichs auswirken würde, u. a. auf die Bestimmungen zur Weiterübermittlung. Infolgedessen kann das Schutzniveau für die aus dem EWR übermittelten Daten durch die Bestimmungen des mit den USA geschlossenen Abkommens erheblich beeinträchtigt werden und sich auf das Schutzniveau für solche Daten auswirken. Der EDSA stellt in diesem Zusammenhang fest, dass sich die Europäische Kommission in Erwägungsgrund 153 ihres Beschlussentwurfs auf Erläuterungen der Behörden des Vereinigten Königreichs bezieht, ohne konkrete schriftliche Zusicherungen oder Verpflichtungen zu zitieren oder zu benennen oder auf spezifische Rechtsvorschriften des Vereinigten Königreichs zu verweisen, die diesen Erläuterungen Wirkung verleihen würden.

89. Der EDSA hat diese Bedenken bereits in einem Schreiben an das Europäische Parlament vom 15. Juni 2020[55] vorgebracht. Der EDSA hatte darauf hingewiesen, dass er angesichts des „EU-Besitzstands im Bereich des Datenschutzes und insbesondere der Datenschutz-Grundverordnung und der Richtlinie zum Datenschutz bei der Strafverfolgung“ Zweifel hege, dass die in dem Abkommen enthaltenen Garantien für den Zugriff auf personenbezogene Daten im Vereinigten Königreich unter bestimmten

[53] Siehe Schrems II, Rn. 134.
[54] Siehe Erwägungsgrund 153 des Beschlussentwurfs.
[55] Siehe die Antwort des EDSA an die MdEP Sophie in't Veld und Moritz Körner zum CLOUD-Act-Abkommen, ergangen am 15. Juni 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

Umständen, unter denen Offenlegungspflichten gegenüber den USA erforderlich wären, weiterhin gelten würden und diese Garantien angesichts der EU-Standards ausreichten, um das in der EU gewährte Schutzniveau nicht zu untergraben.

90. Darüber hinaus können die Bestimmungen des CLOUD-Act-Abkommens erhebliche Auswirkungen auf die materiell- und verfahrensrechtlichen Bedingungen haben, nach denen US-Behörden auf personenbezogene Daten, die sich bei Verantwortlichen oder Auftragsverarbeitern im Vereinigten Königreich befinden, direkt zugreifen können, was sich auf das nach britischem Recht garantierte Schutzniveau auswirkt. Um ein Schutzniveau zu bieten, das dem im EU-Recht garantierten Schutzniveau der Sache nach gleichwertig ist, ist es beispielsweise „von zentraler Bedeutung, dass die Garantien gemäß einer solchen Übereinkunft eine obligatorische vorherige richterliche Genehmigung als grundlegende Garantie für den Zugriff auf Metadaten und Inhaltsdaten umfassen. Der EDSA merkt zwar an, dass sich das Abkommen auf die Anwendung des innerstaatlichen Rechts bezieht, konnte aber auf der Grundlage seiner vorläufigen Bewertung in dem zwischen dem Vereinigten Königreich und den USA geschlossenen Abkommen keine entsprechende klare Bestimmung finden."[56]

91. Die Europäische Kommission betont zwar, dass für nach dem Abkommen abgerufene Daten Schutzvorkehrungen bestehen würden, die den spezifischen Garantien, die das Rahmenabkommen zwischen der EU und den USA vorsieht, gleichwertig sind. Allerdings hat der EDSA Bedenken, ob die Aufnahme dieser Garantien in das CLOUD-Act-Abkommen durch einen einfachen Verweis, der entsprechend Anwendung finden würde, das Kriterium klarer, präziser und zugänglicher Vorschriften für den Zugriff auf personenbezogene Daten erfüllen bzw. solche Garantien hinreichend verankern würde, damit sie wirksam und nach dem Recht des Vereinigten Königreichs einklagbar wären.

92. **Daher empfiehlt der EDSA, dass die Europäische Kommission klarstellt, wie und auf der Grundlage welches Rechtsinstruments Schutzvorkehrungen, die den spezifischen Garantien des Rahmenabkommens zwischen der EU und den USA gleichwertig sind, wirksam würden und nach britischem Recht bindend wären.**

93. Der EDSA stellt ferner fest, dass die Bestimmungen des CLOUD-Act-Abkommens in Verbindung mit Artikel 3 US CLOUD Act[57] Fragen hinsichtlich der tatsächlichen Anwendung der Garantien aufwerfen, die das Abkommen für den Zugriff US-amerikanischer Strafverfolgungsbehörden auf personenbezogene Daten im Vereinigten Königreich bietet, die von Anbietern elektronischer Kommunikationsdienste oder Betreibern von Remote-Computing-Diensten (im Folgenden „Anbieter von Kommunikationsdiensten") verarbeitet werden und die in die Zuständigkeit der USA fallen. Sollte ein im Vereinigten Königreich ansässiger Anbieter von Kommunikationsdiensten dem Recht der USA unterliegen (z. B. weil es sich um die Tochtergesellschaft eines US-amerikanischen Unternehmens handelt), bleibt zu prüfen, ob die US-Behörden verpflichtet wären, sich beim Abruf dieser Daten auf das CLOUD-Act-Abkommen zu berufen. Zu dem Hinweis der Europäischen Kommission, dass besonders auf die Anwendung und Anpassung der Schutzvorkehrungen des Rahmenabkommens bezogen auf die spezifische Art von Übermittlungen geachtet werde, die unter das Abkommen zwischen dem Vereinigten Königreich und den USA fallen, betont der EDSA, dass auf der Grundlage seiner vorläufigen Bewertung nicht klar sei, ob die im CLOUD-Act-Abkommen verankerten Garantien und damit auch die im Rahmenabkommen zwischen der EU und den USA vorgesehenen Garantien

[56] Siehe oben genanntes Schreiben des EDSA.
[57] Siehe US CLOUD Act, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

für alle im Rahmen des US Cloud Act getätigten Zugriffsanforderungen von US-Behörden auf Daten im Vereinigten Königreich gelten würden bzw. ob sie überhaupt dafür gelten würden.

94. Möglicherweise geht das Vereinigte Königreich in Zukunft weitere internationale Übereinkünfte mit Drittländern oder Verpflichtungen gegenüber Drittländern ein, die für personenbezogene Daten gelten würden, die auf der Grundlage des Beschlussentwurfs aus dem EWR in das Vereinigte Königreich übermittelt werden.[58] Je nach den Bestimmungen dieser Übereinkünfte und der Anwendung spezifischer Schutzklauseln können diese internationalen Übereinkünfte, indem sie den Datenschutzrahmen des Vereinigten Königreichs berühren, auch erhebliche Auswirkungen auf die materiell- und verfahrensrechtlichen Bedingungen für den Zugriff von Behörden in Drittländern auf personenbezogene Daten im Vereinigten Königreich haben. Dies gilt insbesondere für den Entwurf eines zweiten Zusatzprotokolls zum Übereinkommen des Europarats über Computerkriminalität (im Folgenden „Budapester Übereinkommen"), das derzeit von den Vertragsparteien dieses Übereinkommens, zu denen mehrere Nicht-EU-Länder gehören, ausgehandelt wird. Dieser Protokollentwurf enthält nämlich Klauseln, die von den Parteien nach eigenem Ermessen aktiviert werden können, beispielsweise in Bezug auf die Ermächtigung, Zugriff auf Inhaltsdaten zu gewähren oder nicht. Während alle EU-Mitgliedstaaten die Klauseln im Einklang mit den EU-Datenschutzvorschriften aktivieren würden, wurde vom Vereinigten Königreich keine entsprechende Garantie abgegeben; es könnte somit erheblich von dem Schutzniveau abweichen, das innerhalb der EU geboten würde. Ein weiteres Beispiel für die oben dargelegte Problematik ist das Abkommen zwischen dem Vereinigten Königreich und Japan über eine umfassende Wirtschaftspartnerschaft[59] (Comprehensive Economic Partnership, „CEPA"), das erste Handelsabkommen des Vereinigten Königreichs nach dem Brexit, das am 1. Januar 2021 in Kraft getreten ist[60] und Bestimmungen über personenbezogene Daten enthält[61]. Der EDSA stellt ferner fest, dass das Vereinigte Königreich am 1. Februar 2021 formell seinen Antrag auf Beitritt zur umfassenden und fortschrittlichen Vereinbarung über eine transpazifische Partnerschaft („CPTPP") angekündigt hat, die das Abkommen über die Transpazifische Partnerschaft („TPP")[62] umfasst.

95. Der EDSA stellt fest, dass, abgesehen von dem CLOUD-Act-Abkommen, die oben genannten internationalen Übereinkünfte im Beschlussentwurf nicht thematisiert werden.

96. **Der EDSA ersucht die Europäische Kommission,**

[58] Siehe Abschnitt 2.3.3.

[59] Siehe Vereinigtes Königreich/Japan: Abkommen über eine umfassende Wirtschaftspartnerschaft zwischen dem Vereinigten Königreich und Japan [CS Japan Nr. 1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Siehe Leitlinien der Regierung des Vereinigten Königreichs zu Handelsabkommen des Vereinigten Königreichs mit Nicht-EU-Ländern, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Gemäß Artikel 8.80 Absatz 5 des CEPA verpflichten sich die Vertragsparteien, die Entwicklung von Mechanismen zur Förderung der Kompatibilität ihrer unterschiedlichen rechtlichen Ansätze beim Schutz von (personenbezogenen) Daten zu fördern. Gemäß Artikel 8.84 verpflichten sich die Vertragsparteien, die grenzüberschreitende Übermittlung von Daten (einschließlich personenbezogener Daten) auf elektronischem Wege nicht zu verbieten oder einzuschränken, wenn diese Tätigkeit der Unternehmensführung einer erfassten Person im Sinne des CEPA dient.

[62] Gemäß Artikel 14.11 Absatz 2 des TPP gestattet jede Vertragspartei die grenzüberschreitende Übermittlung von Daten (einschließlich personenbezogener Daten) auf elektronischem Wege, wenn diese Tätigkeit der Unternehmensführung einer erfassten Person dient.

- **die Wechselwirkungen zwischen dem Datenschutzrahmen des Vereinigten Königreichs und dessen internationalen Verpflichtungen – über das CLOUD-Act-Abkommen hinaus – zu untersuchen, um insbesondere den Fortbestand des Schutzniveaus bei Weiterübermittlungen personenbezogener Daten, die auf der Grundlage eines Angemessenheitsbeschlusses vom EWR in das Vereinigte Königreich übermittelt wurden, in andere Drittländer sicherzustellen, und des Weiteren fortlaufend zu überwachen, ob der Abschluss weiterer internationaler Übereinkünfte zwischen dem Vereinigten Königreich und Drittländern das in der EU gebotene Schutzniveau für personenbezogene Daten untergraben könnte, und erforderlichenfalls entsprechende Maßnahmen zu ergreifen,**

- **dem EDSA in Bezug auf die in Erwägungsgrund 153 des Beschlussentwurfs erwähnte Erläuterung der möglichen Anwendung und Umsetzung des CLOUD-Act-Abkommens schriftliche Zusagen der Behörden des Vereinigten Königreichs zu übermitteln und spezifische Bestimmungen im britischen Recht zu nennen,**

- **in diesem Zusammenhang zu überwachen, ob zusätzlich zu den Garantien, die durch eine angemessene Umsetzung der Anpassung des Rahmenabkommens zwischen der EU und den USA geboten werden könnten, das CLOUD-Act-Abkommen geeignete zusätzliche Garantien bietet, unter Berücksichtigung des Sensibilitätsgrads der betroffenen Datenkategorien und der einzigartigen Anforderungen der Übermittlung elektronischer Beweismittel unmittelbar durch Anbieter von Kommunikationsdiensten anstatt zwischen Behörden,**

- **die Auswirkungen und potenziellen Risiken der Bestimmungen zu personenbezogenen Daten, die in kürzlich vom Vereinigten Königreich unterzeichneten internationalen Übereinkünfte wie dem CEPA enthalten sind, zu bewerten.**

97. **Die fünfte Herausforderung** betrifft die Anwendung von Ausnahmeregelungen für die Übermittlung personenbezogener Daten in ein Drittland. Obwohl die in der UK-DSGVO vorhandenen Ausnahmeregelungen dieselben sind, die auch die EU-DSGVO vorsieht, ist es wichtig, dass die Auslegung zur Anwendung dieser Ausnahmeregelungen durch das ICO an die des EDSA angeglichen ist. Wenn dies nicht der Fall ist oder wenn das Vereinigte Königreich in der Zukunft von dieser Auslegung abweicht, bestünde die Gefahr, dass das Schutzniveau von Daten, die aus dem EWR über das Vereinigte Königreich in Drittländer übermittelt werden, untergraben wird.

98. **Der EDSA ersucht die Europäische Kommission, im Rahmen ihrer Überwachungsaufgabe insbesondere zu prüfen, ob die Auslegung des Vereinigten Königreichs in Bezug auf die Anwendung von Ausnahmeregelungen stets an die Auslegung der EU angeglichen ist. Wenn das Vereinigte Königreich jedoch bei der Anwendung von Ausnahmeregelungen einer anderen Auslegung folgt, die das Schutzniveau untergräbt, ist es von zentraler Bedeutung, dass die Europäische Kommission die erforderlichen Schritte unternimmt und den Angemessenheitsbeschluss ändert, um sicherzustellen, dass das Schutzniveau für personenbezogene Daten, die aus dem EWR in das Vereinigte Königreich übermittelt werden, nicht untergraben wird, wenn diese Daten auf der Grundlage einer anderen Auslegung von Ausnahmeregelungen aus dem Vereinigten Königreich in Drittländer weiterübermittelt werden.**

99. **Die sechste Herausforderung,** die letzte für diesen Abschnitt, bezieht sich auf das Fehlen von Schutzmaßnahmen gemäß Artikel 48 DSGVO im Datenschutzrahmen des Vereinigten Königreichs.

100. Die Europäische Kommission stellt in ihrem Beschlussentwurf klar, dass in Ermangelung von Angemessenheitsregelungen oder geeigneten Garantien eine Übermittlung nur auf der Grundlage von Ausnahmeregelungen gemäß Artikel 49 UK-DSGVO erfolgen kann, „mit Ausnahme von Artikel 48

der Verordnung (EU) 2016/679, den das Vereinigte Königreich nicht in die UK-DSGVO aufgenommen hat".[63] Dass in Bezug auf Übermittlungen oder Offenlegungen im Anschluss an ein Urteil eines Gerichts oder an eine Entscheidung einer Verwaltungsbehörde aus einem anderen Drittland keine Bestimmung im britischen Datenschutzrahmen verankert ist, die der Sache nach gleichwertig mit Artikel 48 EU-DSGVO ist, kann zu Rechtsunsicherheit darüber führen, ob das Schutzniveau für personenbezogene Daten, die auf Grundlage des Beschlussentwurfs aus dem EWR in das Vereinigte Königreich übermittelt werden, wesentlich beeinträchtigt würde.

101. In seiner Referenzgrundlage für Angemessenheit im Sinne der DSGVO weist der EDSA darauf hin, dass bei Weiterübermittlungen „die Weiterleitung der personenbezogenen Daten des ursprünglichen Empfängers der ursprünglichen Datenübermittlung [...] nur zulässig sein [sollte], wenn der weitere Empfänger ebenfalls Vorschriften unterliegt und dadurch ein angemessenes Schutzniveau gewährleistet und die einschlägigen Anweisungen für die Verarbeitung von Daten im Namen des Verantwortlichen befolgt"[64]. Darüber hinaus betont der EDSA, dass „der ursprüngliche Empfänger von aus der EU übermittelten Daten verpflichtet [ist] sicherzustellen, dass ohne Vorliegen eines Angemessenheitsbeschlusses geeignete Garantien für die Weiterleitung der Daten gegeben sind. Solche Weiterleitungen von Daten sollten nur für begrenzte und bestimmte Zwecke erfolgen und solange es eine Rechtsgrundlage für die Verarbeitung gibt."[65] Als Bestandteil von Kapitel V der DSGVO muss Artikel 48 bei der Beurteilung, ob der Rechtsrahmen des Vereinigten Königreichs in diesem Punkt ein der Sache nach gleichwertiges Schutzniveau gewährleistet, in vollem Umfang berücksichtigt werden.[66]

102. Der EDSA verweist in diesem Zusammenhang nachdrücklich auf die Rechtsprechung des EuGH in Bezug auf die Gefahr des Missbrauchs oder des unrechtmäßigen Zugriffs und der unrechtmäßigen Nutzung von Daten und hält insbesondere fest: „Zu dem innerhalb der Union garantierten Schutzniveau der Freiheiten und Grundrechte ist festzustellen, dass eine Unionsregelung, die einen Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte enthält, nach ständiger Rechtsprechung des Gerichtshofs klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen muss, so dass die Personen, deren personenbezogene Daten 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. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht."[67]

103. Der EDSA stellt in diesem Zusammenhang fest, dass, ausgehend von den Informationen im Beschlussentwurf, der Datenschutzrahmen des Vereinigten Königreichs nicht eindeutig vorsieht, dass jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, jedenfalls nur dann anerkannt oder vollstreckbar werden dürfen, wenn sie auf eine in Kraft befindliche internationale Übereinkunft, wie etwa ein Rechtshilfeabkommen zwischen dem

[63] Siehe Fußnote 78 des Beschlussentwurfs.
[64] Siehe WP 254/rev.01, S. 6.
[65] Siehe WP 254/rev.01, S. 6.
[66] Siehe insbesondere Artikel 44 DSGVO, wo es im letzter Satz heißt: „Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird."
[67] Siehe Schrems I, Rn. 91.

ersuchenden Drittland und dem Vereinigten Königreich, gestützt sind. Artikel 48 DSGVO ist eine grundlegende Bestimmung des Kapitels V der DSGVO, da er vorschreibt, dass die Übermittlung oder Offenlegung personenbezogener Daten aufgrund eines Urteils oder einer Entscheidung eines Gerichts oder einer Verwaltungsbehörde eines Drittlands unbeschadet anderer Gründe für die Übermittlung gemäß Kapitel V der DSGVO nur dann anerkannt oder vollstreckbar ist, wenn sie auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt ist. Der EDSA weist auch darauf hin, dass „ein Ersuchen einer ausländischen Behörde [...] an sich keinen Rechtsgrund für die Übermittlung [darstellt]. Die Anordnung kann nur anerkannt werden, ‚wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt' ist."[68] Daher ist es ausschlaggebend, dass im Recht des Vereinigten Königreichs der Sache nach gleichwertige Bestimmungen benannt werden können.

104. In dem Beschlussentwurf führt die Europäische Kommission Erläuterungen der Behörden des Vereinigten Königreichs an, denen zufolge nach dem Common Law bzw. Gesetzesrecht ein ausländisches Urteil, in dem Daten angefordert werden, im Vereinigten Königreich ohne eine internationale Übereinkunft nicht vollstreckbar ist und für jegliche Übermittlung von Daten auf Ersuchen eines ausländischen Gerichts oder einer ausländischen Verwaltungsbehörde ein Übermittlungsinstrument wie eine Angemessenheitsregelung oder geeignete Garantien erforderlich sind, es sei denn, es gilt eine Ausnahmeregelung gemäß Artikel 49 UK-DSGVO. Der EDSA hat jedoch die diesbezügliche Korrespondenz zwischen der Europäischen Kommission und den Behörden des Vereinigten Königreichs nicht erhalten[69] und ist daher nicht in der Lage, zu analysieren und unabhängig zu bewerten, ob die von den Behörden des Vereinigten Königreichs gewährten Garantien ausreichen, um in Bezug auf die in Artikel 48 DSGVO vorgesehenen Garantien ein der Sache nach gleichwertiges Schutzniveau zu gewährleisten.

105. **Der EDSA ersucht die Europäische Kommission, weitere Zusicherungen und spezifische Verweise auf die Rechtsvorschriften des Vereinigten Königreichs zu geben, mit denen sichergestellt wird, dass das Schutzniveau, das der Rechtsrahmen des Vereinigten Königreichs gewährleistet, dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist. Daher ersucht der EDSA die Europäische Kommission, in Bezug auf die Umsetzung von Schutzvorkehrungen, die jenen, die in Artikel 48 DSGVO vorgesehen sind, der Sache nach gleichwertig sind, schriftliche Erklärungen und Zusagen der Behörden des Vereinigten Königreichs vorzulegen.**

106. **Der EDSA ist der Auffassung, dass es umso wichtiger ist, Bestimmungen im Recht des Vereinigten Königreichs zu benennen, die ein der Sache nach gleichwertiges Schutzniveau wie die in Artikel 48 DSGVO vorgesehenen Garantien sicherstellen, als unlängst bereits Bedenken wegen etwaiger Zugriffsanforderungen von Behörden der USA oder anderer Drittländer auf Daten im Vereinigten Königreich geäußert worden sind und gemäß dem Angemessenheitsbeschluss personenbezogene Daten aus dem EWR in das Vereinigte Königreich übermittelt werden könnten, ohne dass weitere Garantien oder bindende Zusagen des Empfängers in Bezug auf Zugriffsanforderungen anderer Drittstaatsbehörden auf Daten vorliegen.**

[68] Siehe Anhang der Gemeinsamen Antwort des EDSA und des EDSB an den LIBE-Ausschuss bezüglich der Auswirkungen des US Cloud Act auf den europäischen Rechtsrahmen für den Schutz personenbezogener Daten, angenommen am 10. Juli 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_de.
[69] Siehe Fußnote 78 des Beschlussentwurfs.

3.2 Verfahrens- und Durchsetzungsmechanismen

107. Ausgehend von der in der Referenzgrundlage für Angemessenheit im Sinne der DSGVO festgelegten Kriterien hat der EDSA folgende Aspekte des Datenschutzrahmens des Vereinigten Königreichs analysiert, die vom Beschlussentwurf erfasst werden: das Bestehen und wirksame Funktionieren einer unabhängigen Aufsichtsbehörde, das Vorhandensein eines Systems, das ein hohes Maß an Konformität gewährleistet, sowie das Bestehen eines Systems für den Zugang zu geeigneten Rechtsschutzverfahren, die natürlichen Personen in der EU die Möglichkeit bieten, ihre Rechte wahrzunehmen und Rechtsbehelfe einzulegen, ohne dabei auf große Hürden zu stoßen.

3.2.1 Zuständige unabhängige Aufsichtsbehörde

108. Der EDSA begrüßt die Bemühungen der Europäischen Kommission, in Kapitel 2.6 des Beschlussentwurfs die Einrichtung, die Arbeitsweise und die Befugnisse der Aufsichtsbehörde des Vereinigten Königreichs ausführlich zu untersuchen. Im Vereinigten Königreich ist der Information Commissioner (im Folgenden „IC“) als Datenschutzbeauftragter mit der Aufsicht und der Durchsetzung der Einhaltung der UK-DSGVO und des DPA von 2018 betraut. Gemäß Anhang 12 des DPA von 2018 ist der IC als „Corporation Sole“ eine eigenständige juristische Einheit, die aus einer einzigen Person besteht und von einem Büro, dem ICO, unterstützt wird.

109. In Bezug auf die Unabhängigkeit des IC hebt der EDSA hervor, dass in Artikel 51 UK- nicht ausdrücklich klargestellt wird, dass es sich bei dem IC um eine unabhängige Behörde handelt, wie dies in Artikel 51 EU-DSGVO in Bezug auf Aufsichtsbehörden festgelegt ist. Der EDSA erkennt jedoch an, dass in Bezug auf die Unabhängigkeit die entsprechenden in Artikel 52 Absätze 1 bis 3 EU-DSGVO vorgesehenen Vorschriften in ähnlicher Weise in Artikel 52 UK-DSGVO übernommen wurden.

110. Darüber hinaus weist der EDSA darauf hin, dass Artikel 52 UK-DSGVO keine Verpflichtungen enthält, die jenen in Artikel 52 Absätze 4 bis 6 EU-DSGVO entsprechen würden, mit denen ausdrücklich sichergestellt wird, dass der jeweiligen Aufsichtsbehörde die Ressourcen zur Verfügung gestellt werden, die für die wirksame Wahrnehmung ihrer Aufgaben und die Ausübung ihrer Befugnisse erforderlich sind. Der EDSA erkennt jedoch an, dass der DPA von 2018 Bestimmungen enthält, mit denen eine angemessene Finanzierung des ICO sichergestellt werden soll[70], und dass das ICO im Vergleich zu den Aufsichtsbehörden in der EU bzw. im EWR derzeit eine der größten Aufsichtsbehörden ist. Da eine kontinuierliche Zuweisung angemessener Ressourcen, insbesondere von Personal und Haushaltsmitteln[71], unerlässlich ist, um das ordnungsgemäße Funktionieren einer Aufsichtsbehörde zwecks Erfüllung aller ihr übertragenen Aufgaben zu gewährleisten, und die Aufsichtsbehörden erst kürzlich auch vom Europäischen Parlament als überaus wichtig eingestuft wurden[72], hält es der EDSA für wesentlich, künftige Entwicklungen in diesem Bereich besonders aufmerksam zu verfolgen.

111. **Daher rät der EDSA der Europäischen Kommission, bezüglich der Zuweisung von Ressourcen an das ICO alle Entwicklungen zu beobachten, die der ordnungsgemäßen Erfüllung der Aufgaben des ICO abträglich wären.**

[70] Siehe die Artikel 137, 138 und 182 sowie Anhang 12 Artikel 9 des DPA von 2018.
[71] Siehe WP 254/rev.01, S. 8.
[72] 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, Ziffer 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_DE.html.

3.2.2 Vorhandensein eines Datenschutzsystems, das ein hohes Maß an Konformität gewährleistet

112. Der Beschlussentwurf beinhaltet eine umfassende Prüfung der Befugnisse, mit denen das ICO gemäß Artikel 58 UK-DSGVOund des DPA von 2018 ausgestattet ist, um die Überwachung und Durchsetzung der Rechtsvorschriften sicherzustellen. Der EDSA erkennt an, dass in Bezug auf die Befugnisse von Aufsichtsbehörden die entsprechenden in Artikel 58 EU-DSGVO vorgesehenen Vorschriften in ähnlicher Weise in Artikel 58 UK-DSGVO übernommen wurden. In Bezug auf die Befugnis zur Verhängung von Geldbußen je nach den Umständen des Einzelfalls enthält Artikel 83 UK-DSGVO ähnliche Bestimmungen und Höchstbeträge wie Artikel 83 EU-DSGVO. Daher ist der EDSA der Auffassung, dass der Rechtsrahmen des Vereinigten Königreichs in diesem Bereich derzeit mit den Standards des einschlägigen EU-Rechts im Einklang steht. Dennoch betont der EDSA in diesem Zusammenhang, dass das Bestehen *wirksamer* Sanktionen eine wichtige Rolle dabei spielt, die Einhaltung von Vorschriften sicherzustellen.[73]

113. **Vor diesem Hintergrund rät der EDSA der Europäischen Kommission, die Wirksamkeit der im Datenschutzrahmen des Vereinigten Königreichs vorgesehenen Sanktionen und Rechtsbehelfe zu überwachen.**

3.2.3 Das Datenschutzsystem muss betroffenen Personen bei der Ausübung ihrer Rechte Unterstützung und Hilfe sowie geeignete Rechtsschutzverfahren bieten

114. Ein wirksamer Aufsichtsmechanismus, der eine unabhängige Untersuchung von Beschwerden ermöglicht, um Verletzungen der Rechte betroffener Personen in der Praxis festzustellen und zu ahnden, sowie wirksame administrative und gerichtliche Rechtsschutzverfahren (einschließlich Schadenersatz für Schäden infolge der rechtswidrigen Verarbeitung personenbezogener Daten der betroffenen Person) sind Schlüsselelemente für die Beurteilung, ob ein Datenschutzsystem ein angemessenes Schutzniveau bietet.

115. Der EDSA begrüßt, dass das ICO auf seiner Website umfassende Informationen und Leitlinien bereitstellt, die darauf abzielen, die Verantwortlichen und Auftragsverarbeiter für ihre Aufgaben und Pflichten zu sensibilisieren und betroffene Personen dabei zu unterstützen, sich über ihre Rechte in Bezug auf personenbezogene Daten zu informieren und ihre individuellen Rechte gemäß der UK-DSGVO und dem DPA von 2018 geltend zu machen.

116. **Ungeachtet des derzeitigen Stands der Dinge empfiehlt der EDSA der Europäischen Kommission, fortlaufend zu beobachten, inwieweit das ICO insbesondere natürlichen Personen, deren personenbezogene Daten auf der Grundlage des Angemessenheitsbeschlusses in das Vereinigte Königreich übermittelt wurden, bei der Wahrnehmung ihrer Rechte gemäß der Datenschutzregelung des Vereinigten Königreichs behilflich ist.**

4. ZUGRIFF AUF UND NUTZUNG VON AUS DER EUR ÜBERMITTELTEN PERSONENBEZOGENEN DATEN DURCH BEHÖRDEN IM VEREINIGTEN KÖNIGREICH

4.1 Zugriff und Nutzung durch Behörden des Vereinigten Königreichs für Strafverfolgungszwecke

[73] Siehe WP 254/rev.01, S. 8.

4.1.1 Rechtsgrundlagen und anwendbare Beschränkungen/Garantien

117. In Bezug auf die von der Europäischen Kommission durchgeführte und in den Erwägungsgründen 132 ff. des Beschlussentwurfs, in denen es **um den Zugriff für Strafverfolgungszwecke** geht, dokumentierte Bewertung, stellt die Europäische Kommission differenzierte und detaillierte Informationen bereit und gelangt zu grundsätzlich nachvollziehbaren Schlussfolgerungen. Daher verzichtet der EDSA in dieser Stellungnahme darauf, den Großteil der sachbezogenen Erkenntnisse und Bewertungen zu wiederholen. In einigen Punkten reicht jedoch die Darstellung der Fakten bzw. die Erläuterung der Schlussfolgerungen für eine Befürwortung durch den EDSA nicht aus.

4.1.1.1 Die Nutzung der Einwilligung

118. Der EDSA nimmt zur Kenntnis, dass die Europäische Kommission in Fußnote 184 des Beschlussentwurfs[74] darauf hinweist, dass **die Nutzung der Einwilligung** in einem Angemessenheitsszenario nicht relevant sei, da in Übermittlungssituationen die Daten einer betroffenen Person nicht unmittelbar von einer britischen Strafverfolgungsbehörde auf der Grundlage einer Einwilligung erhoben würden. Folglich wird die Nutzung der Einwilligung als Rechtsgrundlage bei der Polizeiarbeit von der Europäischen Kommission nicht bewertet.

119. In diesem Zusammenhang erinnert der EDSA daran, dass nach Artikel 45 Absatz 2 Buchstabe a DSGVO eine ganze Reihe von Elementen geprüft werden muss, die nicht auf die Übermittlungssituation beschränkt sind, darunter auch „die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die [...] geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art — auch in Bezug auf [...] Strafrecht".

120. Auch auf der Grundlage der Informationen, die die Europäische Kommission in Erwägungsgrund 38 ihres Entwurfs eines Durchführungsbeschlusses gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (im Folgenden „Beschlussentwurf über die Angemessenheit des Datenschutzes bei der Strafverfolgung") vorgelegt hat, stellt der EDSA fest, dass die Nutzung der Einwilligung gemäß der Regelung des Vereinigten Königreichs im Bereich der Strafverfolgung stets einer Rechtsgrundlage bedürfen würde. Das bedeutet, dass die Polizei, selbst wenn sie über die gesetzlichen Befugnisse zur Verarbeitung der Daten für Ermittlungszwecke verfügt, unter bestimmten Umständen (z. B. bei der Entnahme einer DNA-Probe) die Einholung einer Einwilligung von der betroffenen Person für angebracht erachten kann.

121. **Der EDSA ersucht die Europäische Kommission, ihre Analyse über die im Beschlussentwurf über die Angemessenheit des Datenschutzes bei der Strafverfolgung vorgesehene mögliche Nutzung der Einwilligung im Bereich der Strafverfolgung, die in den Angemessenheitsbeschluss aufzunehmen.**

4.1.1.2 Durchsuchungs- und Herausgabeanordnungen

122. Der EDSA hat zwar keine Anmerkungen zur Beweisgewinnung durch die Polizei im Wege von Durchsuchungs- und Herausgabeanordnungen im Allgemeinen, doch geht aus Erwägungsgrund 136 des Beschlussentwurfs hervor, dass sich die Europäische Kommission bei ihren Überlegungen zum Zugriff auf personenbezogene Daten durch Strafverfolgungsbehörden auf die Polizei konzentriert hat und die Verarbeitung personenbezogener Daten durch andere Strafverfolgungsbehörden in geringerem Maße untersucht wurde.

[74] Siehe S. 37 des Beschlussentwurfs.

123. So wird beispielsweise auf S. 11 der Veröffentlichung des Vereinigten Königreichs *Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement*[75] die **National Crime Agency** (die nationale Kriminalbehörde, im Folgenden „NCA") als eine Strafverfolgungsbehörde von besonderem Interesse genannt, die u. a. umfassendere Funktionen im Bereich der Gewinnung von kriminalpolizeilichen Erkenntnissen ausübt. Die NCA beschreibt ihren Auftrag als Zusammenführung von Erkenntnissen aus verschiedenen Quellen, um die Analyse-, Bewertungs- und taktischen Möglichkeiten zu maximieren, unter anderem durch die technische Überwachung des Kommunikationsverkehrs, durch Strafverfolgungspartner im Vereinigten Königreich und im Ausland sowie durch Sicherheits- und Nachrichtendienste.[76] Die NCA ist auch eine der wichtigsten Anlaufstellen für die internationalen Partner im Bereich der Strafverfolgung und spielt eine Schlüsselrolle beim Austausch strafrechtlich relevanter Erkenntnisse[77].

124. Der EDSA nimmt ferner zur Kenntnis, dass die Government Communications Headquarters (die staatliche Kommunikationszentrale, im Folgenden „GCHQ"), deren Tätigkeiten typischerweise in den Anwendungsbereich von Teil 4 des DPA von 2018 (nationale Sicherheit) fallen, auch eine aktive Rolle bei der Eindämmung des gesellschaftlichen und finanziellen Schadens spielen, der dem Vereinigten Königreich durch schwere und organisierte Kriminalität entsteht, und dabei eng mit dem Innenministerium, der NCA, der Finanz- und Zollbehörde des Vereinigten Königreichs und anderen Regierungsstellen zusammenarbeiten.[78] Die Tätigkeiten der GCHQ betreffen die Bekämpfung des sexuellen Missbrauchs von Kindern, Betrugsdelikte, sonstige Formen der Wirtschaftskriminalität einschließlich Geldwäsche, die rechtswidrige Nutzung von Technologie, Cyberkriminalität, organisierte Kriminalität im Bereich der Einwanderung, einschließlich Menschenhandel, sowie Drogenschmuggel, Waffenschmuggel und andere Formen von Schmuggel.

125. **Der EDSA empfiehlt der Europäischen Kommission, ihre Analyse durch eine Analyse der im Bereich der Strafverfolgung tätigen Behörden zu ergänzen, die offenbar die Erhebung und Auswertung von**

---

[75] Siehe Regierung des Vereinigten Königreichs, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, 13. März 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Siehe Website der National Crime Agency, 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.

[77] Zwar sind nicht alle von der NCA verarbeiteten nachrichtendienstlichen Informationen personenbezogene Daten, doch da es sich womöglich bei einem erheblichen Teil um personenbezogene Daten handelt und die hier beschriebenen Tätigkeiten sich von denen der klassischen Polizeiarbeit unterscheiden, wäre eine Bewertung des Zugriffs auf personenbezogene Daten durch Strafverfolgungsbehörden im Vereinigten Königreich unvollständig, ohne die Tätigkeiten der NCA gründlich zu beurteilen. Es wäre sinnvoll, dafür zu sorgen, dass den Grundsätzen des Datenschutzes in allen einschlägigen Strafverfolgungsbehörden dieselbe Bedeutung beigemessen wird, und gerade über eine so datengesteuerte Behörde wie die NCA Aufschluss zu geben. Darüber hinaus heißt es unter der Überschrift „Ausblick" in der Erklärung weiter: „Wir suchen ständig nach neuen Möglichkeiten, traditionelle Fähigkeiten zu sammeln, auszubauen und zu verbessern, um die Quantität und Qualität der sowohl im Vereinigten Königreich als auch im Ausland auswertbaren nachrichtendienstlichen Erkenntnisse zu erhöhen." „Unter anderem entwickeln wir eine neue National Data Exploitation Capability, in der wir von den Befugnissen, die der Agentur durch den Crime and Courts Act übertragen wurden, Gebrauch machen, um Daten aus allen staatlichen Behörden miteinander zu verbinden, auf sie zuzugreifen und sie zu nutzen." [...] „Durch all diese Entwicklungen werden wir beweglicher und flexibler auf neue Bedrohungen reagieren und proaktiv dagegen vorgehen können, sodass wir in der Lage sein werden, Informationen und Erkenntnisse über neu entstehende Bedrohungen zu sammeln und auszuwerten, und schließlich Maßnahmen ergreifen können, bevor Bedrohungen realisiert werden."

[78] Siehe Website der GCHQ, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime.

Daten, einschließlich personenbezogener Daten, zu einem Schwerpunkt ihrer täglichen Arbeit gemacht haben, insbesondere der NCA. Darüber hinaus ersucht der EDSA die Europäische Kommission, Behörden wie die GCHQ, deren Tätigkeiten sowohl in den Bereich der Strafverfolgung als auch den der nationalen Sicherheit fallen, und den für diese Behörden geltenden Rechtsrahmen für die Verarbeitung personenbezogener Daten genauer zu untersuchen.

4.1.1.3 Ermittlungsbefugnisse für Strafverfolgungszwecke

126. In Kapitel 4 der Referenzgrundlage für Angemessenheit im Sinne der DSGVO(„Wesentliche Garantien in **Drittländern hinsichtlich der Rechtsdurchsetzung** und hinsichtlich des Zugangs nationaler Sicherheitsbehörden zur Begrenzung des Eingriffs in Grundrechte“) weist der EDSA darauf hin, dass „[i]n diesem Zusammenhang [...] das Gericht außerdem entscheidend darauf hingewiesen [hat], dass die frühere Safe-Harbor-Entscheidung ‚keine Feststellung dazu [enthielt], ob es in den Vereinigten Staaten staatliche Regeln gibt, die dazu dienen, etwaige **Eingriffe – zu denen die staatlichen Stellen dieses Landes in Verfolgung berechtigter Ziele** wie der nationalen Sicherheit **berechtigt wären** – in die Grundrechte der Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, zu begrenzen‘.“[79] In diesem Zusammenhang stellt der EDSA fest, dass **beim Zugriff auf Daten, sei es** für Zwecke der nationalen Sicherheit oder **für Strafverfolgungszwecke, die vier wesentlichen europäischen Garantien**[80] **von allen als angemessen beurteilten Drittländern eingehalten werden müssen**; insbesondere **müssen die Erforderlichkeit und die Verhältnismäßigkeit im Hinblick auf die verfolgten legitimen Ziele nachgewiesen werden**.

127. In diesem Abschnitt des Beschlussentwurfs kommt die Europäische Kommission zu folgendem Schluss (Erwägungsgrund 139): „Da die im IPA von 2016 vorgesehenen Ermittlungsbefugnisse dieselben sind wie die, die nationalen Sicherheitsbehörden zur Verfügung stehen, werden die für diese Befugnisse geltenden Bedingungen, Beschränkungen und Garantien ausführlich im Abschnitt über den Zugriff auf und die Nutzung von personenbezogenen Daten durch Behörden des Vereinigten Königreichs für Zwecke der nationalen Sicherheit behandelt.“ Aus der Rechtsprechung des EuGH geht jedoch hervor, dass bei der Anwendung der Erforderlichkeits- und Verhältnismäßigkeitsprüfung auf die Rechtsvorschriften der Mitgliedstaaten, die die Speicherung von und den Zugriff auf personenbezogene Daten durch Behörden ermöglichen, legitime Ziele wie die nationale Sicherheit oder die Bekämpfung schwerer Kriminalität der Art nach unterschiedlich sind und sie daher jeweils unterschiedliche Arten von Eingriffen rechtfertigen können bzw. würden.[81]

128. **Der EDSA würde es daher begrüßen, wenn im Rahmen des Beschlusses die Erforderlichkeit und die Verhältnismäßigkeit der Bedingungen, Beschränkungen und Garantien, die in den Erwägungsgründen 174 ff. (in denen es um Maßnahmen zur Verfolgung nationaler Sicherheitsziele geht) beschrieben werden, konkret im Hinblick auf deren Anwendung im Rahmen einer Maßnahme, mit der ein Strafverfolgungsziel verfolgt wird, geprüft würden. Er rät der Europäischen Kommission daher, näher zu klären, ob die Beschränkungen für die beschriebene Speicherung personenbezogener Daten und den Zugriff auf diese Daten für Strafverfolgungszwecke ausreichen, um ein Schutzniveau zu gewährleisten, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.**

[79] Siehe WP 254/rev.01, S. 9.

[80] Siehe EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen.

[81] Siehe Urteil des EuGH vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, ECLI:EU:C:2020:791.

4.1.2 Weiterverwendung der für Strafverfolgungszwecke erhobenen Daten (Erwägungsgründe 140-154)

129. Der EDSA stellt fest, dass der Datenschutzrahmen des Vereinigten Königreichs in Bezug auf die Weiterverwendung von für Strafverfolgungszwecke erhobenen Daten ähnliche Garantien und Beschränkungen vorsieht wie das EU-Recht.

4.1.2.1 Weiterverwendung für andere Strafverfolgungszwecke

130. Tatsächlich ist im DPA von 2018 vorgesehen, dass personenbezogene Daten, die von einer zuständigen Behörde für Strafverfolgungszwecke erhoben wurden, für einen beliebigen anderen Strafverfolgungszweck weiter verarbeitet werden können (entweder durch den ursprünglichen Verantwortlichen oder durch einen anderen Verantwortlichen), vorausgesetzt, der Verantwortliche ist von Rechts wegen befugt, Daten für diesen anderen Zweck zu verarbeiten, und die Verarbeitung ist für diesen Zweck erforderlich und verhältnismäßig. Die Europäische Kommission stellt fest, dass alle in Teil 3 des DPA von 2018 vorgesehenen Garantien für die von der empfangenden Behörde vorgenommene Verarbeitung gelten. Der EDSA weist jedoch darauf hin, dass gemäß Teil 3 Artikel 44 Absatz 4, Artikel 45 Absatz 4, Artikel 48 Absatz 3 und Artikel 68 Absatz 7 des DPA von 2018 die Möglichkeit vorgesehen ist, die Rechte betroffener Personen zu beschränken, und dass in Artikel 79 die Möglichkeit vorgesehen ist, Bescheinigungen auszustellen, wonach eine solche Einschränkung eine erforderliche und verhältnismäßige Maßnahme zum Schutz der nationalen Sicherheit darstellt. **Der EDSA empfiehlt der Europäischen Kommission daher, die möglichen Auswirkungen solcher Beschränkungen auf das Schutzniveau personenbezogener Daten eingehender zu bewerten, was die Weiterverwendung der erhobenen Daten angeht. In ähnlicher Weise sollten auch in Bezug auf den Rechtsrahmen des Vereinigten Königreichs, der eine solche Weitergabe ermöglicht, zusätzliche Erläuterungen vorgelegt werden, insbesondere zum Digital Economy Act von 2017 und zum Crime and Courts Act von 2013, der den Austausch von Daten mit der NCA ermöglicht.**

4.1.2.2 Weiterverwendung für andere Zwecke als die Strafverfolgung im Vereinigten Königreich

131. Im DPA von 2018 ist ferner vorgesehen, dass personenbezogene Daten, die für Strafverfolgungszwecke erhoben werden, auch zu einem Zweck verarbeitet werden dürfen, der nicht der Strafverfolgung dient, wenn die Verarbeitung gesetzlich zulässig ist. In diesem Fall ist die Rechtsgrundlage, die eine solche Weitergabe gestattet, Artikel 19 des Counter-Terrorism Act von 2008. In diesem Zusammenhang stellt der EDSA fest, dass auf den Anwendungsbereich und die Bestimmungen von Artikel 19 des Counter-Terrorism Act in der Bewertung der Europäischen Kommission nicht umfassend eingegangen wird und dass sie eine allgemeinere Weiterverwendung implizieren können, insbesondere mit Blick auf Artikel 19 Absatz 2, in dem es heißt, dass „[d]ie Daten, die von einem der Nachrichtendienste im Rahmen der Ausübung einer seiner Funktionen erlangt wurden, von diesem Dienst im Zusammenhang mit der Ausübung jedweder seiner anderen Funktionen genutzt werden [können]“.

132. Der EDSA stellt ferner fest, dass der Hinweis der Europäischen Kommission darauf, dass die zuständigen Behörden im Einklang mit der EMRK, einschließlich Artikel 8, handeln müssen, um sicherzustellen, dass der gesamte Datenaustausch zwischen den Strafverfolgungsbehörden und den Nachrichtendiensten im Einklang mit den Datenschutzvorschriften und mit der EMRK erfolgt, untermauert werden könnte, indem die einschlägigen Rechtsakte und Gesetze der Rechtsordnung des Vereinigten Königreichs angegeben werden, in denen diese Grenzen klar und präzise festgelegt sind.

4.1.2.3 Weiterverwendung im Zusammenhang mit Weiterübermittlungen außerhalb des Vereinigten Königreichs

133. Die Europäische Kommission hat zwar darauf hingewiesen, dass sich das CLOUD-Act-Abkommen möglicherweise auf Weiterübermittlungen in die USA durch Anbieter von Kommunikationsdiensten im Vereinigten Königreich auswirkt, doch verweist der EDSA darauf, dass sich das Inkrafttreten dieses Abkommens auch auf die Weiterverwendung von Daten auswirken kann, die von Strafverfolgungsbehörden im Vereinigten Königreich durch Weiterübermittlungen erhoben werden, insbesondere im Zusammenhang mit dem Erlass und der Übermittlung von Anordnungen gemäß Artikel 5 CLOUD-Act-Abkommen.

134. Generell ist der EDSA der Auffassung, dass der künftige Abschluss bilateraler Übereinkünfte mit Drittländern zwecks Zusammenarbeit im Bereich der Strafverfolgung, die eine Rechtsgrundlage für die Übermittlung personenbezogener Daten in diese Länder schaffen, sich auch erheblich auf die Bedingungen für die Weiterverwendung der erhobenen Daten auswirken könnte, da sich solche Übereinkünfte auf den bewerteten Datenschutzrahmen des Vereinigten Königreichs möglicherweise auswirken. Der EDSA empfiehlt der Europäischen Kommission daher, diesen Punkt eingehender zu bewerten, dabei bestehende internationale Übereinkünfte zu benennen und klarzustellen, ob die Bestimmungen dieser Übereinkünfte die Anwendung des Datenschutzrechts des Vereinigten Königreichs beeinträchtigen könnten, sowie eine weitere Beschränkung oder Ausnahmeregelung in Bezug auf die Weiterverwendung und die Offenlegung von Daten im Ausland, die für Strafverfolgungszwecke erhoben werden, vorzusehen. Der EDSA ist der Auffassung, dass solche Informationen und Bewertungen von zentraler Bedeutung sind, um eine umfassende Beurteilung des Schutzniveaus hinsichtlich des Rechtsrahmens und der Rechtspraxis des Vereinigten Königreichs in Bezug auf die Offenlegung von Daten im Ausland und die Weiterverwendung von Daten zu ermöglichen.

4.1.3 Aufsicht

135. Der EDSA stellt fest, dass die Aufsicht über die Strafverfolgungsbehörden durch verschiedene Kommissare ergänzend zum ICO sichergestellt wird. Im Entwurf der Angemessenheitsentscheidungen werden der IPC, der Kommissar für die Speicherung und Verwendung von biometrischem Material sowie der Kommissar für Überwachungskameras genannt. In diesem Zusammenhang ist darauf hinzuweisen, dass der EuGH wiederholt die Notwendigkeit einer unabhängigen Aufsicht hervorgehoben hat. Von zentraler Bedeutung für Fragen des Zugriffs auf personenbezogene Daten, die in das Vereinigte Königreich übermittelt werden, ist der IPC. Der EDSA geht davon aus, dass der IPC ein sogenannter Justizkommissar ist, wie andere Justizkommissare, auf die in dem Kapitel über nationale Sicherheit näher eingegangen wird, und dass diese Justizkommissare die Unabhängigkeit von Richtern genießen, auch dann, wenn sie eine Funktion als Kommissar ausüben. In Bezug auf das IPCO, das Büro des IPC, erläutert die Europäische Kommission in Erwägungsgrund 245 des Beschlussentwurfs, dass dieses als unabhängige Einrichtung fungiert, allerdings vom Innenministerium finanziert wird.

136. Der EDSA hat in dem Beschlussentwurf keine weiteren Hinweise auf eine Bewertung der Unabhängigkeit des Kommissars für die Speicherung und Verwendung von biometrischem Material sowie des Kommissars für Überwachungskameras gefunden.

137. **Die Europäische Kommission wird ersucht, die Unabhängigkeit der Justizkommissare eingehender zu bewerten, auch in Fällen, in denen ein Kommissar nicht (mehr) als Richter tätig ist, sowie die Unabhängigkeit des Kommissars für die Speicherung und Verwendung von biometrischem Material und des Kommissars für Überwachungskameras zu bewerten.**

4.2 Allgemeiner Rechtsrahmen für den Datenschutz im Bereich der nationalen Sicherheit

4.2.1 Nationale Sicherheitsbescheinigungen

138. Nach Artikel 111 des DPA von 2018 können Verantwortliche 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 Ausnahmen von den in den Teilen 4 bis 6 des DPA von 2018 verankerten Pflichten und Rechten eine erforderliche und verhältnismäßige Maßnahme zum Schutz der nationalen Sicherheit darstellen. Diese Bescheinigungen dienen dazu, die Rechtssicherheit für die Verantwortlichen zu erhöhen und nachzuweisen, dass die nationale Sicherheit bei der Verarbeitung personenbezogener Daten maßgeblich ist. Es muss jedoch erwähnt werden, dass die Bescheinigungen nicht erforderlich sind, um Ausnahmeregelungen für die nationale Sicherheit in Anspruch nehmen zu können, sondern dass es sich dabei um eine Transparenzmaßnahme handelt.[82]

139. Der EDSA entnimmt Anhang 20 Nummer 17 und 18 des DPA von 2018, dass eine nach dem Data Protection Act von 1998 ausgestellte nationale Sicherheitsbescheinigung (im Folgenden „alte Bescheinigung“) bis zum 25. Mai 2019 eine verlängerte Wirkung für die Verarbeitung personenbezogener Daten gemäß dem DPA von 2018 besaß. Bis zu diesem Datum wurden die alten Bescheinigungen, sofern sie nicht ersetzt oder widerrufen wurden, so behandelt, als ob sie nach dem DPA von 2018 ausgestellt worden wären.

140. Wenn es jedoch kein ausdrückliches Ablaufdatum für eine nach dem Data Protection Act von 1998 ausgestellte nationale Sicherheitsbescheinigung gibt, geht der EDSA davon aus, dass eine solche Bescheinigung in Bezug auf die Verarbeitung nach dem Data Protection Act von 1998 weiterhin wirksam ist, es sei denn, sie wird widerrufen oder aufgehoben.[83] Obwohl der durch diese alten Bescheinigungen gewährte Schutz auf die Verarbeitung personenbezogener Daten nach dem Data Protection Act von 1998 beschränkt ist, stellt der EDSA fest, dass für personenbezogene Daten, die gemäß dem Data Protection Act von 1998 verarbeitet wurden, neue nationale Sicherheitsbescheinigungen nach dem Data Protection Act von 1998 ausgestellt werden können.[84]

141. **Der Vollständigkeit halber empfiehlt der EDSA der Europäischen Kommission, in ihrem Beschlussentwurf darauf hinzuweisen, dass nach wie vor nationale Sicherheitsbescheinigungen nach dem Data Protection Act von 1998 ausgestellt werden können. Darüber hinaus ersucht der EDSA die Europäische Kommission, in ihrem Beschlussentwurf die Rechtsbehelfs- und Aufsichtsmechanismen in Bezug auf gemäß dem Data Protection Act von 1998 ausgestellte Bescheinigungen dieser Art zu beschreiben. Schließlich rät der EDSA der Europäischen Kommission, in ihrem Beschlussentwurf die Anzahl der vorhandenen, gemäß dem Data Protection Act von 1998 ausgestellten Bescheinigungen zu nennen und diesen Aspekt aufmerksam zu überwachen.**

[82] Siehe Home Office, The Data Protection Act 2018, National Security Certificates, August 2020, Nummer 4, S. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

[83] Siehe Home Office, The Data Protection Act 2018, National Security Certificates, August 2020, S. 5.

[84] Siehe Home Office, The Data Protection Act 2018, National Security Certificates, August 2020, Nummer 8, S. 5.

4.2.2 Recht auf Berichtigung und Löschung personenbezogener Daten

142. In Bezug auf das Recht auf Berichtigung und Löschung personenbezogener Daten nimmt der EDSA zur Kenntnis, dass betroffene Personen gemäß Artikel 100 und Artikel 149 des DPA von 2018 die Möglichkeit haben, sich an den High Court (in Schottland an den Court of Session) zu wenden, um von einem Verantwortlichen die unverzügliche Berichtigung oder Löschung ihrer Daten zu verlangen.

143. **Der EDSA betont, dass die Ausübung der Rechte betroffener Personen wirksam sichergestellt werden muss, und rät der Europäischen Kommission daher, in ihrem Beschlussentwurf zu beschreiben, wie Artikel 100 des DPA von 2018 in der Praxis umgesetzt wird, und die Anwendung dieses Artikels genau zu überwachen.**

4.2.3 Ausnahmeregelungen für die nationale Sicherheit

144. Der EDSA weist auf Artikel 110 des DPA von 2018 und insbesondere auf dessen Anhang 11 hin, in dem die spezifischen Zwecke festgelegt sind, zu denen Nachrichtendienste von bestimmten Datenschutzgrundsätzen abweichen können, auch in Bezug auf die Betroffenenrechte, und nicht verpflichtet sind, dem ICO Verletzungen des Schutzes personenbezogener Daten zu melden.[85]

145. **Der EDSA empfiehlt der Europäischen Kommission, den Anwendungsbereich der Ausnahmen weiter zu präzisieren, da sich die Frage stellt, ob tatsächlich alle in Anhang 11 des DPA von 2018 vorgesehenen Ausnahmen für die Arbeit von Nachrichtendiensten relevant sind und ob bei allen die Gleichwertigkeit mit dem Grundsatz der Erforderlichkeit und Verhältnismäßigkeit sichergestellt ist.** Insbesondere **empfiehlt der EDSA der Europäischen Kommission, genauer zu erläutern, unter welchen Umständen sich ein Nachrichtendienst auf Anhang 11 Nummer 10 des DPA von 2018 berufen könnte („Die aufgeführten Bestimmungen gelten nicht für personenbezogene Daten, die aus Aufzeichnungen über die Absichten des Verantwortlichen in Bezug auf etwaige Verhandlungen mit der betroffenen Person bestehen, sofern die Anwendung der aufgeführten Bestimmungen die Verhandlungen voraussichtlich beeinträchtigen würde“).**

4.3 Zugriff auf und Verwendung von personenbezogenen Daten durch Behörden des Vereinigten Königreichs für Zwecke der nationalen Sicherheit

146. Der EDSA erkennt grundsätzlich an, dass in Fragen der nationalen Sicherheit Staaten ein breiter Ermessensspielraum eingeräumt wird; dies wird auch vom EGMR zugestanden. Der EDSA erinnert ferner daran, dass, wie er in seinen aktualisierten Empfehlungen zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen[86] hervorgehoben hat, in Artikel 6 Absatz 3 des Vertrags über die Europäische Union niedergelegt ist, dass die Grundrechte, wie sie in der EMRK gewährleistet sind, als allgemeine Grundsätze Teil des Unionsrechts sind. Wie der EuGH in seiner Rechtsprechung allerdings festhält, stellt die EMRK, solange die EU ihr nicht beigetreten ist, kein Rechtsinstrument dar, das formell in die Unionsrechtsordnung übernommen wurde.[87] Daher muss das in Artikel 45 DSGVO geforderte Schutzniveau der Grundrechte auf der Grundlage der

[85] Diese Zwecke sind die Prävention und Aufdeckung von „Kriminalität“, „Informationen, die per Gesetz usw. oder im Zusammenhang mit Gerichtsverfahren offengelegt werden müssen“, „Parlamentarische Immunität“, „Gerichtsverfahren“, „Ehre und Würde der Krone“, „Streitkräfte“, „Wirtschaftliches Wohlergehen“, „Vertraulichkeit der anwaltlichen Korrespondenz“, „Verhandlungen“, „Vertrauliche Hinweise des Verantwortlichen“, „Prüfungsschriften und Noten“, „Forschung und Statistik“ und „Archivierung im öffentlichen Interesse“.

[86] Siehe EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen.

[87] Siehe Schrems II, Rn. 98.

Bestimmungen dieser Verordnung festgelegt werden, und zwar im Lichte der in der EU-Charta verankerten Grundrechte. Unbeschadet dessen haben nach Artikel 52 Absatz 3 EU-Charta die darin niedergelegten Rechte, die den durch die EMRK garantierten Rechten entsprechen, die gleiche Bedeutung und Tragweite, die ihnen in der EMRK verliehen werden. Daher ist, wie der EuGH festgehalten hat, die Rechtsprechung des EGMR bezüglich Rechten, die auch in der EU-Charta verankert sind, bei der Auslegung der entsprechenden Rechte in der EU-Charta als Mindestschutzstandard zu berücksichtigen.[88] Der letzte Satz in Artikel 52 Absatz 3 EU-Charta lautet allerdings: „Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt."

147. Daher hat der EDSA bei der folgenden Bewertung die Rechtsprechung des EGMR insofern berücksichtigt, als die EU-Charta in der Auslegung durch den EuGH kein höheres Schutzniveau vorsieht, das andere Anforderungen als die Rechtsprechung des EGMR vorschreibt.

4.3.1 Rechtsgrundlagen, Beschränkungen und Garantien – im Zusammenhang mit der nationalen Sicherheit ausgeübte Ermittlungsbefugnisse

4.3.1.1 Allgemeine Bemerkungen

148. Der EDSA erinnert daran, dass es sich beim IPA von 2016 um ein neues Gesetz handelt, mit dem mehrere Bestimmungen des Intelligence Services Act von 1994 geändert wurden. Im IPA von 2016 wird festgelegt, inwieweit bestimmte Ermittlungsbefugnisse für Eingriffe in die Privatsphäre genutzt werden können.[89] Auch wenn zwei Berichte des IPC vorliegen, die nützliche Informationen zur Anwendung dieses neuen Rechtsrahmens enthalten, wurden bestimmte Aspekte immer noch nicht überprüft, insbesondere zu den verwendeten Selektoren und Suchkriterien.

149. Darüber hinaus weist der EDSA allgemein zum IPA von 2016 und dessen Anwendungsbereich auf folgende vier Punkte hin, die besondere Aufmerksamkeit verdienen:

150. Zum **ersten Punkt**, der sich auf die Merkmale des Gesetzes bezieht, möchte der EDSA zwei Aspekte hervorheben:

151. Erstens stellt der EDSA fest, dass sich die Rechtsvorschriften auf weit gefasste Zwecke für die Anwendung von im IPA von 2016 vorgesehenen Verfahren beziehen und nicht auf die Kategorien von Personen, die von einer Datenerhebung auf der Grundlage der Teile 2 bis 7 des IPA von 2016 betroffen sein könnten. In diesem Zusammenhang erinnert der EDSA daran, dass zur Festlegung des persönlichen Anwendungsbereichs des Gesetzes zwischen den Kategorien von Personen, die Gegenstand von Überwachungsmaßnahmen sein können, und den mit den Rechtsvorschriften verfolgten Zwecken ein Zusammenhang bestehen sollte.

152. Darüber hinaus betont der EDSA, dass die Definitionen der Begriffe „Telekommunikationsanbieter", „Telekommunikationsdienst" und „Telekommunikationssystem", mit denen der Anwendungsbereich des Gesetzes festgelegt wird, ebenfalls sehr weit gefasst und teilweise unklar sind. Der EDSA weist darauf hin, dass diese Begriffe im Bereich des IPA von 2016 viel allgemeiner zu verstehen sind als in den Telekommunikationsvorschriften, wie sie beispielsweise im europäischen

[88] Siehe Urteil des EuGH vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, ECLI:EU:C:2020: 791, Rn. 124.
[89] Siehe Artikel 1 des IPA von 2016.

Kodex für die elektronische Kommunikation definiert sind.[90] Der EDSA stellt fest, dass die Definitionen der Begriffe „Telekommunikationsdienst“ und „Telekommunikationssystem“ im Gesetz bewusst weit gefasst sind, damit sie auch für neue Technologien gültig bleiben. Ebenso ist die Definition des Begriffs „Telekommunikationsanbieter“ sehr weit gefasst und könnte beispielsweise Online-Videospiele mit einer Chat-Funktion oder andere Online-Websites, die lediglich entsprechende Chat-Fenster enthalten, umfassen.[91]

153. Darüber hinaus sind zwar Verfahren und Aufsicht in Bezug auf die Beurteilung der Erforderlichkeit und Verhältnismäßigkeit der Erhebung von und des Zugriffs auf Daten in der Regel vorgesehen, doch die Kriterien für das Vorgehen bei einer solchen Beurteilung sind im Gesetz selbst nicht festgelegt. Zusätzliche Informationen finden sich in anderen Dokumenten wie z. B. Verhaltenskodizes.

154. Wie in den Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen angemerkt wird, hat der EuGH jedoch darauf hingewiesen, „dass das Erfordernis einer gesetzlichen Grundlage für jede Einschränkung der Ausübung der Grundrechte bedeutet, dass die gesetzliche Grundlage für den Eingriff in die Grundrechte den Umfang der Einschränkung der Ausübung des betreffenden Rechts selbst festlegen muss“[92]. Konkret hat der EuGH klargestellt: „Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt.“[93]

155. Auch der EGMR hat dargelegt, dass das Recht hinreichend klar formuliert sein muss, um den Bürgern „angemessene Hinweise darauf zu geben, unter welchen Umständen und Voraussetzungen die Behörden ermächtigt sind, auf solche Maßnahmen zurückzugreifen“.[94]

156. **Der EDSA rät der Europäischen Kommission daher, diese Aspekte betreffend die Genauigkeit, Klarheit und Vollständigkeit der einschlägigen Rechtsvorschriften eingehender zu bewerten und zusätzliche Elemente zu benennen, mit denen nachgewiesen werden kann, dass diese Rechtsvorschriften ein Schutzniveau bieten, das in Bezug auf die Merkmale der Rechtsvorschriften dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist. Der EDSA betont ferner,**

[90] Siehe Artikel 2 Absatz 5 des europäischen Kodex für die elektronische Kommunikation, in dem beispielsweise der Begriff „interpersoneller Kommunikationsdienst“ wie folgt definiert wird: „gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über elektronische Kommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen“.

[91] Siehe Home Office, Interception of communications, Code of practice, März 2018, Nummer 2.5 ff., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Siehe Schrems II, Rn. 175, und die zitierte Rechtsprechung sowie das Urteil des EuGHvom 6. Oktober 2020, Privacy International/Secretary of State for Foreign and Commonwealth Affairs u. a., C-623/17, ECLI:EU:C:2020:790 (im Folgenden „Privacy International“), Rn. 65.

[93] Siehe Privacy International, Rn. 68.

[94] Siehe Urteil des EGMR vom 4. Dezember 2015, Zakharov/Russland, CE:ECHR:2015:1204JUD004714306, Rn. 229.

dass weit gefasste Definitionen auch im Hinblick auf die Verhältnismäßigkeit der Überwachungsmaßnahmen bewertet werden sollten.

157. Auch wenn aus verschiedenen internen Kodizes der zuständigen Behörden der Intelligence Community (Gemeinschaft der Nachrichtendienste) zum Teil einige dieser Elemente hervorgehen, beispielsweise in Bezug auf die Bewertung der Erforderlichkeit und Verhältnismäßigkeit der Datenerhebung, betont der EDSA darüber hinaus, dass die Anforderungen des EuGH an der Rechtsgrundlage implizieren, dass die Kernelemente, einschließlich der Möglichkeit für Einzelne im Falle der Inanspruchnahme von Rechtsschutz sich hierauf berufen zu können, in Rechtsvorschriften enthalten sein müssen, die einklagbare Rechte vorsehen.[95] In Anhang 7 Nummer 6 des IPA von 2016 heißt es nämlich, dass Gerichte (und Aufsichtsbehörden) „bei der Entscheidung über eine Frage in einem solchen Verfahren berücksichtigen, dass eine Person möglicherweise einen Kodex nicht befolgt hat", ohne jedoch darauf einzugehen, ob der Einzelne vor Gerichten (oder Aufsichtsbehörden) einen Verstoß gegen die Kodizes geltend machen kann. Darüber hinaus beziehen sich die bisher im Beschlussentwurf enthaltenen Elemente entweder auf die Anerkennung der Vorhersehbarkeit der in diesen Kodizes enthaltenen Vorschriften durch den EGMR[96] anstatt, wie vom EuGH gefordert, auf deren Einklagbarkeit vor Gericht, oder darauf, dass britische Gerichte sich in bestimmten Rechtssachen auf Kodizes berufen haben, während in keiner der erwähnten Rechtssachen die Möglichkeit für Einzelne erwähnt wird, aus den Kodizes abgeleitete Rechte geltend machen zu können. **Sollte sich herausstellen, dass das Recht des Vereinigten Königreichs die Umstände und Bedingungen, unter denen eine Maßnahme erlassen werden kann, nicht in ausreichendem Umfang vorsieht, und dass diese Elemente durch interne Kodizes der Behörden der Intelligence Community tatsächlich vorgegeben werden, würde der EDSA die Europäische Kommission auffordern, eingehender zu bewerten, ob die in den verschiedenen internen Kodizes der Behörden der Intelligence Community vorgesehenen Beschränkungen und Garantien von Einzelnen vor Gericht eingeklagt und durchgesetzt werden können.**

158. **Der zweite Punkt** betrifft die Tatsache, dass die Bestimmungen bezüglich der gezielten Beschaffung und Speicherung von Kommunikationsdaten einerseits und der Sammelerhebung andererseits sowohl im IPA von 2016 als auch in anderen Rechtsvorschriften wie dem Intelligence Services Act von 1994 oder dem Regulation of Investigatory Powers Act von 2000 auch für aus der EU in das Vereinigte Königreich übermittelte Daten gelten werden. In Bezug auf Sammelerhebungen hebt der EDSA hervor, dass die einschlägigen Bestimmungen des britischen Rechts die Erhebung von Daten außerhalb des Vereinigten Königreichs ermöglichen, was auch Daten während der Übermittlung zwischen dem EWR und dem Vereinigten Königreich auf der Grundlage des Angemessenheitsbeschlusses betreffen könnte.[97] Darüber hinaus stellt der EDSA fest, dass die Europäische Kommission darauf hinweist, „dass das Speichern und Sammeln von Kommunikationsdaten normalerweise keine personenbezogenen Daten betroffener Personen in der

[95] In diesem Zusammenhang vertrat der EuGH beispielsweise die Auffassung, dass die PPD-28 in den USA kein der Sache nach gleichwertiges Schutzniveau bietet, trotz einiger darin vorgesehener Beschränkungen in Bezug auf die Sammelerhebung personenbezogener Daten (siehe Schrems II, Rn. 181).

[96] Siehe Urteil des EGMR vom 13. September 2018, Big Brother Watch u. a./Vereinigtes Königreich, ECLI:CE:ECHR:2018:0913JUD005817013 (im Folgenden „Big Brother Watch"), Rn. 325: „Da es sich bei dem IC-Kodex um ein öffentliches Dokument handelt, das von beiden Kammern des Parlaments gebilligt werden muss und sowohl von den Personen, die Überwachungsaufgaben wahrnehmen, als auch von den Gerichten zu berücksichtigen ist, hat der Gerichtshof ausdrücklich anerkannt, dass seine Bestimmungen bei der Beurteilung der Vorhersehbarkeit des RIPA-Systems berücksichtigt werden können."

[97] Siehe Schrems II, Rn. 183 ff., zur Beurteilung einer Rechtsvorschrift, die den Zugriff auf Daten während ihrer Übermittlung im Rahmen eines Angemessenheitsbeschlusses zwischen der EU und einem Drittland vorsieht.

EU betrifft, die auf Grundlage dieses Beschlusses in das Vereinigte Königreich übermittelt werden. Die Verpflichtung zur Speicherung oder Offenlegung von Kommunikationsdaten gemäß den Teilen 3 und 4 des IPA von 2016 betrifft Daten, die von Telekommunikationsanbietern im Vereinigten Königreich unmittelbar von den Nutzern eines Telekommunikationsdienstes erhoben werden."[98] Der EDSA weist jedoch auf die Unklarheit hin, dass nur Niederlassungen dieser Anbieter im Vereinigten Königreich Anordnungen der zuständigen britischen Behörden erhalten können, da nach der Definition des Begriffs „Telekommunikationsanbieter" in Artikel 261 Absatz 10 des IPA von 2016 „ein Telekommunikationsanbieter eine Person ist, die einen Telekommunikationsdienst für Personen im Vereinigten Königreich anbietet oder bereitstellt oder die ein Telekommunikationssystem kontrolliert oder bereitstellt, das sich (ganz oder teilweise) im Vereinigten Königreich befindet oder vom Vereinigten Königreich aus kontrolliert wird". Folglich könnten personenbezogene Daten betroffener Personen im EWR doch betroffen sein, beispielsweise wenn Daten, die von einer Niederlassung eines britischen Telekommunikationsanbieters mit Sitz im EWR erhoben oder generiert wurden, auf der Grundlage des Angemessenheitsbeschlusses an eine Niederlassung desselben Betreibers im Vereinigten Königreich übermittelt werden (zu gewerblichen Zwecken) und anschließend im Vereinigten Königreich von den zuständigen Behörden erhoben werden.

159. **Der EDSA ist daher der Auffassung, dass die Beurteilung dieser Bestimmungen auch für die Beurteilung des Angemessenheitsniveaus des britischen Rechtsrahmens maßgeblich ist, und er fordert die Europäischen Kommission dazu auf, diesen Aspekt zu klären und noch eingehender zu bewerten, inwieweit dies zutrifft. Insbesondere ersucht der EDSA die Europäische Kommission, ihr Verständnis des Anwendungsbereichs dieser Rechtsvorschriften zu erläutern und dabei auch auf die Frage einzugehen, was unter den Begriff „Nutzer von Telekommunikationsdiensten" fällt, und ob mit Rücksicht auf die weit gefasste Definition von „Telekommunikationsanbieter" Daten von Niederlassungen von Telekommunikationsanbietern außerhalb des Vereinigten Königreichs angefordert werden könnten, wenn Daten betroffener Personen im EWR betroffen sind.**

160. **Der dritte Punkt** betrifft das Double-Lock-Verfahren. Der EDSA stellt fest, dass im IPA von 2016 ein neues Double-Lock-Verfahren eingeführt wurde. Dennoch geht der EDSA davon aus, dass selbst wenn die Erhebung von oder der Zugriff auf Daten für Zwecke der nationalen Sicherheit oder für nachrichtendienstliche Zwecke grundsätzlich nur mit einer von einem Justizkommissar erlassenen Anordnung erfolgen kann, der IPA von 2016 vorsieht, dass „in bestimmten begrenzten Fällen ein rechtmäßiges Abfangen ohne Anordnung möglich ist und nur eine vorherige Genehmigung durch die zuständigen Behörden für das Abfangen von Kommunikationsdaten erforderlich ist [siehe Abschnitt zur Aufsicht], auch für das Abfangen von Daten auf der Grundlage von Anfragen aus dem Ausland (Artikel 52 des IPA von 2016)". Wie im Folgenden dargelegt wird, trägt dies auch zu den Bedenken bei, die der EDSA insbesondere in Bezug auf die Offenlegung von Daten im Ausland hegt. Darüber hinaus stellt der EDSA fest, dass für Eingriffe in Geräte, ob gezielt oder massenhaft, ebenfalls eine Ausnahme vom Double-Lock-Verfahren möglich ist, und dass der Justizkommissar nach einem ersten Zeitraum von maximal sechs Monaten berechtigt ist, lediglich die Verlängerung von Massenüberwachungsanordnungen zu genehmigen. **Der EDSA ersucht die Europäische Kommission, eingehender zu bewerten und nachzuweisen, dass der Rechtsrahmen des Vereinigten Königreichs selbst in Fällen, in denen das Double-Lock-Verfahren nicht zur Anwendung kommt, geeignete Garantien bietet, unter anderem durch wirksame Ex-post-Aufsicht und Rechtsbehelfsmöglichkeiten für den Einzelnen, um ein Schutzniveau zu gewährleisten, das dem in**

[98] Siehe Erwägungsgrund 196 des Beschlussentwurfs.

der EU gebotenen Schutzniveau der Sache nach gleichwertig ist (siehe auch Abschnitt 4.3.3 zur Aufsicht).

161. Auch wenn mit dem IPA von 2016 das Double-Lock-Verfahren eingeführt wurde, ist der EDSA nach wie vor besorgt über bestimmte Aspekte der neuen Rechtsvorschriften. Nach der Präsentation der entsprechenden Abschnitte des Beschlussentwurfs hat der EDSA die folgenden Arten der Erhebung von und des Zugriffs auf Daten in der von der Europäischen Kommission vorgelegten Reihenfolge analysiert. Die Reihenfolge der nachfolgend bewerteten Elemente stellt daher keine Rangfolge in Bezug auf den Grad der Besorgnis des EDSA dar.

4.3.1.2 Gezielte Sammlung und Speicherung von Kommunikationsdaten

162. Der EDSA stellt fest, dass es zwei Beamte gibt, die gezielte Genehmigungen für die Erhebung von Kommunikationsdaten erteilen können: der Anweisungsbefugte im Amt für die Genehmigung von Kommunikationsdaten (im Folgenden „der IPC"), ein dafür ernannter hochrangiger Beamter (eine Person, die ein bestimmtes Amt oder einen bestimmten Rang in einer einschlägigen Behörde innehat), ergänzend zu der Genehmigung durch einen Justizkommissar in bestimmten Fällen. Für den EDSA ist jedoch im Hinblick auf das Gesetz und den maßgeblichen Kodex unklar, welcher Beamte genau welche Art von gezielter Sammlung von Kommunikationsdaten genehmigt und inwieweit ein speziell ernannter Beamter hinreichend unabhängig wäre.[99]

163. **Der EDSA möchte die Europäische Kommission daher bitten, diesen Aspekt eingehender zu bewerten und diese Elemente klarer zu erläutern.**

164. Was Speicherungsanordnungen für Kommunikationsdaten angeht, stellt der EDSA außerdem fest, dass solche Anordnungen an eine „Beschreibung von Anbietern" gerichtet werden können. Mit diesem Begriff ist wahrscheinlich gemeint, dass mehrere Anbieter gleichzeitig aufgefordert werden können, Daten zu speichern. Die Gezieltheit der Datenerhebung bezieht sich also nicht auf die Anzahl der Anbieter, sondern auf den Namen oder die Beschreibung der Personen, der Organisationen, des Standorts oder der Personengruppe, die das „Ziel" darstellen, eine Beschreibung der Art der Untersuchung und eine Beschreibung der Tätigkeiten, für die die Geräte verwendet werden. Der EDSA weist daher darauf hin, dass je nach Anzahl der Anbieter, die zu einer solchen „Beschreibung von Anbietern" gehören, die Speicherungsanordnung möglicherweise weiter gefasst sein kann, als das Verfahren einer gezielten Speicherung vermuten ließe. **Der EDSA rät der Europäischen Kommission, diesen Aspekt eingehender zu bewerten und weitere Zusicherungen dafür zu geben, dass Speicherungsanordnungen auch dann, wenn sie an mehrere Anbieter gerichtet sind, auf das absolut Notwendige beschränkt und verhältnismäßig bleiben.**

4.3.1.3 Eingriff in Geräte

165. Der EDSA stellt fest, dass in dringenden Fällen für Eingriffe in Geräte eine Ausnahme vom Double-Lock-Verfahren möglich ist.[100] Der EDSA ist besorgt darüber, dass die Zwecke, die solche Geräteeingriffe rechtfertigen können, weit gefasst sind, und dass die Kriterien für das Vorliegen von Dringlichkeit (bei der der Justizkommissar nicht um eine Ex-ante-Genehmigung nach vorgehender Beurteilung der Erforderlichkeit und Verhältnismäßigkeit der Geräteeingriffe ersucht werden muss) im Unklaren bleiben. Da in einer solchen Situation, falls der Justizkommissar die Geräteeingriffe nicht nachträglich genehmigt, „die Wirkung der Anordnung endet und nicht verlängert werden kann", geht

[99] Siehe auch nachfolgende Ausführungen zur Bewertung des Double-Lock-Verfahrens und der Unabhängigkeit des Justizkommissars.
[100] Siehe Artikel 109 des IPA von 2016.

der EDSA davon aus, dass die in der Zwischenzeit erhobenen Daten weiterhin als rechtmäßig erhoben gelten. Für die Löschung dieser Daten kann eine besondere Anordnung des Justizkommissars ergehen.[101]

166. **Der EDSA ersucht die Europäische Kommission, eingehender zu bewerten, unter welchen Bedingungen Dringlichkeit geltend gemacht werden kann, und Erläuterungen zu den möglichen Wegen für die Ausübung der Rechte der betroffenen Personen und zu den Rechtsbehelfsmöglichkeiten vorzulegen, die diesen im Zusammenhang mit Eingriffen in Geräte offenstehen, insbesondere wenn diese im Kontext einer Dringlichkeit erfolgen, die zu einer Ausnahme vom Double-Lock-Verfahren führt.**

4.3.1.4 Abfangen von Massendaten über Träger

167. Wie in dem Bericht zur Überprüfung von Massenüberwachungsbefugnissen[102] erläutert, „werden beim Abfangen von Massendaten Kommunikationsdaten in der Regel erhoben, wenn sie bei ihrer Übermittlung bestimmte Träger (Kommunikationsverbindungen) passieren". Im entsprechenden offiziellen Factsheet zum IPA von 2016 wird das Abfangen von Massendaten beschrieben als „das Verfahren der Erhebung einer Menge von Kommunikationsdaten und der anschließenden Auswahl bestimmter Kommunikationsdaten, die gelesen, angesehen oder abgehört werden sollen, wenn dies erforderlich und verhältnismäßig ist". Der EDSA stellt fest, dass der Begriff „Abfangen von Massendaten" impliziert, dass Daten erhoben werden, ohne dass zuvor irgendeine Filterung durch Selektoren (entweder einfache – im Kontext der Überwachung von Personen, von denen bereits bekannt ist, dass sie eine Bedrohung darstellen – oder komplexe – im Kontext der Ermittlung neuer Bedrohungen und bisher unbekannter Personen von besonderem Interesse) stattgefunden hat.

168. Das Sammeln von Massenkommunikationsdaten gehörte auch zu den vom EuGH in der Rechtssache Privacy International untersuchten Fragen, die am 6. Oktober 2020 zu einem Urteil der Großen Kammer führten (zusätzlich zu der Frage, ob eine solche Datenerhebung im Rahmen des Unionsrechts durchgeführt wurde, auch für Zwecke der nationalen Sicherheit). Der IPA von 2016 ist an die Stelle der Rechtsvorschriften getreten, die Gegenstand dieses Urteils waren.

169. Der EDSA stellt fest, dass mit der Einführung des IPA von 2016 in das britische Recht nun auch eine Anordnung erforderlich ist, um Massendaten abzufangen. Das Verfahren zum Erlass dieser Anordnung stützt sich auf die Festlegung „operativer Zwecke". Die Liste dieser operativen Zwecke wird von den Leitern der Nachrichtendienste erstellt und anschließend vom Secretary of State genehmigt. Diese Entscheidung wiederum wird von einem unabhängigen Justizkommissar gebilligt, der prüfen muss, ob die Anordnung im Hinblick auf die operativen Zwecke erforderlich und verhältnismäßig ist. Der EDSA geht davon aus, dass der Justizkommissar nicht befugt ist, die operativen Zwecke als solche zu beurteilen, sondern nur, ob die Anordnung im Hinblick auf die in der Anordnung aufgeführten operativen Zwecke erforderlich und verhältnismäßig ist. Alle drei Monate wird dem Parliamentary Intelligence and Security Committee (Parlamentarischer Ausschuss für Nachrichtendienste und Sicherheit) eine Kopie der Liste zugeleitet, und der Premierminister überprüft die Liste dieser operativen Zwecke mindestens einmal jährlich.

170. Ausgehend von den im Beschlussentwurf durch die Europäische Kommission dargelegten Elementen ist es allerdings schwierig, die Größenordnung der in der Liste aufgeführten operativen Zwecke einzuschätzen und zu beurteilen, ob die dadurch zulässige Datenerhebung dem vom EuGH

[101] Siehe Artikel 110 Absatz 3 Buchstabe b des IPA von 2016.

[102] Siehe Bericht des Independent Reviewer of Terrorism Legislation zur Überprüfung von Massenüberwachungsbefugnissen, August 2016.

festgelegten Mindeststandard entspricht (beispielsweise könnte eine Begrenzung der Datenerhebung auf ein geografisches Gebiet bedeuten, dass Daten aus nur einigen wenigen Straßen oder auch Daten aus dem gesamten EWR erhoben werden dürfen).

171. Darüber hinaus betont der EDSA, dass Daten, die massenhaft erhoben wurden, für lange Zeiträume gespeichert werden können (damit sie für weitere Zugriffe für Prüfzwecke zur Verfügung stehen). Der EDSA stellt fest, dass in Artikel 150 Absätze 5 und 6 des IPA von 2016 nur die Vernichtung der Kopien der erhobenen Daten vorgesehen ist, und dies auch nur dann, wenn ihre Speicherung nicht im Interesse der nationalen Sicherheit oder aus anderen Gründen, die in den Anwendungsbereich von Artikel 138 Absatz 2 des IPA von 2016 fallen, erforderlich oder wahrscheinlich erforderlich ist, oder wenn die Speicherung nicht für mehrere andere Zwecke erforderlich ist.[103] Der EDSA betont, dass diese Gründe sehr weit gefasst sind und in jedem Fall nur von Kopien der abgerufenen Daten die Rede ist.

172. Darüber hinaus stellt der EDSA fest, dass der IPA von 2016 in dringenden Fällen auch eine Änderung von Anordnungen ohne vorherige Genehmigung durch einen Justizkommissar zulässt, und dass in einem solchen Fall, wenn der innerhalb von drei Arbeitstagen nach der Änderung nachträglich konsultierte Justizkommissar die Genehmigung der Änderung verweigert, die Wirksamkeit der Anordnung weiterbesteht, als ob keine Änderung vorgenommen worden wäre, die in der Zwischenzeit erhobenen Daten jedoch weiterhin als rechtmäßig erhoben gelten.[104] Für die Löschung dieser Daten kann eine besondere Anordnung des Justizkommissars ergehen.[105]

173. **Der EDSA fordert daher die Europäische Kommission auf, weitere Präzisierungen und eine Bewertung des Abfangens von Massendaten vorzunehmen, insbesondere bezüglich der Auswahl und Anwendung von Selektoren im Rahmen der Verfahren zum Abfangen von Massendaten, um zu klären, inwieweit beim Zugriff auf personenbezogene Daten der vom EuGH festgelegte Mindeststandard eingehalten wird (siehe auch Abschnitt 4.3.1.7, insbesondere zur Aufsicht über die Selektoren) und welche Garantien vorhanden sind, um die Grundrechte von natürlichen Personen zu schützen, deren Daten in diesem Zusammenhang abgefangen werden, auch in Bezug auf die Speicherfristen der Daten. Besonders nützlich wäre eine unabhängige Bewertung durch die zuständigen Aufsichtsbehörden des Vereinigten Königreichs.**

174. **Der EDSA betont ferner, dass er es für besonders bedenklich hält, dass „mit dem Ausland in Zusammenhang stehende Kommunikationsdaten" in den Anwendungsbereich von Praktiken des Abfangens von Massendaten fallen, und dies offenbar bedeutet, dass Daten vom Vereinigten Königreich unmittelbar im EWR abgefangen und massenhaft erhoben werden könnten, darunter auch Daten während der Übermittlung zwischen dem EWR und dem Vereinigten Königreich, die in den Anwendungsbereich des Beschlussentwurfs fallen würden (siehe Abschnitt 4.3.2 über die Weiterverwendung der gesammelten Daten für Zwecke der nationalen Sicherheit und Offenlegung von Daten im Ausland).**

4.3.1.5 Schutz und Garantien für Sekundärdaten

175. Darüber hinaus ist der EDSA besorgt darüber, dass die einschlägigen Rechtsvorschriften des Vereinigten Königreichs in Bezug auf das Abfangen von Massendaten nicht für alle Kommunikationsdaten das gleiche Schutzniveau vorsehen. „Sekundärdaten", die aufgrund einer Massenüberwachungsanordnung abgerufen werden können, sind nach Artikel 137 des IPA von 2016

[103] Siehe Artikel 150 Absätze3 und 6 des IPA von 2016.
[104] Siehe Artikel 147 des IPA von 2016 (Teil 6 Kapitel I).
[105] Siehe Artikel 181 Absatz 3 Buchstabe b des IPA von 2016.

sowohl „Systemdaten“, „die in der Kommunikation enthalten, als Bestandteil davon enthalten, an sie angehängt oder logisch mit ihr verbunden sind (sei es durch den Absender oder auf andere Weise)“, als auch „Identifizierungsdaten“, „die in der Kommunikation enthalten, als Bestandteil davon enthalten, an sie angehängt oder logisch mit ihr verbunden sind (sei es durch den Absender oder auf andere Weise), die logisch vom Rest der Kommunikation abgetrennt werden können, und die, wenn sie auf diese Weise abgetrennt würden, nichts von dem preisgeben würden, was vernünftigerweise als die Bedeutung (falls vorhanden) der Kommunikation angesehen werden könnte, ungeachtet jeglicher Bedeutung, die sich aus dem Umstand der Kommunikation an sich oder aus Daten im Zusammenhang mit der Übermittlung der Kommunikation ergibt“.[106]

176. Der EDSA stellt fest, dass für diese „Sekundärdaten“, die auch als „Metadaten“[107] bezeichnet und massenhaft erhoben werden, offenbar nicht die gleichen Garantien gelten wie für Daten, die aufgrund einer gezielten Anordnung erhoben werden, aber auch nicht die gleichen Garantien wie für massenhaft erhobene Inhaltsdaten. Der EDSA stellt fest, dass für eine Auswahl abgefangener Inhalte mehr Garantien vorgesehen sind[108] als für eine Auswahl abgefangener Sekundärdaten[109].

177. Darüber hinaus betont der EDSA, dass sowohl der EGMR[110] als auch der EuGH[111] bezweifelt haben, dass solche Daten weniger sensibel sind als andere, insbesondere weniger sensibel als Inhaltsdaten. In der Tat werden im Verhaltenskodex für das Abfangen von Kommunikationsdaten als Beispiele für „Sekundärdaten“ (sowohl „Systemdaten“ wie Routerkonfigurationen, E-Mail-Adressen oder Benutzerkennungen, aber auch alternative Kontokennungen, als auch „Identifizierungsdaten“ wie der Ort eines Termins in einem Kalender oder Informationen zu Fotos wie Uhrzeit, Datum und Ort der Aufnahme) genannt. **Bezüglich des Abfangens von Massendaten verweist der EDSA ferner auf die übereinstimmende Bewertung durch den EGMR und den EuGH und erinnert an die Bedenken, die hinsichtlich Sekundärdaten geäußert wurden, für die aufgrund ihrer Sensibilität besondere**

[106] Die Begriffe „Systemdaten“ und „Identifizierungsdaten“ sind in Artikel 263 des IPA von 2016 definiert.

[107] Siehe Bericht des Independent Reviewer of Terrorism Legislation zur Überprüfung von Massenüberwachungsbefugnissen, August 2016.

[108] Siehe Artikel 152 Absatz 1 Buchstabe c und Artikel 152 Absätze 3 ff. des IPA von 2016.

[108] Siehe Artikel 152 Absatz 1 Buchstabe c und Artikel 152 Absätze 3 ff. des IPA von 2016.

[109] Siehe Artikel 152 Absatz 1 Buchstaben a und b des IPA von 2016.

[110] Siehe Urteil des EGMR, Big Brother Watch, Rn. 357, unter Verweisung an die Große Kammer: „Auch wenn der Gerichtshof nicht bezweifelt, dass zugehörige Kommunikationsdaten für die Nachrichtendienste ein wesentliches Instrument bei der Bekämpfung von Terrorismus und schwerer Kriminalität sind, ist er nicht der Auffassung, dass die Behörden einen gerechten Kompromiss zwischen den konkurrierenden öffentlichen und privaten Interessen gefunden haben, indem sie diese Daten in ihrer Gesamtheit von den für die Durchsuchung und Prüfung von Inhalten geltenden Garantien ausgenommen haben. Der Gerichtshof empfiehlt zwar nicht, dass zugehörige Kommunikationsdaten nur zugänglich sein sollten, um festzustellen, ob sich eine Person auf den Britischen Inseln befindet oder nicht, da dies bedeuten würde, dass für zugehörige Kommunikationsdaten strengerer Standards angewendet werden müssten als diejenigen, die für Inhalte gelten, doch sollten hinreichende Garantien vorhanden sein, um sicherzustellen, dass die Ausnahme zugehöriger Kommunikationsdaten von den Anforderungen gemäß Artikel 16 des RIPA auf das Maß beschränkt wird, das erforderlich ist, um festzustellen, ob sich eine Person derzeit auf den Britischen Inseln befindet.“

[111] Siehe Urteil des EuGH, Privacy International, Rn. 71: „Der mit der Übermittlung von Verkehrs- und Standortdaten an die Sicherheits- und Nachrichtendienste verbundene Eingriff in das in Art. 7 der Charta verankerte Recht ist insbesondere angesichts des sensiblen Charakters der Informationen, die diese Daten liefern können, und vor allem angesichts der Möglichkeit, anhand von ihnen ein Profil der Betroffenen zu erstellen, als besonders schwer anzusehen, da eine solche Information ebenso sensibel ist wie der Inhalt der Kommunikationen selbst. Überdies ist er geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend Urteile vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 27 und 37, sowie vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 99 und 100).“

Garantien vorgesehen werden sollten. Der EDSA bittet die Europäische Kommission daher, sorgfältig zu prüfen, ob die im Recht des Vereinigten Königreichs für diese Kategorie personenbezogener Daten vorgesehenen Garantien ein Schutzniveau gewährleisten, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

4.3.1.6 Automatisierte Verarbeitung von Kommunikationsdaten

178. Der EDSA stellt fest, dass Behörden der Intelligence Community nicht nur einfache oder komplexe Selektoren verwenden, um die gesammelten Massendaten zu filtern, sondern dass sie auch auf andere Instrumente für die automatisierte Verarbeitung zurückgreifen können, um „große Datenmengen zu analysieren, die es den Behörden ermöglichen, auch Verknüpfungen, Muster, Verbindungen oder Verhaltensweisen zu finden, die möglicherweise eine ernsthafte, Ermittlungen erfordernde Bedrohung darstellen“, wie im Bericht des Intelligence and Security Committee von 2015 dargelegt wird.[112] **Dem EDSA ist bewusst, dass dieser öffentliche Bericht Praktiken im Rahmen des vorherigen Rechtsrahmens betrifft, der später durch den IPA von 2016 ersetzt wurde. Dennoch hält er eine weitere unabhängige Bewertung und Überwachung des Einsatzes von Instrumenten für die automatisierte Datenverarbeitung durch die zuständigen Aufsichtsbehörden des Vereinigten Königreichs für erforderlich, und er ersucht die Europäische Kommission, diese Frage und die Garantien, die betroffenen Personen im EWR in diesem Zusammenhang gewährt würden bzw. werden könnten, eingehender zu bewerten.**

4.3.1.7 Compliance-Risiken und nicht konforme Praktiken zuständiger Behörden der Intelligence Community

179. Der EDSA nimmt zur Kenntnis, dass ausführliche Berichte von Aufsichtsbehörden vorliegen. Sie enthalten wertvolle Angaben zu von ihnen als positiv bewerteten Compliance-Verfahren sowie zu festgestellten Compliance-Risiken und nicht konformen Praktiken.

180. In diesem Zusammenhang hat es laut dem Bericht des IPC von 2019 bezüglich der Anwendung des Rechtsrahmens durch die verschiedenen zuständigen Behörden mehrere Anhaltspunkte für (drohende) Verstöße durch die zuständigen Behörden gegeben.

181. Zunächst hat der EDSA beobachtet, dass selbst für den MI5 und den SIS die Kriterien für die Einstufung von Datensätzen als personenbezogene Massendatensätze oder als gezielt abgerufene Daten offenbar nicht immer klar sind, besonders für den MI5 nicht, was dazu führen kann, dass für die Daten keine geeigneten Garantien zur Anwendung kommen.[113] In seinem Bericht von 2019

[112] Siehe Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, 2015, Nummer 18, S. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

[113] Siehe Annual Report of the Investigatory Powers Commissioner 2019, 15. Dezember 2020, Nummer 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: „Wir haben die positive Entwicklung des [Bulk Oversight Panel (BOP)] beobachtet und seine Wirkung auf die interne Einhaltung der Vorschriften zur Kenntnis genommen. Wir bemühen uns weiterhin, mehr Klarheit in Bezug auf das Verfahren zu gewinnen, das der MI5 bei anfänglichen Prüfungen neuer Datensätze anwendet, um Entscheidungen bei der Einstufung von Daten als personenbezogene Massendaten oder beispielsweise als gezielt abgerufene Daten besser zu verstehen. Wir waren besorgt wegen einer unaufgeklärten Aktion im Protokoll des BOP, bei der es darum ging, Unstimmigkeiten bei Zuweisungen von personenbezogenen Massendaten zwischen dem MI5 und dem SIS zu klären. Aufgrund der unterschiedlichen Verwendungszwecke der Daten und der unterschiedlichen Teilbereiche der Daten ist es möglich, dass beide Behörden dieselben Datensätze bzw. dieselben Versionen dieser Datensätze besitzen und dass die Datensätze rechtmäßig von der einen Behörde als Massendaten und von der anderen als gezielt abgerufene Daten

empfahl der IPC, „der Lösung dieser Frage Priorität einzuräumen“[114]. Auch stellt der EDSA in Bezug auf personenbezogene Massendatensätze fest, dass für die GCHQ, obwohl deren Einstufung von personenbezogenen Massendatensätzen zufriedenstellend zu sein scheint (jedoch nach wie vor vom IPC geprüft werden muss), die interne Compliance-Überprüfung von Anordnungen durch das entsprechende Team im März 2019 Anlass zu ernsten Bedenken gegeben hat, da 50 % der Begründungen für Anordnungen zum Sammeln von Massendaten, die vom Compliance-Team der GCHQ überprüft wurden, den erforderlichen Standard nicht erfüllten. Nach Angaben des IPC hatte das Compliance-Team mit Untersuchungen zu diesem Problem und mit Personalschulungen begonnen, um diesen Standard zu verbessern. Die Auffrischungsschulungen zu den Bestimmungen des IPA von 2016 und die zusätzlichen Schulungen, die von Policy- und Compliance-Netzwerken angeboten wurden, haben zu einer besseren Einhaltung der Vorschriften durch die GCHQ in diesem Bereich geführt. Der IPC erwartet bei künftigen Kontrollen nicht, dass dieser Standard wieder sinkt, wird diesen Bereich jedoch weiterhin aufmerksam überprüfen.[115] **Der EDSA teilt daher die Auffassung, dass eine weitere Überprüfung und Überwachung der genannten Elemente durch die Europäische Kommission im Rahmen der Bewertung des Schutzniveaus erforderlich sind, um sicherzustellen, dass dieser Standard – wie im Bericht des IPC hervorgehoben – verbessert wird, und erinnert daran, dass bei der Bewertung, ob das Schutzniveau eines Drittlandes der Sache nach gleichwertig ist, auch die Umsetzung und konkrete Anwendung des Rechtsrahmens zu berücksichtigen sind, wie in Artikel 45 DSGVO vorgesehen.**

182. Allgemein betont der EDSA die auch vom IPC benannten problematischen Aspekte bezüglich der von den MI5-Beamten geleiteten „aufgabenbezogenen Abfragen“, die es einem Ermittler erlauben, die für ihn verfügbaren personenbezogenen Massendatensätze mehr als einmal zu durchsuchen, sowie der „schwerwiegenden Compliance-Risiken im Zusammenhang mit bestimmten, vom MI5 genutzten Technologieumgebungen“ im Hinblick darauf, wo in der Umgebung Daten gespeichert wurden, wer darauf Zugriff hatte, in welchem Umfang sie kopiert oder weitergegeben wurden, welche Löschprozesse auf sie angewandt wurden, sowie bezüglich der Speicherfristen. Obwohl der IPC angibt, dass Maßnahmen ergriffen und Garantien eingeführt wurden, von denen einige nach wie vor manuell sind und von Menschen individuell ausgeführt werden, hebt er hervor, dass es ausschlaggebend sei, dass „der MI5 diese neuen Prozesse fortlaufend pflegt und ausreichend Ressourcen dafür bereitstellt, dass sie gut funktionieren. Wenn der MI5 eine Zunahme nicht konformer Verhaltensweisen feststellt“[116] erwartet der IPC, dass ihm diese so bald wie möglich zur Kenntnis gebracht werden. **Der EDSA bittet die Europäische Kommission daher, diese Aspekte in Zukunft genau zu überwachen.**

183. Was die GCHQ betrifft, so entnimmt der EDSA dem Bericht des IPC, dass bei Operationen im Rahmen der Massenüberwachungsanordnungen „die Qualität der Anträge auf interne Genehmigung schwankte und wir einen Verbesserungsbedarf festgestellt haben hinsichtlich der Art und Weise, wie solche Anträge formuliert waren“[117], und dass die Erläuterungen für die Verwendung allgemeiner Deskriptoren bei gezielten Eingriffen in Geräte in einigen Fällen zu allgemein und unpräzise waren[118]. Der EDSA stellte ferner fest, dass der IPC im Zusammenhang mit massenhaften Geräteeingriffen

eingestuft werden. Wenn eine der Behörden den Datenabruf fälschlicherweise als gezielt eingestuft hat, besteht die Gefahr, dass die Daten ohne entsprechende Anordnung gespeichert werden und möglicherweise keinen angemessenen Garantien unterliegen.“

[114] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 8.39.

[115] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.48.

[116] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 8.52.

[117] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.2.

[118] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummern 10.16 und 10.17.

empfiehlt, dass in den „Anträgen konsequent und ausdrücklich der Zusammenhang zwischen dem Ziel und einem gesetzlichen Zweck sowie den nachrichtendienstlichen Anforderungen festgehalten wird“[119] und dass „in allen Anträgen bei der Beurteilung der Verhältnismäßigkeit unmissverständlich auf die Gefahr kollateraler Eingriffe und auf angemessene Risikominderungsmaßnahmen eingegangen wird“[120], und dass der IPC darauf hingewiesen hat, dass trotz der Fortschritte „noch immer Verbesserungsbedarf besteht“[121] und auch in Zukunft zusätzliche Aufmerksamkeit erforderlich sein werde.

184. In Bezug auf das System der Abfrage von Massendaten gemäß dem Regulation of Investigatory Powers Act (im Folgenden „RIPA“) von 2000, der inzwischen durch Bestimmungen des IPA von 2016 ersetzt wurde, weist der EDSA darauf hin, dass die unzureichende Aufsicht sowohl bei der Auswahl von Internet-Trägern für das Abfangen als auch bei der Filterung und der Durchsuchung sowie der Auswahl abgefangener Kommunikationsdaten zu Prüfzwecken zu den zentralen Aspekten gehörte, die der EGMR in der Rechtssache Big Brother Watch, die nunmehr an die Große Kammer verwiesen wurde, als Verstöße gegen Artikel 8 der EMRK ansah, im Hinblick auf die früher geltenden Rechtsvorschriften zu den Ermittlungsbefugnissen britischer Behörden im Zusammenhang mit der nationalen Sicherheit. **Der EDSA ersucht die Europäische Kommission, den Stand des Verfahrens zu überprüfen, diese Elemente zu berücksichtigen und sie im Angemessenheitsbeschluss anzugeben, falls die Europäische Kommission diesen erlässt.**

185. In diesem Fall war der EGMR „nicht davon überzeugt, dass die Garantien für die Auswahl von Trägern für das Abfangen und für die Auswahl des für Prüfzwecke bestimmten abgefangenen Materials hinreichend solide sind, um einen angemessenen Schutz gegen Missbrauch zu gewährleisten. Höchst besorgniserregend ist jedoch das Fehlen einer leistungsfähigen, unabhängigen Aufsicht über die Selektoren und Suchkriterien, die zur Filterung abgefangener Kommunikationsdaten verwendet werden.“[122] Wie vom IPC hervorgehoben wird, „führte diese Feststellung zu einer ähnlichen Empfehlung in dem Bericht *Privacy and Security: A modern and transparent legal framework* des Intelligence and Security Committee vom März 2015“[123]. **Der EDSA begrüßt, dass der IPC dementsprechend 2019 seinen Ansatz bei der Kontrolle des Abfangens von Massendaten überprüft hat, „unter anderem auch sehr sorgfältig die komplexen technischen Abläufe der Umsetzung des Abfangens von Massendaten“[124], und sich verpflichtet hat, ab 2020 bei den Kontrollen des Abfangens von Massendaten auch „die Selektoren und Suchkriterien, auf die der EGMR in diesem Zusammenhang aufmerksam gemacht hat, eingehend zu prüfen“[125]. Angesichts der Bedeutung dieses Aspekts ist der EDSA besorgt darüber, dass die eingehende Prüfung der Selektoren und Suchkriterien durch den IPC noch nicht stattgefunden hat, und er bittet die Europäische Kommission, die diesbezüglichen Entwicklungen genau zu beobachten, zumal das konkrete Format dieser Aufsicht noch geklärt werden muss[126].**

[119] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.23.
[120] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.23.
[121] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.23.
[122] Siehe Urteil des EGMR, Big Brother Watch, Rn. 347.
[123] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.28.
[124] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.28.
[125] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.28.
[126] Siehe Annual Report of the Investigatory Powers Commissioner 2019, Nummer 10.28: „Das genaue Format dieser Kontrolle muss noch abgestimmt werden“.

4.3.2 Weiterverwendung der für Zwecke der nationalen Sicherheit erhobenen Daten und Offenlegung im Ausland

186. In Bezug auf die Weiterverwendung der für Zwecke der nationalen Sicherheit erhobenen Daten verweist die Europäische Kommission in ihrer Bewertung auf Artikel 87 Absatz 1 des DPA von 2018, in dem es heißt: „Die so erhobenen personenbezogenen Daten dürfen nicht in einer Weise verarbeitet werden, die mit dem Zweck, für den sie erhoben werden, unvereinbar ist." Der EDSA weist jedoch darauf hin, dass für diese Bestimmung Ausnahmeregelungen für die nationale Sicherheit gemäß Artikel 110 des DPA von 2018 gelten können. Der EDSA stellt ferner fest, dass die Rechtsvorschriften unabhängig davon, ob es sich um gezieltes Abfangen und Prüfen, um gezieltes Sammeln und Speichern von Kommunikationsdaten, um gezielte Eingriffe in Geräte oder um das Abfangen von Massendaten und massenhafte Geräteeingriffe handelt, die Rechtsvorschriften die Möglichkeit einer „Offenlegung im Ausland" vorsehen.

4.3.2.1 Weiterverwendung, Offenlegung im Ausland und geltender Rechtsrahmen im Vereinigten Königreich

187. Die Europäische Kommission hat Teil 4 des DPA von 2018 und insbesondere dessen Artikel 109 als einschlägige Bestimmungen genannt, in denen spezifische Anforderungen für die weitere Nutzung der erhobenen Daten und insbesondere für die internationale Übermittlung personenbezogener Daten durch Nachrichtendienste an Drittländer oder internationale Organisationen festgelegt sind. Der EDSA stellt jedoch fest, dass Artikel 110 des DPA von 2018 eine Ausnahmeregelung für die nationale Sicherheit vorsieht, wonach bestimmte Bestimmungen des DPA von 2018 nicht zur Anwendung kommen, wenn eine Ausnahme von diesen Bestimmungen zum Schutz der nationalen Sicherheit erforderlich ist. Zu den Bestimmungen, die möglicherweise nicht zur Anwendung kommen, gehören Teil 4 Kapitel 2 des DPA von 2018 zu den Grundsätzen des Datenschutzes, u. a. Zweckbindung, sowie Teil 4 Kapitel 3 des DPA von 2018 zu den Rechten betroffener Personen. Artikel 109 des DPA von 2018 kann in Verbindung mit Artikel 110 des DPA von 2018 und den Bedingungen, unter denen er angewandt wird, dazu führen, dass durch Nachrichtendienste eine internationale Übermittlung personenbezogener Daten in Drittländer erfolgt, ohne dass Bestimmungen zu den Datenschutzgrundsätzen und den Rechten betroffener Personen Anwendung finden.

188. Wie die Europäische Kommission angibt, muss eine solche Ausnahme in jedem Einzelfall bewertet werden und kann nur geltend gemacht werden, wenn die Anwendung einer bestimmten Bestimmung negative Auswirkungen auf die nationale Sicherheit hätte. So soll mit der Ausstellung einer nationalen Sicherheitsbescheinigung für die Nachrichtendienste des Vereinigten Königreichs beglaubigt werden, dass für bestimmte personenbezogene Daten, die zum Schutz der nationalen Sicherheit verarbeitet werden, eine Ausnahme erforderlich ist. Der EDSA nimmt jedoch zur Kenntnis, dass das Innenministerium des Vereinigten Königreichs in seinen Leitlinien für nationalen Sicherheitsbescheinigungen im Rahmen des DPA von 2018 von vornherein klarstellt, „dass für die Inanspruchnahme einer Ausnahmeregelung für die nationale Sicherheit keine Bescheinigung erforderlich ist; vielmehr werden Verantwortliche in den meisten Fällen selbst entscheiden, ob die Ausnahmeregelung für die nationale Sicherheit anwendbar ist." [127] Darüber hinaus wird in den Leitlinien des britischen Innenministeriums darauf hingewiesen, dass „nationale Sicherheitsbescheinigungen für personenbezogene Daten gelten können, die genau angegeben werden können oder eine breitere Kategorie personenbezogener Daten abdecken. Sie können

[127] Siehe Home Office, The Data Protection Act 2018, National Security Certificates, August 2020, Nummer 3, S. 3.

sowohl präventiv als auch rückwirkend sein.“ [128] Daher kann eine Ausnahmeregelung für die nationale Sicherheit in Bezug auf eine internationale Übermittlung personenbezogener Daten durch Nachrichtendienste in Drittländer auch Anwendung finden, wenn keine nationale Sicherheitsbescheinigung vorliegt.

189. Der EDSA stellt ferner fest, dass beispielsweise in der nationalen Sicherheitsbescheinigung DPA/S27/Security[129] des britischen Security Service (Inlandsnachrichtendienst) vorgesehen ist, dass bis zum 24. Juli 2024 personenbezogene Daten, die „für den oder im Namen, auf Anforderung, mithilfe oder mit Unterstützung des Security Service“ verarbeitet werden oder die verarbeitet werden, „wenn eine solche Verarbeitung erforderlich ist, um die ordnungsgemäße Erfüllung der in Artikel 1 des Security Service Act von 1989 beschriebenen Aufgaben des Security Service zu erleichtern“, von den entsprechenden Bestimmungen des britischen Rechts in Kapitel V der DSGVO („Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen“) ausgenommen sind. Auch wenn in den anderen öffentlich zugänglichen nationalen Sicherheitsbescheinigungen keine Ausnahme von den Bestimmungen des Artikels 109 des DPA von 2018 vorgesehen ist, muss beachtet werden, dass der Wortlaut einer nationalen Sicherheitsbescheinigung ganz oder teilweise zurückgehalten werden kann, wenn seine Veröffentlichung den Interessen der nationalen Sicherheit zuwiderlaufen würde, dem öffentlichen Interesse zuwiderlaufen würde oder die Sicherheit einer Person gefährden könnte.

190. Allgemein stellt der EDSA bei der Bewertung des Beschlussentwurfs im Hinblick auf diese Bestimmungen fest, dass die Garantien für diese Offenlegungen lediglich die Anforderung umfassen, dass der Empfänger der Daten die Erfordernisse in Bezug auf die Datensicherheit, die Beschränkung der Offenlegung auf das erforderliche Maß, die Speicherung von Daten und die Beschränkung des Zugangs zu Daten auf eine begrenzte Personenzahl erfüllt. Daher **weist der EDSA darauf hin, dass, wenn es um die Offenlegung von Daten im Ausland geht, die Anwendung der im Recht des Vereinigten Königreichs vorgesehenen Ausnahmeregelung für die nationale Sicherheit dazu führen kann, dass Garantien, die sicherstellen sollen, dass die Grundsätze der Zweckbindung, der Erforderlichkeit und der Verhältnismäßigkeit sowie die Rechte der Betroffenen, Aufsicht und Rechtsbehelfe im Bestimmungsdrittland nicht in vollem Umfang gewährt oder eingehalten würden. Der EDSA empfiehlt der Europäischen Kommission daher, in Bezug auf die Offenlegung von Daten im Ausland die im Recht des Vereinigten Königreichs vorgesehenen allgemeinen Garantien noch weiter zu prüfen, insbesondere im Hinblick auf die Anwendung von Ausnahmeregelungen für die nationale Sicherheit.**

4.3.2.2 Offenlegung von Daten im Ausland und Austausch nachrichtendienstlicher Erkenntnisse im Rahmen der internationalen Zusammenarbeit

191. Ferner stellt der EDSA fest, dass die Europäische Kommission im Zuge ihrer Angemessenheitsbewertung bestehende internationale Übereinkünfte zwischen dem Vereinigten Königreich und Drittländern oder internationalen Organisationen nicht berücksichtigt hat, die möglicherweise spezifische Bestimmungen für die internationale Übermittlung personenbezogener Daten durch Nachrichtendienste in Drittländer enthalten.

192. Der EDSA betont auch, dass sich die Bewertung der Europäischen Kommission hauptsächlich auf die Beurteilung von Teil 4 des DPA von 2018 stützt, und ist insbesondere besorgt darüber, dass es im

[128] Siehe Home Office, The Data Protection Act 2018, National Security Certificates, August 2020, Nummer 5, S. 4.

[129] Siehe DPA/S27/Security Service, Artikel 27 des DPA von 2018, Certificate of the Secretary of State, 24. Juli 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

IPA von 2016 schwerpunktmäßig um „Ersuchen“ um den Austausch nachrichtendienstlicher Erkenntnisse mit ausländischen Partnern geht, während auf andere Formen des Austauschs nachrichtendienstlicher Erkenntnisse nicht eingegangen wird. Der EDSA stellt in diesem Zusammenhang fest, dass im Beschlussentwurf der Europäischen Kommission die Verbindung zwischen dem Rechtsrahmen des Vereinigten Königreichs und der Vereinbarung zur Zusammenarbeit der Geheimdienste zwischen dem Vereinigten Königreich und den USA weder angesprochen noch bewertet wird. In einer kürzlich ergangenen Mitteilung zum 75. Jahrestag dieses Abkommens betonte die National Security Agency, die nationale Sicherheitsbehörde der USA (im Folgenden „NSA“), dass diese Partnerschaft es ermögliche, „bei minimalen Einschränkungen so viele Informationen wie möglich zwischen den beiden Behörden auszutauschen“, und dass „dieses bahnbrechende Dokument die Strategien und Verfahren für den Austausch von Kommunikations-, Übersetzungs-, Analyse- und Entschlüsselungsdaten für britische und US-amerikanische Geheimdienstexperten geschaffen“[130] habe. Das Abkommen bildete später auch die Grundlage für weitere Geheimdienstpartnerschaften mit Australien, Kanada und Neuseeland.

193. Was die Klarheit und Vorhersehbarkeit des Rechts angeht, stellt der geheime Charakter dieses Abkommens und seiner spezifischen Bestimmungen mit Blick auf die Weiterverwendung und Offenlegung von Daten im Ausland, die von Behörden des Vereinigten Königreichs zu Zwecken der nationalen Sicherheit erhoben werden, eine ernsthafte Herausforderung dar. In diesem Zusammenhang weist der EDSA darauf hin, dass der EuGH in Bezug auf das in der EU garantierte Schutzniveau betont hat, dass eine Regelung, die einen Eingriff in das Grundrecht auf Schutz personenbezogener Daten enthält, „klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen muss, so dass die Personen, deren personenbezogene Daten 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. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht“[131]. Der EDSA ist daher der Auffassung, dass die Europäische Kommission die Auswirkungen der Vereinbarung zur Zusammenarbeit der Geheimdienste zwischen dem Vereinigten Königreich und den USA im Rahmen ihrer Angemessenheitsbewertung berücksichtigen sollte.

194. Die Erste Kammer des EGMR hat in dem Urteil in der Rechtssache Big Brother Watch vom 13. September 2018 das System zum Nachrichtenaustausch im Vereinigten Königreich und insbesondere die Vereinbarung zur Zusammenarbeit der Geheimdienste zwischen dem Vereinigten Königreich und den USA geprüft. Der EGMR stellte Folgendes fest: „Der gesetzliche Rahmen, der es den Nachrichtendiensten des Vereinigten Königreichs erlaubt, abgefangenes Material von ausländischen Nachrichtendiensten anzufordern, ist nicht im RIPA enthalten. Das British–U.S. Communication Intelligence Agreement vom 5. März 1946 erlaubt ausdrücklich den Austausch von Material zwischen den Vereinigten Staaten und dem Vereinigten Königreich.“[132] Der EGMR vertrat auch die Auffassung, dass „eine rechtliche Grundlage für die Anforderung von Informationen von ausländischen Nachrichtendiensten vorhanden ist und dass dieses Recht hinreichend zugänglich

[130] Siehe Pressemitteilung der NSA, GCHQ and NSA Celebrate 75 Years of Partnership, 5. Februar 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.
[131] Siehe Schrems I, Rn. 91.
[132] Siehe Urteil des EGMR, Big Brother Watch, Rn. 425.

ist."[133] Zwar ist der EGMR zu dem Schluss gekommen, dass in Bezug auf das System zum Austausch nachrichtendienstlicher Erkenntnisse keine Verletzung von Artikel 8 EMRK[134] vorlag, doch bemerkt der EDSA, dass dieses Urteil zwischenzeitlich an die Große Kammer verwiesen wurde, deren Entscheidung noch aussteht. Der EDSA verweist ferner darauf, dass Richterin Koskelo in einem teilweise übereinstimmenden und teilweise abweichenden Sondervotum zu diesem Urteil, dem Richterin Turković folgte[135], zu dem Schluss gelangte, dass in Bezug auf das System zum Austausch nachrichtendienstlicher Erkenntnisse sehr wohl ein Verstoß gegen Artikel 8 EMRK vorliegt, und feststellte: „Man kann sich ohne Weiteres auf den Grundsatz einigen, dass eine Regelung, nach der Erkenntnisse aus abgefangenen Kommunikationen über ausländische Nachrichtendienste gewonnen werden, sei es auf der Grundlage von Ersuchen, solche Abfangoperationen durchzuführen oder ihre Ergebnisse zu übermitteln, nicht zu einer Umgehung der Garantien führen darf, die für jede Überwachung durch inländische Behörden gelten müssen (siehe Randnummern 216, 423 und 447). Jeder andere Ansatz wäre unglaubwürdig."

195. Wie in mehreren Medienberichten und Beiträgen nichtstaatlicher Organisationen[136][137] hervorgehoben wurde, stammt die letzte Fassung der Vereinbarung zur Zusammenarbeit der Geheimdienste zwischen dem Vereinigten Königreich und den USA, die veröffentlicht wurde, aus dem Jahr 1956, und seither haben sich die Kommunikationstechnologien und der Charakter der signalerfassenden Aufklärung erheblich verändert. In Medienberichten wurde beispielsweise aufgedeckt, dass die Daten, die über Seekabel übermittelt werden, die im Vereinigten Königreich anlanden, von den GCHQ abgefangen und der NSA zugänglich gemacht werden.[138]

196. Für den EDSA besteht eine zentrale Frage beim Thema des Austauschs nachrichtendienstlicher Erkenntnisse darin, ob Artikel 109 des DPA 2018 und die Bestimmungen des IPA von 2016 weiterhin anwendbar sind, wenn britische Nachrichtendienste gemäß der Vereinbarung zur Zusammenarbeit der Geheimdienste zwischen dem Vereinigten Königreich und den USA agieren. Ein weiterer zentraler Aspekt, der bewertet werden muss, ist, ob sich die Bestimmungen oder die praktische Anwendung dieses Abkommens auf das Schutzniveau personenbezogener Daten während der Übermittlung aus dem EWR in das Vereinigte Königreich auswirken oder ob ermöglicht wird, dass Nachrichtendienste anderer Drittländer unmittelbar auf personenbezogene Daten zugreifen oder diese sammeln.

197. Zusätzlich zu den Vorbehalten, die der EDSA sowohl bezüglich der „Offenlegung von Daten im Ausland" auf der Grundlage von Teil 4 des DPA von 2018 und der damit zusammenhängenden Ausnahmeregelung für die nationale Sicherheit als auch bezüglich Ersuchen gemäß dem IPA von 2016 geäußert hat, ist er **besorgt über andere Formen des Austauschs und der Offenlegung von Daten auf der Grundlage weiterer Instrumente, insbesondere der verschiedenen internationalen Übereinkünfte, die das Vereinigte Königreich mit anderen Drittländern geschlossen hat, vor allem wenn diese Instrumente nicht für die Öffentlichkeit zugänglich sind, wie etwa die Vereinbarung**

[133] Siehe Urteil des EGMR, Big Brother Watch, Rn. 427.
[134] Siehe Urteil des EGMR, Big Brother Watch, Rn. 448.
[135] Siehe Urteil des EGMR, Big Brother Watch, teilweise übereinstimmendes, teilweise abweichendes Sondervotum von Richterin Koskelo, gefolgt von Richterin Turković.
[136] Siehe BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes, 5. März 2021, https://www.bbc.com/news/uk-56284453.
[137] Siehe Privacy International, Policy Briefing – UK Intelligence Sharing Arrangements, April 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] Siehe The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 21. Juni 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

zur Zusammenarbeit der Geheimdienste zwischen dem Vereinigten Königreich und den USA. Eine solche Übereinkunft könnte bewirken, dass die genannten Garantien in Bezug auf den Zugriff auf und die Nutzung von personenbezogenen Daten für Zwecke der nationalen Sicherheit umgangen werden.

198. Der EDSA teilt die Auffassung des Sonderberichterstatters der Vereinten Nationen, Joe Cannataci, dass „der Austausch nachrichtendienstlicher Erkenntnisse weder zu einer Hintertür führen darf, um Dritten den Abruf von Daten ohne inländische Garantien zu ermöglichen, noch zu einem Schlupfloch für ausländische Regierungen mit niedrigeren Standards für den Schutz der Privatsphäre (oder anderer Menschenrechte), um Erkenntnisse von Nachrichtendiensten des Vereinigten Königreichs zu erlangen, die zu Menschenrechtsverletzungen führen könnten“[139].

199. Darüber hinaus ist **der EDSA der Auffassung, dass der Abschluss bilateraler oder multilateraler Übereinkünfte mit Drittländern für den Zweck der nachrichtendienstlichen Zusammenarbeit, die eine Rechtsgrundlage für das direkte Abfangen und Sammeln personenbezogener Daten oder für die Übermittlung personenbezogener Daten in diese Länder bieten, sich auch erheblich auf die Bedingungen für die Weiterverwendung der erhobenen Daten auswirken können, da solche Übereinkünfte den bewerteten Datenschutzrechtsrahmen des Vereinigten Königreichs beeinträchtigen dürften.**

4.3.3 Aufsicht

200. Der EDSA betont, wie wichtig eine umfassende Aufsicht durch unabhängige Aufsichtsbehörden für ein angemessenes Datenschutzniveau ist. Die Garantie der Unabhängigkeit der Aufsichtsbehörden im Sinne von Artikel 8 Absatz 3 EU-Charta soll eine wirksame und zuverlässige Überwachung der Einhaltung der Vorschriften zum Schutz natürlicher Personen im Hinblick auf die Verarbeitung personenbezogener Daten gewährleisten.

201. Beim Zugriff auf und bei der Verwendung von personenbezogenen Daten für Zwecke der nationalen Sicherheit wird die Aufsichtsfunktion hauptsächlich vom IPC und den Justizkommissaren (im Folgenden „die Justizkommissare“) wahrgenommen.

202. **Der EDSA erkennt die Einführung von Justizkommissaren im IPA von 2016 grundsätzlich als wesentliche Verbesserung an.** Übereinstimmend mit einer oben ausgesprochener Bitte wird die Europäische Kommission ersucht, die Unabhängigkeit der **Justizkommissare ausführlicher zu bewerten und insbesondere zu prüfen, inwieweit die Unabhängigkeit des IPC und des Büros des IPC (im Folgenden „IPCO“) rechtlich abgesichert ist, da im IPA von 2016 hierzu nichts zu finden ist.** Dies ist vor allem deshalb wichtig, weil der IPC über Rechtsmittel der Regierung entscheidet, wenn ein Antrag auf eine Überwachungs**maßnahme von** einem Justizkommissar abgelehnt wurde.

203. Der IPC hat sowohl Ex-ante- als auch Ex-post-Aufsichtsfunktionen. Was die Ex-ante-Aufsicht anbelangt, versteht der EDSA die Aufgabe der Justizkommissare dahingehend, dass sie darin besteht, in Einzelfällen verschiedene Überwachungsmaßnahmen zu genehmigen, darunter das gezielte Abfangen von Kommunikationsdaten und das Sammeln von Massenkommunikationsdaten. Der EDSA stellt ferner fest, dass die Vorabgenehmigung von Überwachungsmaßnahmen nicht als

[139] Siehe End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, London, 29. Juni 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

zwingende Voraussetzung für die Verhältnismäßigkeit von Überwachungsmaßnahmen aus der Rechtsprechung des EuGH abgeleitet werden kann.[140]

204. Um die Wirksamkeit dieser Aufsichtsebene beurteilen zu können, hält es der EDSA dennoch für notwendig, weiter zu klären, in welchen Szenarien rechtmäßige Abfangoperationen ohne vorherige Genehmigung der Justizkommissare möglich sind.

205. In ihrem Beschlussentwurf erwähnt die Europäische Kommission in den Fußnoten 201 und 266 „spezifische begrenzte Fälle", in denen laut den Artikeln 44 bis 52 des IPA von 2016 gezielte Abfangoperationen möglich sind. Der EDSA stellt fest, dass es sich bei den Artikeln 45 bis 51 des IPA von 2016 um Ausnahmeregelungen handelt, die angeblich nicht regelmäßig von Nachrichtendiensten in Anspruch genommen werden. Darüber hinaus **geht der EDSA davon aus**, dass in den **Fällen, in denen die Ausnahmeregelungen gelten** (z. B. Telekommunikations- und Postanbieter), die vorherige Genehmigung durch die Justizkommissare erfolgen muss, falls Strafverfolgungsbehörden oder Nachrichtendienste Zugriff auf diese Daten **anfordern**, **und ersucht die Europäische Kommission, in ihrem Beschluss zu bestätigen, dass dies korrekt ist**.

206. Der EDSA erkennt an, dass Artikel 44 Absatz 2 des IPA von 2016 das Abfangen von Kommunikationsdaten zulässt, wenn eine der Parteien (Absender oder Empfänger) darin eingewilligt hat und eine Genehmigung nach dem RIPA von 2000 oder dem Regulation of Investigatory Powers (Scotland) Act von 2000 (2000 asp 11) vorliegt, d.h. die frühere Rechtslage vor der Einsetzung der Justizkommissare. Der EDSA **ersucht** die Europäische Kommission, klarzustellen, ob dies bedeutet, dass in Fällen, in denen eine einseitige Einwilligung vorliegt, das Vorabgenehmigungsverfahren überhaupt nicht zur Anwendung käme.

207. Im Hinblick auf die Ex-post-Aufsicht ist es ebenfalls wichtig, zu überprüfen, ob eine effiziente unabhängige Aufsicht lückenlos gewährleistet ist, insbesondere wenn sie nicht als Ex-ante-Aufsicht vorgesehen ist.

208. Der EDSA stellt fest, dass für die Artikel 48 bis 52 des IPA von 2016 eine Ex-post-Überprüfung durch die Justizkommissare erfolgt, und **regt an, dass die Europäische Kommission klärt, mit welchen Anforderungen und auf wessen Initiative eine solche Ex-post-Überprüfung durchzuführen ist**.

209. Gemäß Artikel 229 Absatz 4 des IPA von 2016 muss der IPC die Ausübung bestimmter Funktionen nicht fortlaufend überprüfen. In diesem Zusammenhang ersucht der EDSA die Europäische Kommission, die Bestimmungen von Artikel 229 Absatz 4 Buchstaben d und e des IPA von 2016 hinsichtlich ihrer praktischen Auswirkungen auf die Überprüfungskompetenz des IPC zu erläutern. **Nach dem Verständnis des EDSA ist das ICO die zuständige Aufsichtsbehörde, für die die Ausnahmeregelungen nach Artikel 229 Absatz 4 des IPA von 2016 gelten, und der EDSA ersucht die Europäische Kommission, in ihrem Beschluss zu bestätigen, dass dies korrekt ist.**

210. **Es scheint,** dass die Funktion **des IPC** bei der Ex-post-Aufsicht darauf **beschränkt** ist, in Fällen von Verstößen Empfehlungen abzugeben und die betroffene Person zu informieren, wenn der Verstoß schwerwiegend ist und es im öffentlichen Interesse liegt, dass die Person informiert wird. **Der EDSA**

[140] Er stellt jedoch auch fest, dass der EuGH anlässlich der Ungültigerklärung des Datenschutzschild-Beschlusses in der Rechtssache Schrems II zur Kenntnis genommen hat, dass nach US-Recht der sogenannte FISA Court „keine individuellen Überwachungsmaßnahmen [autorisiert]; vielmehr genehmigt e[r] Überwachungsprogramme (wie PRISM oder UPSTREAM) auf der Grundlage jährlicher Zertifizierungen" (Rn. 179).

rät der Europäischen Kommission, klarzustellen, wie das IPCO wirksam für die Einhaltung der Rechtsvorschriften sorgen kann.

211. **Schließlich geht der EDSA davon aus, dass betroffene Personen sich nicht direkt an das IPCO wenden können, sondern eine Beschwerde beim ICO einreichen müssen, das allerdings im Bereich der nationalen Sicherheit nur über begrenzte Zuständigkeiten verfügt. Der EDSA empfiehlt der Europäischen Kommission daher, genauer zu erläutern, wie rechtlich sichergestellt wird, dass das IPCO in diesen Fällen Beschwerden bearbeitet.**

4.3.4 Rechtsbehelfe

212. Im Lichte der EuGH-Urteile Schrems I und Schrems II ist klar, dass das Recht auf wirksamen Rechtsschutz im Sinne von Artikel 47 EU-Charta von grundlegender Bedeutung dafür ist, dass von der Angemessenheit der Gesetze eines Drittlands ausgegangen werden kann. Die Urteile haben auch gezeigt, dass in diesem Zusammenhang dem wirksamen Rechtsschutz im Bereich des Zugriffs auf personenbezogene Daten für Zwecke der nationalen Sicherheit besondere Aufmerksamkeit gewidmet werden muss.

213. **Der EDSA erkennt an, dass das Vereinigte Königreich das IPT eingerichtet hat. Das IPT ist nicht nur für Fälle zuständig, in denen Strafverfolgungsbehörden von Ermittlungsbefugnissen Gebrauch machen, sondern auch für Fälle, in denen Nachrichtendienste dies tun. Nach dem Verständnis des EDSA fungiert das IPT als ordentliches Gericht im Sinne von Artikel 47 EU-Charta. Was ihre Befugnisse anbelangt, so wird die Europäische Kommission ersucht zu bestätigen, dass das IPT über alle in Erwägungsgrund 262 des Beschlussentwurfs genannten Befugnisse verfügt, unabhängig davon, auf welcher Rechtsgrundlage die Beschwerde eingereicht wird.**

214. Eine verdeckte Überwachung durch Nachrichtendienste bedeutet häufig, dass der Gegenstand der Überwachung, die betroffene Person, von der Überwachung keine Kenntnis hat und auch nicht haben wird. In diesem Zusammenhang hat der EDSA, wenn er US-amerikanische Rechtsvorschriften zu analysieren hatte, schon häufig seine Besorgnis über das Erfordernis der „Klagebefugnis“ in Überwachungsfällen, wie sie im US-Recht ausgelegt wird, zum Ausdruck gebracht. Vor diesem Hintergrund weist der EDSA darauf hin, dass bei einer Beschwerde beim IPT die beschwerdeführende Person lediglich vorbringen muss, dass sie glaubt, Gegenstand einer Überwachungsmaßnahme zu sein.

215. Bei der Analyse des IPT nimmt der EDSA auch besonders in den Blick, dass wiederholt festgestellt wurde, dass die Arbeitsweise des IPT mit der EMRK, wie sie vom EGMR ausgelegt wird, im Einklang steht.