

**Stellungnahme 26/2025 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 16. Oktober 2025**

## **Zusammenfassung**

Am 22. Juli 2025 leitete die Europäische Kommission das Verfahren zur Annahme ihres Entwurfs eines Durchführungsbeschlusses über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich (UK) gemäß Artikel 45 Absatz 2 DSGVO ein. Dieser Beschlussentwurf verlängert die Gültigkeit bestimmter Teile der vorherigen Angemessenheitsentscheidung vom 28. Juni 2021 in Form einer Bezugnahme bis Dezember 2031.

Am selben Tag ersuchte die Europäische Kommission den Europäischen Datenschutzausschuss um eine Stellungnahme. Die Angemessenheit des von dem Vereinigten Königreich gewährten Schutzniveaus wurde vom EDSA gestützt auf die Prüfung des Beschlussentwurfs selbst sowie auf Grundlage einer Auswertung der von der Europäischen Kommission zur Verfügung gestellten Unterlagen bewertet.

In den Mittelpunkt seiner Beurteilung stellte der EDSA sowohl die allgemeinen Datenschutzaspekte des Beschlussentwurfs als auch den Zugang von Behörden zu personenbezogenen Daten, die aus dem EWR für Zwecke der Strafverfolgung und der nationalen Sicherheit an das Vereinigte Königreich übermittelt werden, einschließlich der Rechtsbehelfe, die Personen im EWR zur Verfügung stehen.

Der EDSA prüfte ferner, ob die im Rechtsrahmen des Vereinigten Königreichs vorgesehenen Garantien tatsächlich vorhanden und wirksam sind.

Der EDSA hat hierfür seine am 28. November 2017 angenommene und zuletzt am 6. Februar 2018 überarbeitete und angenommene DSGVO-Referenzgrundlage für die Angemessenheit („DSGVO-Referenzgrundlage für Angemessenheit“) und die Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen als Hauptreferenz herangezogen.

Der EDSA begrüßt die fortgesetzte Angleichung zwischen dem Datenschutzrahmen des Vereinigten Königreichs und dem der EU, ungeachtet der jüngsten Entwicklungen im einschlägigen Rechtsrahmen des Vereinigten Königreichs. Vor diesem Hintergrund werden in dieser Stellungnahme mehrere Punkte hervorgehoben, die einer weiteren Analyse bedürfen, sowie einige Themen, die die Kommission im Rahmen ihrer Überwachungspflicht gemäß Artikel 45 Absatz 4 DSGVO in den kommenden Jahren genau beobachten sollte.

Der EDSA stellt fest, dass das Vereinigte Königreich mit dem Gesetz für die Rücknahme und Reform des beibehaltenen EU-Rechts (Retained EU Law (Revocation and Reform) Act („REUL Act“)) von 2023 Änderungen in Bezug auf den „übernommenen“ allgemeinen Rechtsrahmen der EU eingeführt hat, mit dem unter anderem der Grundsatz des Vorrangs des EU-Rechts (mit Garantien für einige Bestimmungen der DSGVO) aufgehoben und die direkte Anwendung der Grundsätze des EU-Rechts, einschließlich des Rechts auf Privatsphäre und Datenschutz, wie sie sich aus der Charta der Grundrechte ergeben, gestrichen wird. Der EDSA fordert die Kommission auf, die durch das REUL Act eingeführten Änderungen zu erläutern und genauer zu bewerten und deren Auswirkungen auf den Rechtsrahmen des Vereinigten Königreichs im Allgemeinen und dessen Datenschutzrahmen im Besonderen zu beurteilen. Der EDSA ist ferner der Ansicht, dass dies ein Bereich ist, der in Zukunft von der Kommission genau überwacht werden muss.

Der EDSA stellt fest, dass dem Secretary of State durch sekundäre Verordnungen neue Befugnisse zur Einführung von Änderungen des neuen Datenschutzrahmens eingeräumt wurden, die in bestimmten Fällen, z. B. bei internationalen Übermittlungen, bei der automatisierten Entscheidungsfindung und bei der Governance der Interoperabilitätskomponente, eine geringere parlamentarische Kontrolle

erfordern. Der EDSA fordert die Kommission auf, in der endgültigen Angemessenheitsentscheidung die Bereiche hervorzuheben, die sie sorgfältig überwachen will, da die Gefahr besteht, dass es durch sekundäre Rechtsvorschriften des Vereinigten Königreichs zu weiteren Abweichungen vom EU-Datenschutzrecht kommt.

Der EDSA nimmt Änderungen an den Vorschriften für die Übermittlung personenbezogener Daten zur Kenntnis, insbesondere die neue indikative Liste der Elemente, die bei der Angemessenheitsprüfung zu berücksichtigen sind und die wichtige Elemente nicht enthält, die in der vorherigen Angemessenheitsprüfung für das Vereinigte Königreich enthalten waren<sup>1</sup>. Dies gilt sowohl für Übermittlungen in Drittländer, die im Rahmen der DSGVO des Vereinigten Königreichs durchgeführt werden, als auch für Übermittlungen von Daten, die zu Strafverfolgungszwecken verarbeitet werden. Der EDSA fordert die Kommission auf, ihre Bewertung dieser Aspekte konkret weiter auszuarbeiten und die Entwicklungen sowie die praktische Umsetzung dieser neuen Angemessenheitsprüfung zu überwachen.

Der EDSA fordert die Kommission auf, eine detailliertere Bewertung der Umstrukturierung des Information Commissioner's Office („ICO“) als Gremium sowie der Regeln für die Ernennung und Entlassung von geschäftsführenden und nicht geschäftsführenden Mitgliedern des Gremiums vorzunehmen. Der EDSA fordert die Kommission außerdem auf, nähere Angaben zu der jüngsten Konsultation des ICO zu machen, die nach diesem Beschlussentwurf veröffentlicht wurde und die Einführung eines neuen Triage-Systems für die Bearbeitung von Beschwerden zum Gegenstand hat. Der EDSA fordert die Kommission auf, alle diese Änderungen zu überwachen, sobald sie in Kraft treten. Der EDSA nimmt die Transparenzpolitik des ICO und die Verfügbarkeit der statistischen und analytischen Daten zu seinen Durchsetzungstätigkeiten positiv zur Kenntnis, fordert die Kommission jedoch auch auf, eine detailliertere Bewertung vorzunehmen und die Anwendung der Abhilfebefugnisse, die Wirksamkeit von Sanktionen und die Abhilfemaßnahmen für betroffene Parteien im Rahmen des Datenschutzrahmens des Vereinigten Königreichs zu überwachen.

Der EDSA hält es für unerlässlich, die erweiterten Ausnahmen aus Gründen der nationalen Sicherheit im Rahmen der Strafverfolgung zu bewerten, und bleibt besonders wachsam gegenüber Ausnahmen vom Grundsatz der Verhältnismäßigkeit sowie von der Anforderung, personenbezogene Daten für einen legitimen Zweck zu verarbeiten. Ebenso sollten etwaige Ausnahmen von den Befugnissen der Aufsichtsbehörde mit Vorsicht angegangen werden. Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Der EDSA fordert die Kommission auf, ihre Bewertung in der endgültigen Angemessenheitsentscheidung zu ergänzen und insbesondere die praktische Anwendung der Ausnahmeregelungen für Strafverfolgungsbehörden im Bereich der nationalen Sicherheit zu überwachen.

Der EDSA stellt fest, dass die Verarbeitungstätigkeiten der für die Strafverfolgung zuständigen Behörden unter bestimmten Umständen unter die Vorschriften fallen können, die normalerweise für die Verarbeitung personenbezogener Daten durch nationale Sicherheitsbehörden gelten. In diesem

---

<sup>1</sup> i) die Vorschriften des Drittlandes in Bezug auf „die öffentliche Sicherheit, Verteidigung, nationale Sicherheit und das Strafrecht sowie den Zugang der Behörden zu personenbezogenen Daten“, ii) die Rechtsprechung, iii) das Bestehen wirksamer und durchsetzbarer Rechte der betroffenen Personen und die verwaltungsrechtlichen und gerichtlichen Rechtsbehelfe, die betroffene Personen, deren personenbezogene Daten übermittelt werden, tatsächlich einlegen können, und iv) eine oder mehrere unabhängige Aufsichtsbehörde(n).

Zusammenhang sollte besonders darauf geachtet werden, dass die Datenschutzregelung für die Verarbeitung im Bereich der nationalen Sicherheit nicht auf Kontexte ausgedehnt wird, die nicht mit dem nationalen Kontext in Zusammenhang stehen. Der EDSA fordert die Kommission auf zu überwachen, ob die zuständigen Behörden in der Lage sind, eine klare Unterscheidung zwischen verschiedenen Verarbeitungszwecken zu treffen, um den entsprechenden Rechtsrahmen entsprechend einzuhalten.

Der EDSA begrüßt die zwischen dem Vereinigten Königreich und den USA im Rahmen des Cloud-Act-Abkommens zwischen dem Vereinigten Königreich und den USA erzielten Klarstellungen, die für mehr Rechtsklarheit sorgen. Gleichzeitig möchte der EDSA auf die Notwendigkeit hinweisen, das Niveau der im Rahmenabkommen zwischen der EU und den USA vorgesehenen Garantien zu verbessern, dessen Garantien für den Schutz der Privatsphäre und den Datenschutz in das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den USA aufgenommen wurden. Insgesamt sieht der EDSA Klärungsbedarf hinsichtlich der Bewertung des Cloud-Act-Abkommens zwischen dem Vereinigten Königreich und den Vereinigten Staaten durch die Kommission und hinsichtlich möglicher Auswirkungen auf das Schutzniveau. Der EDSA fordert die Kommission auf, das das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den Vereinigten Staaten auch weiterhin in ihre künftigen Bewertungen und Überprüfungen einzubeziehen.

Wie kürzlich in der Erklärung 05/2024 dargelegt, hält der EDSA die Verschlüsselung für unerlässlich, um die Sicherheit und Vertraulichkeit personenbezogener Daten und der elektronischen Kommunikation zu gewährleisten. Technische Leistungshinweise gemäß IPA 2016, die Unternehmen dazu verpflichten, auf Anfrage der Regierung Verschlüsselungen zu entfernen, schaffen systemische Schwachstellen und stellen eine direkte Bedrohung für die Integrität und Vertraulichkeit elektronischer Kommunikation dar. Solche Entwicklungen verdienen Beachtung in der Angemessenheitsentscheidung, insbesondere im Hinblick auf Artikel 45 Absatz 2 Buchstabe a DSGVO, der eine Bewertung nicht nur des rechtlichen Rahmens auf dem Papier, sondern auch seine Umsetzung vorschreibt, und sollten überwacht werden.

Der EDSA stellt fest, dass mit der Änderung der Ermittlungsbefugnisse von 2024 eine spezifische Regelung für die Speicherung und Prüfung großer Mengen personenbezogener Datensätze eingeführt wurde, bei denen die Personen, auf die sich die personenbezogenen Daten beziehen, „keine oder nur geringe begründete Erwartungen an die Privatsphäre haben könnten“. Der EDSA sieht weiteren Klärungsbedarf hinsichtlich der relevanten Änderungen, insbesondere in Bezug auf die Begriffe „Einzelgenehmigungen“ und „Kategoriegenehmigungen“. Darüber hinaus fordert der EDSA die Kommission auf, die Umsetzung des Begriffs „geringe oder keine berechtigten Erwartungen an den Schutz der Privatsphäre“ in der Praxis genau zu überwachen.

## Inhaltsverzeichnis

|          |                                                                                                                                                                                   |    |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1.       | EINLEITUNG .....                                                                                                                                                                  | 7  |
| 1.1.     | Anwendungsbereich des Beschlussentwurfs der Kommission .....                                                                                                                      | 7  |
| 1.2.     | Geltungsbereich dieser Stellungnahme des EDSA .....                                                                                                                               | 8  |
| 1.3.     | Entwicklungen im Rechtsrahmen des Vereinigten Königreichs .....                                                                                                                   | 9  |
| 1.4.     | Allgemeine Bemerkungen und Bedenken .....                                                                                                                                         | 11 |
| 1.4.1.   | Vom Vereinigten Königreich eingegangene internationale Verpflichtungen .....                                                                                                      | 11 |
| 1.4.2.   | Befugnis des Secretary of State, Änderungen am DUAA im Wege von<br>Sekundärverordnungen vorzunehmen .....                                                                         | 11 |
| 2.       | Allgemeine Datenschutzaspekte .....                                                                                                                                               | 12 |
| 2.1.     | Anerkannte berechtigte Interessen .....                                                                                                                                           | 12 |
| 2.1.1.   | Allgemeine Bemerkungen .....                                                                                                                                                      | 12 |
| 2.1.2.   | Offenlegung zum Zwecke der Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe e .....                                                                                                | 13 |
| 2.2.     | Rechte des Einzelnen .....                                                                                                                                                        | 14 |
| 2.2.1.   | Auskunftsrecht .....                                                                                                                                                              | 14 |
| 2.2.2.   | Garantien für die „Ausnahme von der Einwanderungsregelung“ .....                                                                                                                  | 15 |
| 2.3.     | Einschränkungen der Weiterübermittlung .....                                                                                                                                      | 16 |
| 2.4.     | Automatisierte Entscheidungsfindung .....                                                                                                                                         | 17 |
| 2.4.1.   | Automatisierte Entscheidungsfindung und menschliche Beteiligung .....                                                                                                             | 18 |
| 3.       | Verfahrens- und Durchsetzungsmechanismus .....                                                                                                                                    | 19 |
| 3.1.     | Aufsicht und Durchsetzung .....                                                                                                                                                   | 19 |
| 3.1.1.   | Unabhängige Aufsicht .....                                                                                                                                                        | 19 |
| 3.1.2.   | Durchsetzung, einschließlich Sanktionen .....                                                                                                                                     | 20 |
| 4.       | ZUGANG ZU PERSONENBEZOGENEN DATEN UND VERWENDUNG VON PERSONENBEZOGENEN<br>DATEN, DIE AUS DER EUROPÄISCHEN UNION AN BEHÖRDEN IM VEREINIGTEN KÖNIGREICH<br>ÜBERMITTELT WERDEN ..... | 22 |
| 4.1.     | Zugriff und Nutzung durch Behörden des Vereinigten Königreichs zu Strafverfolgungszwecken<br>23                                                                                   |    |
| 4.1.1.   | Rechtsgrundlagen und anwendbare Garantien .....                                                                                                                                   | 23 |
| 4.1.1.1. | Ermittlungsbefugnisse für Strafverfolgungszwecke .....                                                                                                                            | 23 |
| 4.1.1.2. | Ausnahmen aus Gründen der nationalen Sicherheit für Strafverfolgungsbehörden .....                                                                                                | 24 |
| 4.1.2.   | Gemeinsame Kontroversen zwischen Nachrichtendiensten und Strafverfolgungsbehörden<br>des Vereinigten Königreichs .....                                                            | 27 |

|          |                                                                                                                                          |    |
|----------|------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.1.3.   | Das Recht auf Auskunft .....                                                                                                             | 27 |
| 4.1.4.   | Weitergaben.....                                                                                                                         | 28 |
| 4.1.4.1. | Ein neuer Datenschutz-Test .....                                                                                                         | 28 |
| 4.1.4.2. | Das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den USA.....                                                              | 30 |
| 4.1.5.   | Aufsicht und Rechtsschutz .....                                                                                                          | 31 |
| 4.2.     | Zugang von und Verwendung durch Behörden des Vereinigten Königreichs zu<br>Kommunikationsdaten für Zwecke der nationalen Sicherheit..... | 32 |
| 4.2.1.   | Die Verwendung von Hinweisen über die technische Leistungsfähigkeit .....                                                                | 33 |
| 4.2.2.   | Rechtsgrundlagen und anwendbare Garantien .....                                                                                          | 34 |
| 4.2.3.   | Aufsicht und Rechtsschutz .....                                                                                                          | 36 |
| 5.       | Überprüfung, Dauer und Verlängerung des Beschlussentwurfs.....                                                                           | 37 |

## 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“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum („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<sup>2</sup>,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

### HAT FOLGENDE STELLUNGNAHME ERLASSEN:

## 1. EINLEITUNG

### 1.1. ANWENDUNGSBEREICH DES BESCHLUSSENTWURFS DER KOMMISSION

1. Am 22. Juli 2025 ersuchte die Europäische Kommission („Kommission“) den Europäischen Datenschutzausschuss („EDSA“) um eine Stellungnahme zum Entwurf eines Durchführungsbeschlusses zur Änderung des Durchführungsbeschlusses (EU) 2021/1772 der Kommission vom 28. Juni 2021 gemäß der DSGVO über den Schutz personenbezogener Daten durch das Vereinigte Königreich („Beschlussentwurf“). In ihrem Beschlussentwurf kam die Kommission zu dem Schluss, dass das Vereinigte Königreich weiterhin ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die im Anwendungsbereich der DSGVO aus der Europäischen Union an das Vereinigte Königreich übermittelt werden.
2. Der EDSA stellt fest, dass mit diesem Beschlussentwurf die Geltungsdauer des Durchführungsbeschlusses (EU) 2021/1772 der Kommission vom 28. Juni 2021 gemäß der DSGVO über den Schutz personenbezogener Daten durch das Vereinigte Königreich (im Folgenden „vorheriger Angemessenheitsbeschluss zum Vereinigten Königreich“), der am 27. Juni 2025 auslaufen sollte (Sunset-Klausel), um sechs Jahre verlängert wird. Der vorherige Angemessenheitsbeschluss für das Vereinigte Königreich wurde mit dem Beschluss (EU) 2025/1225 vom 24. Juni 2025 um sechs Monate bis zum 27. Dezember 2025 verlängert, damit das Vereinigte Königreich seine Datenschutzreformen abschließen kann.<sup>3</sup>
3. In ihrem Beschlussentwurf hat die Kommission geprüft, ob die Schlussfolgerung, dass das Vereinigte Königreich ein angemessenes Schutzniveau gewährleistet, angesichts der Entwicklungen seit der Annahme der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich sachlich und rechtlich nach wie vor gerechtfertigt ist.

---

<sup>2</sup> Soweit in dieser Stellungnahme auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

<sup>3</sup> Der EDSA hat auf Anfrage die „Stellungnahme 06/2025 zur Verlängerung der Durchführungsbeschlüsse der Europäischen Kommission im Rahmen der DSGVO und der Richtlinie zum Datenschutz bei der Strafverfolgung über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich“ abgegeben.

4. Die Kommission konzentrierte sich bei ihrer Bewertung auf neue Entwicklungen im Datenschutzrecht des Vereinigten Königreichs, insbesondere auf diejenigen, die durch den Data (Use and Access) Act 2025 („DUAA“) eingeführt wurden. Die Kommission prüfte insbesondere die in Erwägungsgrund 281 des früheren Angemessenheitsbeschlusses für das Vereinigte Königreich aufgeführten Elemente, die alle im Beschlussentwurf enthalten sind.
5. Der EDSA stimmt zu, dass der Schwerpunkt der Bewertung auf allen neuen relevanten Entwicklungen in der britischen Gesetzgebung und den in der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich hervorgehobenen Elementen liegen sollte, soweit alle in Artikel 45 Absatz 2 DSGVO genannten Elemente bewertet werden. Der EDSA würde es daher begrüßen, wenn die Kommission in ihrer endgültigen Angemessenheitsentscheidung ausdrücklich klarstellt, dass alle in Artikel 45 Absatz 2 DSGVO aufgeführten Elemente geprüft wurden, um zu dem Schluss zu gelangen, dass der gesamte Rechtsrahmen des Vereinigten Königreichs weiterhin ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die aus der Europäischen Union an das Vereinigte Königreich übermittelt werden. Der EDSA würde auch die Klarstellung der Kommission begrüßen, dass sie diese Elemente im Rahmen ihrer Überwachungsfunktion laufend bewerten wird.

## 1.2. GELTUNGSBEREICH DIESER STELLUNGNAHME DES EDSA

6. Der EDSA soll der Kommission eine unabhängige Stellungnahme zur Bewertung der Angemessenheit des Schutzniveaus in einem Drittland vorlegen<sup>4</sup>, etwaige Unzulänglichkeiten im Angemessenheitsrahmen aufzeigen und Vorschläge zu deren Behebung unterbreiten<sup>5</sup>. Aufgrund der besonderen Situation des Vereinigten Königreichs ergänzt die neue Angemessenheitsentscheidung die Angemessenheitsentscheidung von 2021, die für die in diesem Beschlussentwurf nicht ausdrücklich behandelten Teile weiterhin gültig bleibt. Ebenso wie in dieser Stellungnahme stützt sich der EDSA auf seine Stellungnahme 14/2021<sup>6</sup> und entwickelt diese weiter. Daher bleiben die Analyse und die Kommentare des EDSA in seiner früheren Stellungnahme zur vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich im Allgemeinen weiterhin relevant.
7. Unter Berücksichtigung der vorstehenden Ausführungen hat sich der EDSA in seinen Stellungnahmen auf ausgewählte Punkte des Beschlussentwurfs konzentriert, insbesondere wenn weitere Klarstellungen, zusätzliche Informationen oder eine künftige Überwachung durch die Europäische Kommission erforderlich sind.
8. Der EDSA stellt ferner fest, dass gemäß den Artikeln 47 und 94 der Verordnung (EU) 2018/1725<sup>7</sup> die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union personenbezogene Daten an ein Drittland, ein Gebiet, einen Sektor oder eine internationale Organisation übermitteln dürfen, das bzw. die von der Europäischen Kommission gemäß Artikel 45 Absatz 3 DSGVO als ein angemessenes Schutzniveau gewährleistend anerkannt ist, sofern die Übermittlung ausschließlich Aufgaben dient, die

---

<sup>4</sup> Vgl. Artikel 70 Absatz 1 Buchstabe s DSGVO.

<sup>5</sup> Siehe Artikel-29-Datenschutzgruppe, Referenzgrundlage für Angemessenheit, Kapitel 2 Verfahrensaspekte für Angemessenheitsfeststellungen gemäß der DSGVO, angenommen am 28. November 2017, zuletzt überarbeitet und angenommen am 6. Februar 2018, WP254 rev.01 (gebilligt vom EDSA, siehe <https://edpb.europa.eu/our-worktools/general-guidance/endorsed-wp29-guidelines>); (im Folgenden „DSGVO-Referenzgrundlage für Angemessenheit“).

<sup>6</sup> Stellungnahme 32/2021 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 über die Angemessenheit des Datenschutzniveaus im Vereinigten Königreich, angenommen am 13. April 2021, [https://www.edpb.europa.eu/system/files/2021-04/edpb\\_opinion142021\\_ukadequacy\\_gdpr.pdf\\_en.pdf](https://www.edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf).

<sup>7</sup> Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, Abl. L 295 vom 21.11.2018, S. 39.

in die Zuständigkeit des Verantwortlichen fallen, ohne dass eine weitere Genehmigung erforderlich ist. Der EDSA fordert die Kommission auf, diese rechtliche Möglichkeit in den Erwägungsgründen der endgültigen Angemessenheitsentscheidung zu erwähnen.

### 1.3. ENTWICKLUNGEN IM RECHTSRAHMEN DES VEREINIGTEN KÖNIGREICHS

9. Wie im Beschlussentwurf dargelegt<sup>8</sup>, beabsichtigte das Vereinigte Königreich nach Ablauf des im Austrittsabkommen zwischen dem Vereinigten Königreich und der EU<sup>9</sup> am 31. Dezember 2020 vereinbarten Umsetzungszeitraums, eine neue Datenschutzregelung anzunehmen, die vom EU-Rechtsrahmen abweichen würde. Schließlich verabschiedete das Vereinigte Königreich begrenzte Änderungen seines bestehenden Datenschutzrahmens, insbesondere aufgrund des DUAA.
10. Neben dem Datenschutz betrifft eine der wichtigsten Änderungen des Rechtsrahmens des Vereinigten Königreichs seit der Annahme des vorherigen Angemessenheitsbeschlusses den „übernommenen“ allgemeinen Rechtsrahmen der EU (das sogenannte „beibehaltene EU-Recht“), d. h. Rechtsvorschriften, die durch den European Union (Withdrawal) Act 2018 in das Recht des Vereinigten Königreichs aufgenommen wurden. Das beibehaltene EU-Recht umfasste die allgemeinen Grundsätze des EU-Rechts, einschließlich der Grundrechte aus der Charta der Grundrechte der Europäischen Union („die Charta<sup>10</sup>“) und der Grundsätze der Verhältnismäßigkeit und Notwendigkeit, die für die Entwicklung und Auslegung des Datenschutzrechts im Vereinigten Königreich von Bedeutung waren. Gemäß dem Gesetz über den Austritt aus der Europäischen Union von 2018 behielt das beibehaltene EU-Recht seinen Vorrang gegenüber sekundären Rechtsvorschriften des Vereinigten Königreichs, und das beibehaltene EU-Recht war im Einklang mit den allgemeinen Grundsätzen des EU-Rechts auszulegen. Seit der Einführung des Gesetzes über das beibehaltene EU-Recht (Aufhebung und Reform) von 2023 („REUL Act“)<sup>11</sup> hat das Vereinigte Königreich jedoch die direkte Anwendung der Grundsätze des EU-Rechts aus seinem innerstaatlichen Recht gestrichen, einschließlich der aus der Charta abgeleiteten Grundrechte. Mit dem REUL Act wurde auch der Grundsatz des Vorrangs des EU-Rechts abgeschafft, da das beibehaltene EU-Recht (jetzt als „angepasstes Recht“ bezeichnet) nun im Einklang mit dem innerstaatlichen Recht des Vereinigten Königreichs und nicht mehr mit den Grundsätzen des EU-Rechts auszulegen ist. Dies stellt eine bedeutende Änderung der Rechtsordnung des Vereinigten Königreichs dar.
11. Darüber hinaus könnte, obwohl derzeit ausgesetzt, ein neuer, weniger strenger rechtlicher Test für Richter des Berufungsgerichts und des Obersten Gerichtshofs eingeführt werden, um von der bestehenden EU-Rechtsprechung abzuweichen, und zwar aufgrund des REUL Act<sup>12</sup>. Diese Änderung könnte, wenn sie umgesetzt wird, eine bedeutende Veränderung im Vereinigten Königreich bewirken.
12. Trotz dieser Änderungen begrüßt der EDSA die Aufnahme von Garantien in das REUL Act, um sicherzustellen, dass die Datenschutzgesetzgebung unter bestimmten Umständen nicht außer Kraft gesetzt wird. Zu diesen Garantien gehören die Anforderungen, dass Rechtsvorschriften, „die eine Pflicht oder Befugnis zur Verarbeitung personenbezogener Daten auferlegen, eine Anforderung der

---

<sup>8</sup> Siehe Erwägungsgrund 2 des Beschlussentwurfs.

<sup>9</sup> Der Umsetzungszeitraum ist ein im Austrittsabkommen zwischen dem Vereinigten Königreich und der EU vereinbarter Zeitraum, in dem das Vereinigte Königreich nicht mehr Mitglied der EU sein, sondern weiterhin den EU-Vorschriften unterliegen und Mitglied des Binnenmarkts und der Zollunion bleiben wird. Siehe European Union (Withdrawal Agreement) Act 2020 (Gesetz über das Austrittsabkommen).

<sup>10</sup> Charta der Grundrechte der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 391).

<sup>11</sup> Siehe Erwägungsgrund 11 des Beschlussentwurfs.

<sup>12</sup> Siehe Abschnitt 6 der Verordnung von 2024 zum Gesetz über das beibehaltene EU-Recht (Aufhebung und Reform) von 2023 (Inkrafttreten Nr. 2 und Übergangsbestimmungen) (Aufhebung).

wichtigsten Datenschutzvorschriften in Bezug auf die Verarbeitung personenbezogener Daten nicht überwiegen“ und dass der Datenschutzrahmen weiterhin Vorrang vor anderen Rechtsvorschriften des Vereinigten Königreichs hat<sup>13</sup>. Der EDSA weist jedoch darauf hin, dass diese Garantien auch zwei Ausnahmen umfassen: i) wenn das Parlament des Vereinigten Königreichs beschließt, Datenschutzanforderungen bewusst außer Kraft zu setzen<sup>14</sup> und ii) wenn bestimmte Bestimmungen des DPA 2018 ausgenommen sind und somit Vorrang vor der DSGVO des Vereinigten Königreichs haben<sup>15</sup>. Die Auswirkungen der zweiten Ausnahme sind nach wie vor ungewiss und werden im Vereinigten Königreich erörtert.

13. In Bezug auf den Schutz der in der Charta verankerten Grundrechte wird in Erwägungsgrund 12 des Beschlussentwurfs erläutert, dass alle Verweise auf Grundrechte und Grundfreiheiten in der DSGVO des Vereinigten Königreichs und im Datenschutzgesetz von 2018 (DPA 2018) durch Verweise auf Rechte gemäß der Europäischen Menschenrechtskonvention ersetzt wurden, die gemäß dem Menschenrechtsgesetz von 1998 (Human Rights Act 1998) in die nationale Gesetzgebung aufgenommen wurden<sup>16</sup>.
14. Der EDSA fordert die Kommission auf, eine detailliertere Bewertung dieser Änderungen der britischen Rechtsordnung vorzunehmen, die unter den Punkten 10, 11 und 12 oben beschrieben sind, um die durch das REUL Act herbeigeführten Änderungen zu erläutern und ihre Auswirkungen auf den britischen Datenschutzrahmen zu bewerten. Der EDSA ist ferner der Ansicht, dass dies ein Bereich ist, der in Zukunft von der Kommission genau überwacht werden muss, und fordert die Kommission auf, dies zu tun.
15. Schließlich weist der EDSA auf mehrere Änderungen im DUAA hinsichtlich des für die elektronische Kommunikation, einschließlich Cookies, geltenden Rechtsrahmens hin und erinnert daran, dass die Verarbeitung personenbezogener Daten den sachlichen Anwendungsbereich der DSGVO des Vereinigten Königreichs auslösen könnte<sup>17</sup>. Daher fordert sie die Kommission auf, diese in ihre Bewertung für die endgültige Entscheidung einzubeziehen, soweit sie Auswirkungen auf den Datenschutz haben könnten. Der EDSA fordert die Kommission ferner auf, die praktischen Auswirkungen der Änderungen im Zusammenhang mit Cookies, die von der Einwilligung ausgenommen sind, genau zu überwachen.

---

<sup>13</sup> Siehe Abschnitt 183A DSB 2018 in der durch Abschnitt 106 Absatz 2 DUAA eingeführten Fassung.

<sup>14</sup> Siehe Abschnitt 183(A)(3) DPA 2018 in der durch Abschnitt 106 Absatz 2 DUAA eingeführten Fassung.

<sup>15</sup> Diese Bestimmungen sind in Abschnitt 186 Absatz 3 DPA 2018 aufgeführt. Das bedeutet, dass bei einem Konflikt zwischen Artikel 23 der DSGVO des Vereinigten Königreichs und einem der aufgeführten Abschnitte, beispielsweise Anhang 2 DPA 2018, der die Ausnahmen von den Rechten der betroffenen Personen enthält, die Auslegung des DPA 2018 Vorrang hat.

<sup>16</sup> Siehe Artikel 8 der Europäischen Menschenrechtskonvention.

<sup>17</sup> Europäischer Datenschutzausschuss, Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO, insbesondere in Bezug auf die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden, angenommen am 12. März 2019, abrufbar unter: [https://www.edpb.europa.eu/sites/default/files/files/file1/201905\\_edpb\\_opinion\\_eprivacydir\\_gdpr\\_interplay\\_en\\_0.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf).

## 1.4. ALLGEMEINE BEMERKUNGEN UND BEDENKEN

### 1.4.1.VOM VEREINIGTEN KÖNIGREICH EINGEGANGENE INTERNATIONALE VERPFLICHTUNGEN

16. In Bezug auf die vom Vereinigten Königreich eingegangenen internationalen Verpflichtungen<sup>18</sup> begrüßt der EDSA, dass sich das Vereinigte Königreich weiterhin an die EMRK hält und der Gerichtsbarkeit des EGMR unterliegt. Darüber hinaus ist das Vereinigte Königreich auch dem Übereinkommen 108<sup>19</sup> und seinem Zusatzprotokoll<sup>20</sup> beigetreten und hat das Übereinkommen 108+<sup>21</sup> im Jahr 2018 unterzeichnet. Diese internationalen Verpflichtungen sind wichtige Erwägungen<sup>22</sup> und sollten im Rahmen der Bewertung der Verlängerung sowohl der Angemessenheitsbeschlüsse für das Vereinigte Königreich nach der DSGVO als auch der Richtlinie zum Datenschutz bei der Strafverfolgung berücksichtigt werden.
17. Insgesamt unterstützt der EDSA die Bemühungen um eine rasche Ratifizierung des Übereinkommens 108+ durch Drittländer als einen bedeutenden Schritt zur Angleichung an international anerkannte Datenschutzgrundsätze und als Zeichen ihres Engagements für umfassendere Standards und Grundrechte.

### 1.4.2.BEFUGNIS DES SECRETARY OF STATE, ÄNDERUNGEN AM DUAA IM WEGE VON SEKUNDÄRVERORDNUNGEN VORZUNEHMEN

18. Obwohl die meisten der am Datenschutzrahmen des Vereinigten Königreichs vorgenommenen Änderungen darauf abzielen, die Einhaltung der Rechtsvorschriften zu klären und zu erleichtern, können einige Änderungen je nach ihrer Umsetzung Auswirkungen auf die Standards für den Schutz personenbezogener Daten im Vereinigten Königreich haben.
19. In diesem Zusammenhang stellt der EDSA fest, dass dem Secretary of State neue Befugnisse übertragen wurden, um Änderungen an der DUAA über sekundäre Rechtsvorschriften vorzunehmen, die einer geringeren parlamentarischen Kontrolle unterliegen. In bestimmten Fällen, z. B. bei internationalen Übermittlungen (siehe Abschnitt 2.3), automatisierter Entscheidungsfindung (Abschnitt 2.4) und der Verwaltung der Interoperabilitätskomponenten (Abschnitt 3), sind diese neuen Befugnisse weit gefasst, ohne dass im Beschlussentwurf weitere Angaben dazu gemacht werden, welche Garantien eingeführt werden und wie diese Befugnisse in der Praxis genutzt werden sollen.
20. Der EDSA fordert die Kommission auf, in der endgültigen Angemessenheitsentscheidung die Bereiche hervorzuheben, die sie sorgfältig überwachen will, da die Gefahr besteht, dass es durch sekundäre Rechtsvorschriften des Vereinigten Königreichs zu weiteren Abweichungen vom EU-Datenschutzrecht kommt.

---

<sup>18</sup> Siehe Kapitel 1: Einige allgemeine Informationen zum Konzept der Angemessenheit des Angemessenheitsreferenzrahmens.

<sup>19</sup> Siehe Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, Übereinkommen 108, 28. Januar 1981.

<sup>20</sup> Siehe Zusatzprotokoll zum Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, zur Unterzeichnung aufgelegt am 8. November 2001.

<sup>21</sup> Siehe Protokoll zur Änderung des Übereinkommens zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten („Übereinkommen 108+“), 18. Mai 2018.

<sup>22</sup> Siehe Erwägungsgrund 105 DSGVO.

## 2. ALLGEMEINE DATENSCHUTZASPEKTE

### 2.1. ANERKANNTE BERECHTIGTE INTERESSEN

#### 2.1.1. ALLGEMEINE BEMERKUNGEN

21. In den Erwägungsgründen 22, 23 und 24 konzentriert sich die Kommission in ihrer Bewertung auf die Einführung einer neuen Rechtsgrundlage, nämlich die Verarbeitung, die zur Wahrung eines anerkannten berechtigten Interesses erforderlich ist. In Anhang 1 der aktualisierten DSGVO des Vereinigten Königreichs sind diese anerkannten berechtigten Interessen aufgeführt.
22. Gemäß den Leitlinien des ICO zu diesem Thema<sup>23</sup> müssen Datenverantwortliche, die sich auf ein anerkanntes berechtigtes Interesse als Rechtsgrundlage stützen, weiterhin alle anderen Anforderungen der DSGVO des Vereinigten Königreichs erfüllen, einschließlich der Gewährleistung, dass die Verarbeitung notwendig und verhältnismäßig ist, um den vorab genehmigten Zweck zu erreichen. Da dies im Beschlussentwurf nicht erwähnt wird und ein wesentliches Element für die Schlussfolgerung darstellt, dass diese neue Rechtsgrundlage das Schutzniveau der Rechte der betroffenen Personen nicht beeinträchtigt, fordert der EDSA die Kommission auf, diesen Punkt zu klären.
23. Die Auflistung anerkannter berechtigter Interessen im Gesetz erscheint an sich nicht problematisch, ebenso wenig wie die Entscheidung, eine solche neue Rechtsgrundlage einzuführen – die für mehr Klarheit für die Verantwortlichen sorgt und zu begrüßen ist.
24. Der EDSA stellt jedoch fest, dass bestimmte anerkannte legitime Interessen Folgendes umfassen: i) die Notwendigkeit der Verarbeitung personenbezogener Daten zum Schutz der nationalen Sicherheit, zum Schutz der öffentlichen Sicherheit oder aus Verteidigungsgründen („Bedingung der nationalen Sicherheit, der öffentlichen Sicherheit und der Landesverteidigung“), ii) die Notwendigkeit der Verarbeitung personenbezogener Daten zur Aufdeckung, Untersuchung oder Verhütung einer Straftat („Straftatbestand“) und iii) die „Offenlegung für die Zwecke der in Artikel 6 Absatz 1 Buchstabe e beschriebenen Verarbeitung“.
25. In Bezug auf die Voraussetzung „nationale Sicherheit, öffentliche Sicherheit und Verteidigung“ und die Voraussetzung „Kriminalität“ stellt der EDSA fest, dass der Beschlussentwurf keine weiteren Informationen über die praktische Anwendung dieser Rechtsgrundlagen durch Verantwortliche und Auftragsverarbeiter enthält. Der EDSA würde es begrüßen, wenn die Kommission weitere Einzelheiten zu den zusätzlichen Informationen und Garantien vorlegen könnte, die sie von den zuständigen britischen Behörden zur praktischen Anwendung dieser Rechtsgrundlage erhalten hat, und fordert die Kommission auf, die Anwendung dieser Rechtsgrundlage zu überwachen.
26. Der EDSA stellt außerdem fest, dass das ICO derzeit spezifische Leitlinien zu diesem Thema ausarbeitet, die zum Zeitpunkt dieser Stellungnahme eine Definition dieser Begriffe enthalten. Angesichts der Bedeutung von Klarstellungen zu diesen Konzepten fordert der EDSA die Kommission auf, die Entwicklung der Leitlinien des ICO genau zu beobachten.

---

<sup>23</sup> Siehe ICO-Leitlinien zu berechtigten Interessen, abrufbar unter <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/>.

## 2.1.2. OFFENLEGUNG ZUM ZWECKE DER VERARBEITUNG GEMÄß ARTIKEL 6 ABSATZ 1 BUCHSTABE E

27. Der EDSA stellt fest, dass das neu eingeführte anerkannte berechtigte Interesse, das „die Offenlegung für die in Artikel 6 Absatz 1 Buchstabe e beschriebenen Verarbeitungszwecke“ erlaubt, die Möglichkeit einführt, personenbezogene Daten auf freiwilliger Basis an Behörden weiterzugeben. Wie das ICO in seinen jüngsten Leitlinien erläutert<sup>24</sup>, verleiht dieses anerkannte berechtigte Interesse den ersuchenden Behörden an sich kein Recht auf Zugang zu personenbezogenen Daten, aber ein Verantwortlicher kann sich auf dieses vorab genehmigte Interesse berufen, wenn die Behörden angeben, dass sie Daten für die Wahrnehmung ihrer öffentlichen Aufgaben oder Funktionen benötigen. Der EDSA weist außerdem darauf hin, dass solche Anträge auf Offenlegung öffentlicher Aufgaben nicht nur für personenbezogene Daten gestellt werden können, die für Zwecke verwendet werden sollen, die unter die DSGVO des Vereinigten Königreichs fallen, sondern sich auch auf Verarbeitungszwecke gemäß Teil 3 und Teil 4 des Datenschutzgesetzes von 2018 beziehen können. Folglich ist diese Änderung auch im Hinblick auf den Zugang staatlicher Stellen zu Zwecken der Strafverfolgung und der nationalen Sicherheit von Bedeutung.<sup>25</sup>
28. In diesem Zusammenhang stellt sich die Frage, welche Kriterien der Verantwortliche prüfen muss, um zu entscheiden, ob er auf ein Auskunftersuchen hin freiwillig Daten bereitstellt. Insbesondere, wie das ICO in ihren Leitlinien<sup>26</sup> hervorhebt, geht der EDSA davon aus, dass sich die Notwendigkeitsprüfung für diese anerkannte berechtigte Interessenbedingung von den anderen in Anhang 1 genannten Bedingungen unterscheidet. Bei Anträgen auf Offenlegung öffentlicher Aufgaben bedeutet die Notwendigkeit, dass der Verantwortliche prüfen muss, welche Verarbeitung erforderlich ist, um die angeforderten personenbezogenen Informationen offenzulegen. Der Verantwortliche muss prüfen, ob die Informationen, die er weitergeben möchte, verhältnismäßig und für die Erfüllung des Antrags erforderlich sind. Die Notwendigkeitsprüfung erstreckt sich hingegen nicht darauf, ob die personenbezogenen Daten für die Erfüllung der öffentlichen Aufgabe oder Funktion tatsächlich erforderlich sind, da sich der für die Verarbeitung Verantwortliche auf die Erklärung des Antragstellers verlassen kann, dass er die personenbezogenen Daten für eine bestimmte öffentliche Aufgabe benötigt<sup>27</sup>. Tatsächlich ist der Verantwortliche in vielen Fällen, insbesondere wenn Ersuchen aus Gründen der Strafverfolgung oder der nationalen Sicherheit gestellt werden, nicht in der Lage, eine solche Bewertung durchzuführen.
29. Vor diesem Hintergrund fordert der EDSA die Kommission auf, die praktische Anwendung dieser Bestimmung genau zu überwachen.
30. Nach Ansicht des EDSA sollten Strafverfolgungs- und nationale Sicherheitsbehörden diesen Mechanismus nicht dazu nutzen, um bestehende gesetzliche Beschränkungen ihrer verbindlichen Datenerhebungsbefugnisse zu umgehen oder mehr Daten zu erheben, als für die Erfüllung ihrer Aufgaben unbedingt erforderlich sind. Darüber hinaus hält es der EDSA für wichtig, dass die für die Verarbeitung Verantwortlichen die Leitlinien des ICO zur Validierung von Anträgen auf Offenlegung

---

<sup>24</sup> Siehe Fußnote 23.

<sup>25</sup> Siehe ICO-Leitlinien zu den Bedingungen für Anträge auf Offenlegung öffentlicher Aufgaben, abrufbar unter <https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/what-are-the-recognised-legitimate-interest-conditions/public-task-disclosure-request-condition/>.

<sup>26</sup> Siehe Fußnote 23.

<sup>27</sup> Siehe Fußnote 23.

öffentlicher Aufgaben berücksichtigen, und fordert die Kommission auf, diesen Aspekt in die regelmäßige Überprüfung der Entscheidung aufzunehmen.<sup>28</sup>

## 2.2. RECHTE DES EINZELNEN

31. Der EDSA nimmt die Analyse der Kommission zur Kenntnis, dass im Bereich der Rechte des Einzelnen nur begrenzte Änderungen vorgenommen wurden. Dies umfasst Änderungen an Artikel 12 und einen neuen Artikel 12A der DSGVO des Vereinigten Königreichs, in denen die Fristen für die Beantwortung von Anfragen betroffener Personen näher ausgeführt werden.<sup>29</sup> Darüber hinaus enthält Artikel 13 Absatz 5 der DSGVO des Vereinigten Königreichs eine Ausnahme vom Recht auf Auskunft, wenn personenbezogene Daten für wissenschaftliche oder historische Forschungszwecke unter weiteren Schutzvorkehrungen gemäß Artikel 84B der DSGVO des Vereinigten Königreichs verarbeitet werden. Der EDSA ist der Ansicht, dass beide Änderungen das in der Sache gleichwertige Schutzniveau, das die DSGVO des Vereinigten Königreichs bietet, nicht untergraben.

### 2.2.1. AUSKUNFTSRECHT

32. Mit Artikel 15 Absatz 1A der DSGVO des Vereinigten Königreichs wird eine Verhältnismäßigkeitsprüfung eingeführt, wie sie in der nationalen Rechtsprechung des Vereinigten Königreichs entwickelt wurde. Insbesondere müssen die für die Verarbeitung Verantwortlichen nur „angemessene und verhältnismäßige Suchmaßnahmen“ durchführen, um Zugangsanfragen nachzukommen.
33. Der EDSA stellt fest, dass eine solche Verhältnismäßigkeitsprüfung im EU-Datenschutzrahmen nicht vorgesehen ist, der keine allgemeine Vorbehaltsklausel hinsichtlich der Verhältnismäßigkeit der Anstrengungen vorsieht, die der Verantwortliche unternehmen muss, um dem Antrag der betroffenen Person gemäß Artikel 12 DSGVO nachzukommen, sondern lediglich in Unterabschnitt 5 Gründe für eine Ablehnung nennt.<sup>30</sup>
34. Daher ist es nach Ansicht des EDSA wichtig, den Begriff „angemessene und verhältnismäßige Durchsuchungen“ angemessen zu definieren, der eng und in ausreichend einheitlicher Weise ausgelegt werden sollte. Die Verantwortlichen sollten ein einheitliches Verständnis davon haben, was „angemessen und verhältnismäßig“ ist, sei es auf der Grundlage der Rechtsprechung oder auf der Grundlage der Leitlinien einer Aufsichtsbehörde, da die Anwendung dieses Begriffs möglicherweise zu unterschiedlichen Standards bei der Einhaltung des Auskunftsrechts führen könnte, insbesondere je nach dem Umfang der technischen und organisatorischen Maßnahmen, die der Verantwortliche zur Bearbeitung von Auskunftersuchen ergriffen hat. Der EDSA würde es begrüßen, wenn die Kommission detailliertere Informationen zur Auslegung des Begriffs „angemessene und verhältnismäßige

---

<sup>28</sup> In den Leitlinien des ICO zu den Bedingungen für Anträge auf Offenlegung öffentlicher Aufgaben (siehe Fußnote 25) wird klargestellt, dass Verantwortliche z. B. verlangen sollten, dass das Ersuchen schriftlich gestellt wird, und Überprüfungen vornehmen sollten, um die Echtheit des Ersuchens oder die Befugnis der Mitarbeiter der Organisation sicherzustellen, in ihrem Namen zu handeln.

<sup>29</sup> Vor allem aufgrund der Notwendigkeit, die Identität der betroffenen Person zu bestätigen oder eine Gebühr zu entrichten.

<sup>30</sup> Artikel 12 Absatz 5 DSGVO: „Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) eine angemessene Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.“

Durchsuchungen“ auf der Grundlage der verfügbaren nationalen Leitlinien und Rechtsprechung bereitstellen könnte. Vor diesem Hintergrund fordert der EDSA die Kommission auf, darauf zu achten, dass das Recht auf Zugang nicht unangemessen eingeschränkt wird.

### 2.2.2. GARANTIE FÜR DIE „AUSNAHME VON DER EINWANDERUNGSREGELUNG“

35. Die frühere sogenannte „Einwanderungsausnahmeregelung“<sup>31</sup> ermöglichte es den mit der „Einwanderungskontrolle“ befassten Kontrollstellen, bestimmte Rechte der betroffenen Personen gemäß dem DPA 2018 einzuschränken, wenn dies bestimmte Einwanderungskontrollmaßnahmen beeinträchtigen könnte<sup>32</sup>. Aufgrund von Zweifeln an der Rechtmäßigkeit zum Zeitpunkt der Annahme der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich wurde die Verarbeitung personenbezogener Daten im Rahmen der Ausnahmeregelung aus dem Anwendungsbereich dieser Entscheidung ausgeschlossen.
36. Seit der letzten Angemessenheitsentscheidung für das Vereinigte Königreich wurde die Einwanderungsausnahme zweimal durch Schutzmaßnahmen ergänzt<sup>33</sup>. Der Vorschlag enthält nun die folgenden Garantien: i) sie darf nur von Fall zu Fall geltend gemacht werden, ii) die Rechte und Freiheiten der betroffenen Person und mögliche Schwachstellen werden berücksichtigt, iii) der Secretary of State Aufzeichnungen über die Inanspruchnahme der Einwanderungsausnahme führt und die betroffene Person allgemein über deren Anwendung informiert, und iv) klargestellt wird, dass die Inanspruchnahme der Einwanderungsausnahme auf die Verarbeitung durch den Secretary of State (einschließlich des Secretary of Stateiums des Vereinigten Königreichs und seiner Agenturen) beschränkt ist. Darüber hinaus wurde die erforderliche Abwägung detailliert beschrieben, anhand derer festgestellt werden soll, ob die Ausübung der Rechte der betroffenen Person eine wirksame Einwanderungskontrolle beeinträchtigen könnte. Das ICO hat außerdem detaillierte Leitlinien zur Anwendung der Ausnahmeregelung herausgegeben. In seinen Leitlinien bestätigte es die enge Auslegung der Ausnahmeregelung und dass Beschränkungen im Rahmen der Einwanderungsausnahmeregelung nur selektiv auf bestimmte Rechte der betroffenen Personen angewendet werden sollten. Sie stellte ferner fest, dass die für die Abwägungsprüfung Verantwortlichen bei der Durchführung der Abwägungsprüfung sicherstellen müssen, dass das Risiko für die Einwanderungskontrolle erheblich ist und das Risiko für die Interessen der Person überwiegt.
37. Der EDSA nimmt die detaillierte Analyse der Kommission zur Kenntnis. Vor dem Hintergrund der rechtlichen Herausforderungen, die diesen Änderungen vorausgingen, fordert der EDSA die Kommission auf, ihre weitere Anwendung zu überwachen.

---

<sup>31</sup> Siehe Anhang 2 zum DPA 2018, Teil 1 der vorherigen Fassung des DPA.

<sup>32</sup> Siehe Absätze 61 und 62 der Stellungnahme 14/2021 des EDSA: „die Aufrechterhaltung einer wirksamen Einwanderungskontrolle“ oder „die Untersuchung oder Aufdeckung von Tätigkeiten, die die Aufrechterhaltung einer wirksamen Einwanderungskontrolle untergraben würden“.

<sup>33</sup> Durch Verordnungen in den Jahren 2022 und 2024.

### 2.3. EINSCHRÄNKUNGEN DER WEITERÜBERMITTLUNG

38. Der EDSA begrüßt, dass die Kommission der praktischen Anwendung der Vorschriften des Vereinigten Königreichs über die Übermittlung personenbezogener Daten an Drittländer weiterhin Aufmerksamkeit widmet, und fordert die Kommission auf, dieses Engagement aufrechtzuerhalten und zu vertiefen. Dies ist insbesondere relevant im Hinblick auf die Befugnis des Secretary of State, neue gezielte Vorschriften zu erlassen, um Übermittlungen zu genehmigen i) an einen bestimmten Sektor oder ein bestimmtes geografisches Gebiet innerhalb eines Drittlandes; ii) an einen bestimmten Verantwortlichen oder Auftragsverarbeiter; iii) an einen bestimmten Empfänger der personenbezogenen Daten; iv) bestimmter spezifischer Arten personenbezogener Daten; v) die mit bestimmten spezifischen Mitteln erfolgen; oder vi) auf der Grundlage einschlägiger Rechtsvorschriften, Regelungen, Listen oder anderer Vereinbarungen oder Dokumente, die von Zeit zu Zeit in Kraft treten; und einer Person einen Ermessensspielraum einzuräumen (Artikel 45A Absatz 4 der DSGVO des Vereinigten Königreichs).
39. Der EDSA geht davon aus, dass Artikel 45A Absatz 4 der DSGVO des Vereinigten Königreichs Flexibilität bei der Genehmigung bestimmter Übermittlungen ermöglichen soll. So geht der EDSA beispielsweise in Bezug auf die Ziffern ii und iii davon aus, dass sie Übermittlungen an private Stellen in einem Drittland abdecken könnten. Dies würde bedeuten, dass solche privaten Einrichtungen sich verpflichten, die Datenschutzprüfung zu erfüllen. Es bleibt unklar, wie der Secretary of State in der Praxis beurteilen würde, ob bestimmte für die Verarbeitung Verantwortliche mit Sitz in einem Drittland, das nicht als angemessen angesehen wird, die Datenschutzanforderungen erfüllen können (beispielsweise in Bezug auf Rechtsbehelfe). Ebenso bleibt unklar, wie die Datenschutzprüfung für die Ziffern iv und v von Artikel 45A Absatz 4 DSGVO des Vereinigten Königreichs durchgeführt würde.
40. Der EDSA würde es begrüßen, wenn die Kommission weitere Einzelheiten zu den zusätzlichen Informationen und Garantien zur praktischen Anwendung des Datenschutztests vorlegen und ihre Einschätzung dazu erläutern würde, wie das Schutzniveau in solchen Situationen gewahrt wird.<sup>34</sup> Der EDSA fordert die Kommission außerdem auf, die Entwicklungen bei der Anwendung dieser Bestimmung genau zu beobachten.
41. Darüber hinaus geht aus zusätzlichen Informationen der Kommission hervor, dass das Kriterium der Zweckmäßigkeit einer Erleichterung der Übermittlung personenbezogener Daten nach und aus dem Vereinigten Königreich kein Bestandteil der Datenschutzprüfung ist, sondern lediglich ein zusätzlicher Faktor, den der Secretary of State berücksichtigen kann, wenn die Kriterien der Prüfung vollständig erfüllt sind. Der EDSA fordert die Kommission auf, dies in ihrem endgültigen Angemessenheitsbeschluss klarzustellen, da dies aus dem Wortlaut des Gesetzes nicht ganz klar hervorgeht, und die praktischen Auswirkungen und die Umsetzung dieses Kriteriums zu überwachen.
42. In Bezug auf den neuen Datenschutztest, der durch die DUAA (<sup>35</sup>) eingeführt wurde, stellt der EDSA fest, dass die neue indikative Liste der Elemente, die bei der Angemessenheitsprüfung zu berücksichtigen sind, nicht erschöpfend ist und dass der neue Angemessenheitstest vorsieht, dass das Schutzniveau für betroffene Personen in Empfänger-Drittländern oder internationalen Organisationen „nicht wesentlich niedriger“ ist als das Schutzniveau, das für betroffene Personen nach den einschlägigen Datenschutzvorschriften des Vereinigten Königreichs vorgesehen ist. In dieser Liste werden wichtige Elemente gestrichen, die beim vorherigen Angemessenheitstest des Vereinigten Königreichs aufgeführt wurden und die eine wichtige Rolle bei der Beurteilung spielen, ob ein Drittland

---

<sup>34</sup> Siehe Artikel 45 Buchstabe A Nummer 4 DSGVO des Vereinigten Königreichs.

<sup>35</sup> Siehe Erwägungsgrund 42 des Beschlussentwurfs.

ein im Wesentlichen gleichwertiges Schutzniveau für personenbezogene Daten bietet. Der neue Test bezieht sich nicht mehr auf i) die Vorschriften des Drittlandes in Bezug auf „öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie den Zugang öffentlicher Behörden zu personenbezogenen Daten“, ii) die Rechtsprechung (stattdessen bezieht sich der neue Test nun auf „Verfassung, Traditionen und Kultur des Landes“), iii) das Bestehen wirksamer und durchsetzbarer Rechte der betroffenen Personen und die Verwaltungs- und Rechtsbehelfe, die betroffene Personen, deren personenbezogene Daten übermittelt werden, tatsächlich einlegen können (stattdessen bezieht sich der neue Test auf (b) das Bestehen und die Befugnisse einer Behörde, die für die Durchsetzung des Schutzes der betroffenen Personen in Bezug auf die Verarbeitung personenbezogener Daten in dem Land oder durch die Organisation zuständig ist, (c) Vorkehrungen für gerichtliche oder außergerichtliche Rechtsbehelfe für betroffene Personen im Zusammenhang mit einer solchen Verarbeitung) und iv) eine oder mehrere unabhängige Aufsichtsbehörden (stattdessen bezieht sich der neue Test auf eine „Behörde, die für die Durchsetzung des Schutzes der betroffenen Personen in Bezug auf die Verarbeitung personenbezogener Daten in dem Land oder durch die Organisation zuständig ist“).

43. Zwar wird anerkannt, dass die Angemessenheitsreferenz der DSGVO nur begrenzte Einzelheiten zu diesem Aspekt enthält, doch erinnert der EDSA an seinen Verweis darauf, dass „das Schutzniveau natürlicher Personen, deren Daten übermittelt werden, durch die Weiterübermittlung nicht beeinträchtigt werden darf“ <sup>(36)</sup>, was nicht so ausgelegt werden kann, dass es nicht auch die Notwendigkeit einer unabhängigen Aufsichtsbehörde und wirksamer und durchsetzbarer Rechte der betroffenen Personen umfasst.
44. Der EDSA fordert die Kommission auf, ihre Bewertung dieser Aspekte konkret weiter auszuarbeiten. Eine solche Klarstellung würde große Rechtssicherheit schaffen und dazu beitragen, das Vertrauen in das Angemessenheitsinstrument zu stärken. Der EDSA fordert die Kommission außerdem auf, die Entwicklungen und die praktische Umsetzung des neuen Angemessenheitstests genau zu beobachten.
45. In Bezug auf die (assoziierte) Mitgliedschaft des Vereinigten Königreichs im CBPR stellt der EDSA fest, dass die derzeitige Mitgliedschaft keine Erleichterung des Datentransfers vom Vereinigten Königreich zu anderen Mitgliedern des CBPR-Forums mit sich bringt. Der EDSA begrüßt die diesbezügliche Haltung der Kommission, einschließlich der Verpflichtung, die weiteren Entwicklungen in dieser Hinsicht weiterhin genau zu beobachten, insbesondere wenn das Vereinigte Königreich beabsichtigt, Vollmitglied zu werden, und erinnert daran, dass CBPRs nicht als ausreichender Schutz für personenbezogene Daten aus der EU anerkannt sind.

## 2.4. AUTOMATISIERTE ENTSCHEIDUNGSFINDUNG

46. Der EDSA nimmt Abschnitt 80 des DUAA (Einführung der Artikel 22A bis 22D der DSGVO des Vereinigten Königreichs) zur Kenntnis, der wesentliche Änderungen am Rahmen für automatisierte Entscheidungsfindung („ADM“) vorsieht, insbesondere wenn diese auf der Verarbeitung von Daten aus nicht besonderen Kategorien basiert. Bis zur Verabschiedung des DUAA spiegelte Artikel 22 der DSGVO des Vereinigten Königreichs den EU-Datenschutzrahmen wider, der ein generelles Verbot von ADM mit begrenzten Ausnahmen vorsah.

---

<sup>36</sup> Siehe Kapitel 3: Allgemeine Datenschutzgrundsätze, um sicherzustellen, dass das Schutzniveau in einem Drittland, einem Gebiet oder einem oder mehreren bestimmten Sektoren in diesem Drittland oder dieser internationalen Organisation im Wesentlichen dem durch die EU-Rechtsvorschriften gewährleisteten Niveau der Angemessenheitsreferenz in der DSGVO entspricht.

47. Artikel 22B Absatz 1 DSGVO verbietet die Verarbeitung besonderer Kategorien personenbezogener Daten für Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen und – mit bestimmten Ausnahmen – rechtliche oder ähnlich erhebliche Auswirkungen auf die betroffene Person haben (Artikel 22B Absatz 2 Nummer 3 DSGVO des Vereinigten Königreichs, auch wenn die Verarbeitung auf einer Einwilligung, einem Vertrag oder einer gesetzlichen Verpflichtung beruht).
48. Der EDSA stellt fest, dass dieses Verbot nicht gilt, wenn Verantwortliche wichtige Entscheidungen unter Verwendung automatisierter Verfahren auf der Grundlage von Daten treffen, die nicht zu besonderen Kategorien gehören, es sei denn, die Rechtsgrundlage für die Verarbeitung ist ein anerkanntes berechtigtes Interesse gemäß Artikel 6 Absatz 1 Buchstabe ea der DSGVO des Vereinigten Königreichs.
49. Der Schwerpunkt des Gesetzes ändert sich von der Beschränkung der Anwendung von ADM auf die Sicherstellung, dass Garantien für wichtige Entscheidungen vorhanden sind. Zu diesen Garantien gehören i) die Unterrichtung der betroffenen Person über den Entscheidungsprozess, ii) die Möglichkeit, sich zu der Entscheidung zu äußern<sup>37</sup>, iii) die Anfechtung einer solchen Entscheidung sowie iv) die Möglichkeit, dass die betroffene Person das Eingreifen des für die Verarbeitung Verantwortlichen beantragen kann. Der EDSA stellt fest, dass dieser neue Ansatz zwar eine Abweichung vom bisherigen Rechtsrahmen darstellt, Artikel 22C der DSGVO des Vereinigten Königreichs jedoch von den Verantwortlichen verlangt, geeignete Garantien zu implementieren, die ein angemessenes Schutzniveau für die betroffenen Personen gewährleisten.
50. Angesichts des sich rasch wandelnden regulatorischen Umfelds und der Fortschritte bei automatisierten Technologien wie KI fordert der EDSA die Kommission auf, in ihrer endgültigen Angemessenheitsentscheidung die voraussichtlichen praktischen Auswirkungen dieses neuen Ansatzes, der noch nicht in der Praxis erprobt wurde, umfassender zu bewerten und dessen Umsetzung zu überwachen.

#### 2.4.1. AUTOMATISIERTE ENTSCHEIDUNGSFINDUNG UND MENSCHLICHE BETEILIGUNG

51. Der EDSA begrüßt die Klarstellung hinsichtlich der Bedeutung von automatisierten Entscheidungen und menschlicher Beteiligung. In Artikel 22a DSGVO des Vereinigten Königreichs wird klargestellt, dass eine Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung beruht, bedeutet, dass es keine sinnvolle menschliche Beteiligung am Entscheidungsprozess gibt. Die Verantwortlichen müssen auch bewerten, in welchem Umfang Profiling zu einer Entscheidung beiträgt, um festzustellen, ob die menschliche Beteiligung sinnvoll war.
52. Darüber hinaus ist der Secretary of State gemäß Artikel 22D der DSGVO des Vereinigten Königreichs befugt, in Verordnungen festzulegen, ob eine sinnvolle menschliche Beteiligung an der Entscheidungsfindung im Sinne der Verordnung besteht oder nicht. Ebenso erhält der Secretary of State die Befugnis, zu beschreiben, ob die in der Verordnung beschriebene Entscheidung als ähnlich bedeutende Auswirkung auf die betroffenen Personen angesehen wird oder nicht.

---

<sup>37</sup> Das heißt zusätzliche Informationen und Begründungen vorlegen, die noch keine formelle rechtliche Anfechtung darstellen.

53. Der Umfang und der Ermessensspielraum dieser Befugnisse sind unklar. Der EDSA fordert die Kommission daher auf, diese dem Secretary of State neu übertragenen Befugnisse zu analysieren und alle diesbezüglichen Entwicklungen zu verfolgen. Andererseits sind die zusätzlichen Befugnisse des Secretary of State in Bezug auf die nach Artikel 22c der DSGVO des Vereinigten Königreichs erforderlichen Garantien eine begrüßenswerte Änderung, da sie die bereits erforderlichen Garantien ergänzen und/oder ergänzen sowie festlegen werden, was in Bezug auf die Garantien unzureichend ist.

### 3. VERFAHRENS- UND DURCHSETZUNGSMECHANISMUS

#### 3.1. AUFSICHT UND DURCHSETZUNG

##### 3.1.1. UNABHÄNGIGE AUFSICHT

54. Der EDSA stellt fest, dass mit dem Inkrafttreten des DUA Act<sup>38</sup> der Datenschutzbeauftragte (ICO), der zuvor als alleinige Aktiengesellschaft strukturiert war, durch die Einführung eines Organs (einer Aufsichtsbehörde), nämlich der Informationskommission (IC) gemäß Artikel 148 und Anhang 12A der DSB 2018 in eine neue Struktur umgewandelt wird.
55. Der EDSA stellt fest, dass die Umstrukturierung einer Behörde von einer Einzelperson zu einem Gremium an sich keinen Einfluss auf die Unabhängigkeit der Behörde und ihre wirksame Durchsetzung hat. Andere Elemente wie die Regeln für die Ernennung und Entlassung sollten ebenfalls berücksichtigt werden. In diesem Zusammenhang begrüßt der EDSA, dass nur Seine Majestät den Vorsitzenden des IC auf Empfehlung beider Häuser des Parlaments des Vereinigten Königreichs im Falle eines schwerwiegenden Fehlverhaltens seines Amtes entheben kann.
56. Detaillierte Vorschriften über die Arbeit und die Funktionsweise der neuen Interoperabilitätsvereinbarung sind in Anhang 12A des DPA 2018 enthalten. Dieser regelt unter anderem die strukturellen und organisatorischen Rahmenbedingungen des IC, die Anforderungen für die Ernennung seiner geschäftsführenden und nicht geschäftsführenden Mitglieder sowie anderer Mitarbeiter (Angestellte und ein externes Komitee) und enthält Bestimmungen zur Amtszeit, Vergütung, Kontenführung und Entlassung. Die Nummern 5 und 6 von Anhang 12A<sup>39</sup> enthalten Regeln und Garantien, die bei der Ernennung nicht geschäftsführender Mitglieder zu beachten sind und die für die Einrichtung und Unabhängigkeit des Gremiums relevant sein könnten (z. B. Auswahl in Bezug auf Verdienste und Interessenkonflikte).
57. Der EDSA stellt fest, dass der Beschlussentwurf keine Einzelheiten zu den Änderungen der Arbeitsweise und Funktionsweise der neuen Datenschutzbehörde enthält. Des Weiteren gibt es keine Einzelheiten zum Verfahren für die Ernennung und Abberufung von geschäftsführenden und nicht geschäftsführenden Mitgliedern. Da diese Elemente für die Bewertung des Aufsichtsmechanismus relevant sind, fordert der EDSA die Kommission auf, die Änderungen und die einschlägige Bewertung genauer zu beschreiben, insbesondere in Bezug auf die Struktur und Organisation des Prüfungsausschusses, die Ernennung und Entlassung seiner Mitglieder, einschließlich seiner nicht geschäftsführenden Mitglieder.

---

<sup>38</sup> Siehe Teil 6 „Die Informationskommission“, DUAA Nr. 117, S. 133 ff.

<sup>39</sup> Siehe Anhang 12A des DPA 2018.

58. In Bezug auf die Unabhängigkeit des IC stellt der EDSA fest, dass gemäß Abschnitt 6 von Anhang 12A DPA 2018 Interessenkonflikte die Ernennung durch den Secretary of State zum Vorsitzenden oder zum nicht geschäftsführenden Mitglied des IC verhindern können. Bei der Formulierung des Begriffs „Interessenkonflikt“ wird in Abschnitt 6 Absatz 5 auf „ein finanzielles oder sonstiges Interesse, das die Wahrnehmung der Funktion der Person als Mitglied der Kommission beeinträchtigen könnte“, Bezug genommen. Was die Unabhängigkeit der IC-Mitglieder betrifft, so können solche „sonstigen Interessen“, z. B. besondere wirtschaftliche Nähe und/oder Geschäftsbeziehungen, auch auf Interessenkonflikte hindeuten und sollten beim Ernennungsverfahren für IC-Mitglieder berücksichtigt werden. Der EDSA fordert die Kommission daher auf, zu überwachen, dass die Beschränkungen in der Praxis auch angewendet werden.
59. In Bezug auf die aktualisierten Ziele, die die Interoperabilitätskomponenten bei der Wahrnehmung ihrer Aufgaben und der Ausarbeitung ihrer Strategie berücksichtigen muss, wie unter anderem die Förderung von Innovation und Wettbewerb (Abschnitt 120B des Datenschutzgesetzes 2018), erinnert die Kommission daran, dass „auch das EU-Datenschutzrecht den Schutz personenbezogener Daten mit mehreren anderen Grundrechten und Zielen in Einklang bringt“, und zitiert die Erwägungsgründe 2 und 4 sowie Artikel 23 DSGVO. Der EDSA erkennt an, dass der Datenschutz kein absolutes Recht ist und im Einklang mit dem Grundsatz der Verhältnismäßigkeit gegen andere Grundrechte und Ziele abgewogen werden muss. Der EDSA stellt jedoch fest, dass sich die Erwägungsgründe 2 und 4 DSGVO sowie Artikel 23 DSGVO von einer Rechtsvorschrift unterscheiden, die die Datenschutzbehörden ausdrücklich verpflichtet, eine Reihe von Zielen bei der Wahrnehmung ihrer Aufgaben zu berücksichtigen. Aus Gründen der Klarheit fordert der EDSA die Kommission auf, diesen Erwägungsgrund umzuformulieren, um nicht den Eindruck zu erwecken, dass die Erwägungsgründe 2 und 4 sowie Artikel 23 DSGVO dieselbe Bedeutung haben wie Abschnitt 120B des Datenschutzgesetzes 2018, und zu überwachen, dass die Umsetzung dieser aktualisierten Ziele in der Praxis nicht zu einem übermäßigen Ungleichgewicht zulasten des Rechts auf personenbezogene Daten führt, das das Schutzniveau für personenbezogene Daten untergraben würde.

### 3.1.2. DURCHSETZUNG, EINSCHLIEßLICH SANKTIONEN

60. Der EDSA begrüßt, dass die Bestimmung aus dem früheren Gesetzentwurf zur Reform des britischen Datenschutzrahmens (Data Protection and Digital Information Bill „DPDI Bill“<sup>40</sup>), wonach das ICO bei der Ausübung ihrer Befugnisse die Stellungnahme des Secretary of State berücksichtigen muss, nicht mehr im neuen Datenschutzrahmen enthalten ist.
61. Der EDSA bewertet es ebenfalls als positiv, dass das ICO seit der Verabschiedung der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich zahlreiche hilfreiche Verhaltenskodizes, Leitlinien, Stellungnahmen und andere Leitfäden für die betroffenen Parteien veröffentlicht hat.
62. Wie in seiner Stellungnahme 14/2021<sup>41</sup> betont der EDSA, dass ein wirksamer Aufsichtsmechanismus, der eine unabhängige Untersuchung von Beschwerden ermöglicht, sowie wirksame administrative und gerichtliche Rechtsbehelfsverfahren Schlüsselemente für die Beurteilung sind, ob ein Datenschutzsystem ein angemessenes Schutzniveau bietet. Darüber hinaus spielt das Vorhandensein wirksamer Sanktionen eine wichtige Rolle bei der Gewährleistung der Einhaltung von Regeln.

---

<sup>40</sup> Siehe Abschnitt 32 (neuer Artikel 120 E, F, G und H des Gesetzes über Datenschutz und digitale Informationen).

<sup>41</sup> Siehe Stellungnahme 14/2021 des EDSA, Absätze 112 bis 114.

63. Vor diesem Hintergrund weist der EDSA die Kommission auf die vom ICO am 22. August veröffentlichte öffentliche Konsultation zu seinen Vorschlägen für die Bearbeitung von Beschwerden<sup>42</sup> hin, die erst nach Erlass des Beschlussentwurfs der Kommission eingeleitet wurde. In seiner Einleitung<sup>43</sup> zu den Vorschlägen im Rahmen der öffentlichen Konsultation erklärt das ICO, es gehe davon aus, dass nach Inkrafttreten des DUAA mehr Beschwerden von den Organisationen selbst ohne Beteiligung des ICO beigelegt würden. Hintergrund dieser Bewertung durch das ICO ist, dass im DUAA neue Anforderungen an Organisationen festgelegt sind, die ein Beschwerdeverfahren speziell für Datenschutzfragen einführen müssen. Gemäß Artikel 164A DSB 2018<sup>44</sup> müssen für die Verarbeitung Verantwortliche Maßnahmen ergreifen, um Personen zu helfen, die Beschwerden über die Verwendung ihrer personenbezogenen Daten einreichen möchten. Beispielsweise müssen sie ein Beschwerdeformular bereitstellen, das elektronisch und auf andere Weise ausgefüllt werden kann, sie müssen Beschwerden innerhalb von 30 Tagen bestätigen und „ohne unnötige Verzögerung“ geeignete Maßnahmen ergreifen, um auf die Beschwerde zu reagieren und den Beschwerdeführer über das Ergebnis der Beschwerde zu informieren. Wenn Beschwerden tatsächlich von des ICO bearbeitet werden müssen, sollten die zur öffentlichen Konsultation vorgelegten Vorschläge die Grundlage für die Bearbeitung der Beschwerden durch das ICO bilden. In diesem Zusammenhang schlägt das ICO eine Art Triage-System vor, wonach Beschwerden mit unterschiedlichen Prioritäten und Ergebnissen bearbeitet werden sollen. Dies dürfte es dem ICO als strategischer Regulierungsbehörde ermöglichen, seine Ressourcen auf die wichtigsten Risiken zu konzentrieren und systemische Probleme zu einem früheren Zeitpunkt zu ermitteln. In dem Vorschlag des ICO sind Kriterien in einer nicht erschöpfenden Liste aufgeführt, die die Wahrscheinlichkeit, dass eine Beschwerde weiter verfolgt wird, erhöhen oder verringern können.<sup>45</sup>
64. Die in Absatz 57 beschriebenen Änderungen können zu einer Änderung der Vorgehensweise des IC bei der Bearbeitung von Beschwerden führen. Aufgrund der Einleitung der öffentlichen Konsultation nach Veröffentlichung des Beschlussentwurfs der Kommission sind diese Änderungen noch nicht im Beschlussentwurf berücksichtigt worden.
65. Der EDSA fordert die Kommission auf, dieses Element in ihre Bewertung einzubeziehen und insbesondere die Ergebnisse der öffentlichen Konsultation des ICO weiterzuverfolgen. Darüber hinaus fordert der EDSA die Kommission auf, die künftige Bearbeitung von Beschwerden durch die Interoperabilitätskomponente genau zu überwachen, um sicherzustellen, dass weiterhin ein gleichwertiges Schutzniveau gewährleistet ist.

---

<sup>42</sup> Siehe die Konsultation des ICO zum Entwurf von Änderungen an der Art und Weise, wie wir Datenschutzbeschwerden bearbeiten: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/08/ico-consultation-on-draft-changes-to-how-we-handle-data-protection-complaints/>; <https://ico.org.uk/media2/nrljbhr2/proposed-dpt-framework-20250822.pdf>

<sup>43</sup> Siehe Fußnote 41.

<sup>44</sup> Siehe Artikel 164A DPA 2018.

<sup>45</sup> Siehe Fußnote 41.

66. Der EDSA stellt ferner fest, dass die dem Secretary of State durch das DUA-Gesetz übertragenen weitreichenden Regulierungsbefugnisse, einschließlich der Befugnis zum Erlass von Rechtsvorschriften, Auswirkungen auf die Arbeit des IC und seiner Mitglieder haben könnten. Der EDSA verweist beispielsweise auf die Notwendigkeit, dass der IC den Secretary of State in Bezug auf einige seiner Aufgaben konsultieren muss. Insbesondere sieht Artikel 124A DPA 2018<sup>46</sup> vor, dass der IC geeignete Verhaltenskodizes mit Leitlinien für die ordnungsgemäße Verarbeitung personenbezogener Daten festlegen muss, wenn dies aufgrund einer vom Secretary of State erlassenen Verordnung erforderlich ist. Der IC ist verpflichtet, vor der Änderung oder Ausarbeitung solcher Kodizes den Secretary of State zu konsultieren.
67. Angesichts der Bedeutung der Unabhängigkeit des IC fordert der EDSA die Kommission auf, diese neuen Befugnisse des Secretary of State genau zu überwachen, insbesondere ihre praktischen Auswirkungen auf die Arbeit des IC.
68. Wie bereits vom EDSA in seiner Stellungnahme 14/2021 betont, verfügt das ICO über die erforderlichen Befugnisse, die weitgehend den Befugnissen der Aufsichtsbehörden der EU-Mitgliedstaaten gemäß Artikel 58 DSGVO entsprechen. Gleichzeitig spielt, wie bereits vom EDSA hervorgehoben, das Vorhandensein wirksamer Sanktionen eine wichtige Rolle bei der Gewährleistung der Einhaltung der Vorschriften. Der EDSA fordert die Kommission auf, im Rahmen des Datenschutzrahmens des Vereinigten Königreichs eine detailliertere Bewertung vorzunehmen und die Anwendung der Abhilfebefugnisse, die Wirksamkeit der Sanktionen und der Rechtsbehelfe für betroffene Parteien zu überwachen<sup>47</sup>.

#### 4. ZUGANG ZU PERSONENBEZOGENEN DATEN UND VERWENDUNG VON PERSONENBEZOGENEN DATEN, DIE AUS DER EUROPÄISCHEN UNION AN BEHÖRDEN IM VEREINIGTEN KÖNIGREICH ÜBERMITTELT WERDEN

69. Der Beschlussentwurf konzentriert sich auf Entwicklungen, die für die Bewertung des Schutzniveaus im Vereinigten Königreich seit der Verabschiedung der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich relevant sind, die für diejenigen Aspekte des britischen Datenschutzrahmens, die nicht geändert oder betroffen sind, weiterhin gültig bleibt. Dieser allgemeine Ansatz umfasst auch die Analyse der Kommission zum Zugang zu personenbezogenen Daten und zu deren Nutzung durch Behörden im Vereinigten Königreich. Dieser spezifische Aspekt wird oft als „Zugriff durch Behörden“ bezeichnet und ist eines der in Artikel 45 Absatz 2 Buchstabe a DSGVO aufgeführten Elemente, die von der Kommission bei der Feststellung, ob das Schutzniveau im Wesentlichen gleichwertig ist, zu berücksichtigen sind.

---

<sup>46</sup> Praxiskodex für die Verarbeitung personenbezogener Daten.

<sup>47</sup> Vgl. EDSA, Stellungnahme 14/2021, Randnummer 113.

70. Vor diesem Hintergrund werden in den folgenden Abschnitten eine Reihe spezifischer Punkte behandelt, die in dem Beschlussentwurf, der derzeit geprüft wird, angesprochen werden und die in Bezug auf personenbezogene Daten relevant sind, die im Rahmen des Angemessenheitsbeschlusses des Vereinigten Königreichs aus dem EWR übermittelt und von Behörden im Vereinigten Königreich abgerufen und verarbeitet werden, einschließlich Weiterübermittlungen. Die Analyse und die Bemerkungen des EDSA in der Stellungnahme 14/2021 behalten<sup>48</sup> im Allgemeinen ihre Gültigkeit.

#### 4.1. ZUGRIFF UND NUTZUNG DURCH BEHÖRDEN DES VEREINIGTEN KÖNIGREICHS ZU STRAFVERFOLGUNGSZWECKEN

71. Der Datenschutzrahmen, der den Zugang und die Nutzung durch Behörden des Vereinigten Königreichs zu Strafverfolgungszwecken regelt, wurde seit der im vorherigen Angemessenheitsbeschluss für das Vereinigte Königreich vorgenommenen Bewertung durch die Kommission Gesetzesänderungen unterzogen. Dazu gehören das Gesetz über die nationale Sicherheit 2023, das Gesetz zur Änderung der Ermittlungsbefugnisse von 2024 und die Einführung des DUAA. Letzteres wird auch im Entwurf einer Entscheidung der Kommission zur Änderung des Durchführungsbeschlusses (EU) 21/1773 sowie in der entsprechenden Stellungnahme des EDSA auf der Grundlage von Artikel 51 Absatz 1 Buchstabe g der Strafverfolgungsrichtlinie behandelt.

##### 4.1.1. RECHTSGRUNDLAGEN UND ANWENDBARE GARANTIE

###### 4.1.1.1. ERMITTLUNGSBEFUGNISSE FÜR STRAFVERFOLGUNGSZWECKE

72. In den Erwägungsgründen 81 bis 85 des Beschlussentwurfs skizziert die Kommission die Änderungen am Investigative Powers Act 2016 („IPA 2016“), wie sie durch den Investigative Powers Amendment Act 2024 (Gesetz über die Untersuchungsbefugnisse 2016) eingeführt wurden, soweit sie die Verarbeitung zu Strafverfolgungszwecken betreffen.<sup>49</sup> Insgesamt liefert die Kommission detaillierte Informationen. In Bezug auf eine bestimmte Änderung ist der EDSA jedoch der Ansicht, dass der Beschlussentwurf einer weiteren Klarstellung bedürfte.

---

<sup>48</sup> Siehe Stellungnahme 14/2021 des EDSA.

<sup>49</sup> Die Kommission weist darauf hin, dass bestimmte Strafverfolgungsbehörden, wie in den Erwägungsgründen 139 bis 141 des Durchführungsbeschlusses (EU) 2021/1772 beschrieben, auch gezielte Ermittlungsbefugnisse im Rahmen des IPA 2016 nutzen können, um schwere Straftaten zu verhüten oder aufzudecken. Änderungen dieser Bestimmungen betreffen daher nicht nur den Zugriff auf Daten zu Zwecken der nationalen Sicherheit, sondern auch zu Strafverfolgungszwecken.

73. Mit dem Gesetz zur Änderung der Untersuchungsbefugnisse 2024 wurde die Definition des Begriffs „Telekommunikationsbetreiber“ überarbeitet, d. h. die potenziellen Adressaten eines Aufbewahrungsbescheids im Rahmen des IPA 2016.<sup>50</sup> Die geänderte Definition umfasst nun jede Person, die „ein Telekommunikationssystem kontrolliert oder bereitstellt, das i) sich nicht (ganz oder teilweise) im Vereinigten Königreich befindet oder von dort aus kontrolliert wird und ii) von einer anderen Person genutzt wird, um Personen im Vereinigten Königreich Telekommunikationsdienste anzubieten oder bereitzustellen“. Die Kommission verweist zwar auf die Erläuterungen des Investigatory Powers Amendment Act 2024 (Gesetz zur Änderung der Ermittlungsbefugnisse von 2024), in denen es heißt, dass Section 261(10)(c) „zusätzliche Klarstellungen enthält, um sicherzustellen, dass große Unternehmen mit komplexen Unternehmensstrukturen in ihrer Gesamtheit durch das IPA 2016 abgedeckt werden“, und dass „die Änderung [...] nicht darauf abzielt, weitere Unternehmen in den Anwendungsbereich zu bringen“, die Auswirkungen dieser Änderung jedoch unklar bleiben, z. B. ob sie den Umfang der personenbezogenen Daten, die möglicherweise Gegenstand einer Speicherfrist sind, erweitern würde. Der EDSA fordert die Kommission daher auf, sich eingehender mit den Auswirkungen dieser Änderung zu befassen und diesen Aspekt insbesondere im Lichte der Grundsätze der Notwendigkeit und der Verhältnismäßigkeit zu überwachen.

#### 4.1.1.2. AUSNAHMEN AUS GRÜNDEN DER NATIONALEN SICHERHEIT FÜR STRAFVERFOLGUNGSBEHÖRDEN

74. In Abschnitt 88 des DUAA werden die bestehenden Ausnahmen in Bezug auf die nationale Sicherheit im Rahmen der Strafverfolgung aktualisiert, um sie an die Ausnahmen anzupassen, die in der DSGVO des Vereinigten Königreichs und den Regelungen für Nachrichtendienste vorgesehen sind.<sup>51</sup> Zwar sind die Strafverfolgungsbehörden bereits in der Lage, bestimmte Verpflichtungen aus Gründen des Schutzes der nationalen Sicherheit – z. B. in Bezug auf die Rechte betroffener Personen – einzuschränken, doch werden in Abschnitt 78A des Datenschutzgesetzes von 2018<sup>52</sup> auch die meisten Datenschutzgrundsätze<sup>53</sup> und bestimmte Anforderungen an die internationale Datenübermittlung<sup>54</sup> als Bestimmungen aufgenommen, die möglicherweise nicht angewendet werden, wenn dies zum Schutz der nationalen Sicherheit erforderlich ist. Darüber hinaus<sup>55</sup> können einige der Einreisebefugnisse des Information Commissioner zur Durchführung von Inspektionen und zur Ergreifung von Durchsetzungsmaßnahmen unter solchen Umständen unangewendet bleiben.

---

<sup>50</sup> Abschnitt 261(10)(c) des IPA 2016 in der durch Abschnitt 19 der Investigative Powers Amendment Act 2024 (Gesetz zur Änderung der Untersuchungsbefugnisse 2024) eingefügten Fassung.

<sup>51</sup> Siehe auch Informationsblatt des Secretary of State für Wissenschaft, Innovation und Technologie zum Gesetz über Daten (Nutzung und Zugang): DSGVO des Vereinigten Königreichs und DPA, veröffentlicht am 27. Juni 2025, S. 14 <https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa>.

<sup>52</sup> Die DUAA wird in mehreren Phasen schrittweise eingeführt. Die wichtigsten Änderungen der Datenschutzgesetzgebung in Teil 5 des Gesetzes über Daten (Verwendung und Zugriff) treten im Rahmen von Stufe 3 etwa sechs Monate nach der königlichen Zustimmung in Kraft, <https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement>.

<sup>53</sup> Siehe Abschnitt 78A Absatz 1, Absatz 2 Buchstabe a und Absatz 3 des Datenschutzgesetzes von 2018 in der durch Abschnitt 88 DUAA eingeführten Fassung.

<sup>54</sup> Siehe Abschnitt 78A Absatz 1, Absatz 2 Buchstabe d, Absatz 4 des Datenschutzgesetzes von 2018 in der durch Abschnitt 88 DUAA eingeführten Fassung.

<sup>55</sup> Siehe Abschnitt 78A Absatz 1, Absatz 2 Buchstaben e, f und g des Datenschutzgesetzes von 2018, eingeführt durch Abschnitt 88 DUAA.

75. Diese Änderungen werden weder im Entwurf des Angemessenheitsbeschlusses nach Artikel 45 der DSGVO noch im Entwurf des Angemessenheitsbeschlusses nach Artikel 36 der Strafverfolgungsrichtlinie erwähnt. Der EDSA hält es jedoch für unerlässlich, diese erweiterten Ausnahmen anhand der Grundsätze der Notwendigkeit und Verhältnismäßigkeit zu prüfen. In diesem Zusammenhang erinnert der EDSA an die zweite der vier sogenannten „europäischen Grundgarantien“: Jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten muss deren Wesen achten und darf vorbehaltlich des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie notwendig ist und tatsächlich den von der Union anerkannten Zielen von allgemeinem Interesse oder der Notwendigkeit, die Rechte und Freiheiten anderer zu schützen, entspricht.<sup>56</sup> Der EDSA ist besorgt über die Ausnahmen von wichtigen Datenschutzgrundsätzen, Anforderungen an internationale Übermittlungen und die Befugnisse des Datenschutzbeauftragten.
76. Nach der überarbeiteten Regelung können fünf der sechs Datenschutzgrundsätze nicht angewandt werden, wenn dies zum Schutz der nationalen Sicherheit erforderlich ist.<sup>57</sup> Diese Grundsätze besagen unter anderem, dass der Strafverfolgungszweck, zu dem personenbezogene Daten erhoben werden, genau, eindeutig und rechtmäßig sein muss und dass personenbezogene Daten dem Zweck angemessen, erheblich und in Bezug auf diesen Zweck nicht unverhältnismäßig sein müssen. Sie legen auch fest, dass personenbezogene Daten korrekt sein müssen und nur so lange wie nötig aufbewahrt werden dürfen. Wie bereits erwähnt, umfassen die künftigen Ausnahmen zusätzlich einige der Anforderungen an die internationale Übermittlung, wie die sogenannte zweite Bedingung für internationale Übermittlungen gemäß Abschnitt 73 Absatz 3 des Datenschutzgesetzes von 2018. Diese Bedingung setzt voraus, dass Übermittlungen entweder auf Angemessenheitsvorschriften, geeigneten Garantien oder – falls keines davon zutrifft – auf besonderen Umständen beruhen. Die Ausnahmen betreffen auch die Befugnisse des Datenschutzbeauftragten, z. B. die Befugnis, Informationen und Durchsetzungsmitteilungen herauszugeben.<sup>58</sup>
77. Der EDSA stellt fest, dass die Ausnahmen zwar eindeutig von der Richtlinie zum Datenschutz bei der Strafverfolgung abweichen, aber den in Artikel 11 des modernisierten Übereinkommens 108 des Europarats („Übereinkommen 108+“)<sup>59</sup> vorgesehenen Ausnahmen und Beschränkungen der nationalen Sicherheit sehr ähnlich sind, das vom Vereinigten Königreich am 10. Oktober 2018 unterzeichnet wurde, zum Zeitpunkt dieser Stellungnahme aber noch nicht vom Vereinigten Königreich ratifiziert wurde oder noch nicht in Kraft getreten ist.<sup>60</sup> In diesem Zusammenhang erinnert der EDSA daran, dass der Beratende Ausschuss des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (T-PD) kürzlich Leitlinien zu den

---

<sup>56</sup> Siehe Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, angenommen am 10. November 2020, S. 10.

<sup>57</sup> Gemäß Abschnitt 78A(2) und (3) des Datenschutzgesetzes von 2018 findet Teil 3 Kapitel 2 dieses Gesetzes keine Anwendung, wenn dies zum Zwecke der Wahrung der nationalen Sicherheit erforderlich ist, mit Ausnahme von (a) Abschnitt 35(1) (dem ersten Datenschutzgrundsatz), soweit dieser die Rechtmäßigkeit der Verarbeitung personenbezogener Daten vorschreibt; (b) Abschnitt 35(2) bis (5) (Rechtmäßigkeit der Verarbeitung und Beschränkungen für die Verarbeitung sensibler Daten); (c) Abschnitt 42 (Schutzmaßnahmen: Verarbeitung sensibler Daten); und (d) Anhang 8 (Bedingungen für die Verarbeitung sensibler Daten).

<sup>58</sup> In Informationsmitteilungen wird von einem Verantwortlichen oder Auftragsverarbeiter verlangt, dem Kommissionsmitglied Informationen zur Verfügung zu stellen, die für die Wahrnehmung der Aufgaben des Kommissionsmitglieds nach vernünftigem Ermessen erforderlich sind. Durch Vollstreckungsbescheide ist der Kommissar befugt, von einer Person bestimmte Maßnahmen zu verlangen (oder ihr bestimmte Maßnahmen zu untersagen), wenn er zu der Überzeugung gelangt ist, dass diese Person bestimmte Datenschutzverpflichtungen nicht erfüllt.

<sup>59</sup> Siehe Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 223)

<sup>60</sup> <https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223>

allgemeinen Grundsätzen von Artikel 11 des modernisierten Übereinkommens 108 veröffentlicht hat<sup>61</sup>.

78. In seinen Leitlinien betont der Europarat ausdrücklich, dass unter anderem für die Grundsätze der Verhältnismäßigkeit und der Rechtmäßigkeit des Zwecks der Verarbeitung keine Ausnahmen gelten. Das bedeutet, dass die Verhältnismäßigkeit der Datenverarbeitung gewährleistet sein muss, ebenso wie die Anforderungen an die Verarbeitung personenbezogener Daten für einen legitimen Zweck. In Übereinstimmung mit den Leitlinien der T-PD bleibt der EDSA besonders wachsam hinsichtlich jeglicher Ausnahmen vom Grundsatz der Verhältnismäßigkeit sowie von der Anforderung, personenbezogene Daten für einen legitimen Zweck zu verarbeiten. Ebenso sollten nach Ansicht des EDSA Ausnahmen von den Befugnissen der Aufsichtsbehörde mit Vorsicht angegangen werden. Während spezifische Anforderungen für Überwachungstätigkeiten – wie Sicherheitsüberprüfungen – im Zusammenhang mit der Verarbeitung von Daten im Bereich der nationalen Sicherheit angemessen sein können, ist es unerlässlich, eine wirksame Aufsicht sicherzustellen, um das Entstehen eines Überwachungsvakuums zu verhindern. In diesem Sinne ist in Artikel 11 Absatz 3 des Übereinkommens 108+ festgelegt, dass Ausnahmen von Artikel 15<sup>62</sup> des Übereinkommens „unbeschadet des Erfordernisses gelten, dass Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und Verteidigung einer unabhängigen und wirksamen Überprüfung und Überwachung nach den innerstaatlichen Rechtsvorschriften der Vertragsparteien des Übereinkommens unterliegen“. Darüber hinaus sollten alle Ausnahmen so restriktiv wie möglich ausgelegt werden. Die Tatsache, dass personenbezogene Daten zu Zwecken der nationalen Sicherheit verarbeitet werden, sollte für sich genommen nicht ausreichen, um eine Ausnahme geltend zu machen. Es sollte klar sein, dass eine Ausnahme von der Datenschutzregelung von Fall zu Fall und nur dann gewährt werden muss, wenn dies erforderlich und verhältnismäßig ist.<sup>63</sup>
79. Da der Entwurf der Angemessenheitsbeschlüsse diesen Punkt nicht behandelt, fordert der EDSA die Kommission auf, ihre Bewertung im Beschlussentwurf zu ergänzen und insbesondere die praktische Anwendung der Ausnahmeregelungen für Strafverfolgungsbehörden im Bereich der nationalen Sicherheit zu überwachen.

---

<sup>61</sup> <https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/1680b6c146>

<sup>62</sup> Siehe Artikel 15 des Übereinkommens 108+, in dem festgelegt ist, wie die Vertragsparteien des Übereinkommens durch die Einrichtung einer oder mehrerer Aufsichtsbehörden die Einhaltung der Bestimmungen des Übereinkommens sicherstellen sollen.

<sup>63</sup> Siehe auch Artikel 11 des Übereinkommens 108+, in dem festgelegt ist, dass Ausnahmen gesetzlich vorgesehen sein müssen, den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen müssen. Nach den Leitlinien der TP-D zu den allgemeinen Grundsätzen des Artikels 11 bedeutet dies, dass eine Abwägung der Interessen zwischen der Notwendigkeit, Ausnahmen von bestimmten Bestimmungen des Übereinkommens vorzusehen, und der Achtung der Menschenrechte und Grundfreiheiten des Einzelnen vorgenommen und gerechtfertigt werden muss.

#### 4.1.2. GEMEINSAME KONTROVERSEN ZWISCHEN NACHRICHTENDIENSTEN UND STRAFVERFOLGUNGSBEHÖRDEN DES VEREINIGTEN KÖNIGREICHS

80. Auf der Grundlage der Änderungen durch das DUAA können Verarbeitungstätigkeiten, die von für die Strafverfolgung zuständigen Behörden durchgeführt werden, unter bestimmten Umständen unter die Vorschriften fallen, die normalerweise für die Verarbeitung personenbezogener Daten durch nationale Sicherheitsbehörden gelten.<sup>64</sup> Mit anderen Worten: Vorbehaltlich der in Abschnitt 89 des DUAA festgelegten Bedingungen wird die in Teil 4 des Datenschutzgesetzes von 2018 festgelegte Datenschutzregelung für die Verarbeitung von Daten im Bereich der nationalen Sicherheit auf die Datenverarbeitung durch Strafverfolgungsbehörden ausgeweitet.
81. Die Kommission betont, dass die Bedingungen in Abschnitt 89 des DUAA strenge Schutzvorkehrungen vorsehen: Eine zuständige Behörde muss in den vom Secretary of State erlassenen Vorschriften als „qualifizierte zuständige Behörde“ bezeichnet werden, der darüber hinaus eine bestimmte Verarbeitungstätigkeit, die von der qualifizierten zuständigen Behörde als gemeinsamer Verantwortlicher zusammen mit mindestens einem Nachrichtendienst zum Zwecke der Wahrung der nationalen Sicherheit durchgeführt wird, benennen muss.<sup>65</sup>
82. Der EDSA erkennt zwar an, dass diese Schutzmaßnahmen erhebliche Einschränkungen mit sich bringen, fordert die Kommission jedoch auf, die praktische Umsetzung dieser Vorschriften zu überwachen. Insbesondere sollte darauf geachtet werden, dass Teil 4 des Datenschutzgesetzes von 2018 strikt auf Verarbeitungsvorgänge für Zwecke der nationalen Sicherheit angewandt wird, ohne auf andere Kontexte ausgedehnt zu werden. Obwohl den Staaten in Fragen der nationalen Sicherheit ein weiter Ermessensspielraum eingeräumt wird, wie auch vom EGMR<sup>66</sup> in der Rechtssache anerkannt wurde, vertritt der EDSA die Auffassung, dass Gefahren für die nationale Sicherheit sich aufgrund ihrer Art, ihrer Schwere und der besonderen Umstände von allgemeinen Risiken für die öffentliche Sicherheit oder von schweren Straftaten unterscheiden müssen. Nur in solchen Fällen ist die Tätigkeit der Strafverfolgungsbehörden im Rahmen der Datenschutzregelung für Nachrichtendienste mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit vereinbar.<sup>67</sup> Darüber hinaus hält es der EDSA für erforderlich, zu überwachen, ob die zuständigen Behörden in der Praxis in der Lage sind, eine klare Unterscheidung zwischen verschiedenen Verarbeitungszwecken zu treffen, um den entsprechenden Rechtsrahmen entsprechend einzuhalten.

#### 4.1.3. DAS RECHT AUF AUSKUNFT

83. Die DUAA legt fest, dass betroffene Personen nur dann Anspruch auf Zugang zu den relevanten Informationen haben, wenn der Verantwortliche diese auf der Grundlage einer angemessenen und verhältnismäßigen Suche bereitstellen kann. Diese Änderung wird sowohl im Bereich der Strafverfolgung als auch im Bereich der nationalen Sicherheit eingeführt.<sup>68</sup>

---

<sup>64</sup> Siehe Erwägungsgrund 72 des Beschlussentwurfs.

<sup>65</sup> Siehe Erwägungsgrund 73 des Beschlussentwurfs.

<sup>66</sup> Siehe EGMR, Big Brother Watch und andere / Vereinigtes Königreich, 25. Mai 2025, Rn. 350.

<sup>67</sup> Aus der Rechtsprechung des EuGH ergibt sich bei der Anwendung der Erforderlichkeits- und Verhältnismäßigkeitsprüfung auf die Rechtsvorschriften der Mitgliedstaaten, die die Speicherung personenbezogener Daten und den Zugang zu diesen Daten durch Behörden ermöglichen, dass legitime Ziele wie die nationale Sicherheit oder die Bekämpfung schwerer Straftaten unterschiedlich sind und daher verschiedene Arten von Eingriffen rechtfertigen könnten. Siehe EuGH, verbundene Rechtssachen C-51/18, C-512/18 und C-520/18, La Quadrature du Net u. a., 6. Oktober 2020.

<sup>68</sup> Siehe § 78 Absätze 3 und 4 des Data (Use and Access) Act, mit dem die §§ 45 und 94 des Datenschutzgesetzes 2018 geändert werden.

84. Die Kommission erklärt dies als Klarstellung im Einklang mit etablierten Standards, die in der innerstaatlichen Rechtsprechung entwickelt wurden und die auch die Interessen der betroffenen Person berücksichtigen. Dennoch hätte der EDSA detailliertere Informationen darüber begrüßt, wie der Begriff „angemessene und verhältnismäßige Suche“ ausgelegt wird, auch da Artikel 14 der Richtlinie zum Datenschutz bei der Strafverfolgung kein solches Element enthält. Der EDSA erkennt an, dass es tatsächlich Szenarien geben kann, in denen die Bemühungen eines Verantwortlichen, Informationen über die betroffene Person zu identifizieren und zu lokalisieren, als unangemessen und unverhältnismäßig angesehen werden könnten, ohne dass dadurch die wesentliche Gleichwertigkeit beeinträchtigt wird.<sup>69</sup> Der EDSA verweist auf die Analyse und Schlussfolgerung in Absatz 34 dieser Stellungnahme, die gleichermaßen für die Strafverfolgung und die nationale Sicherheit relevant sind.

#### 4.1.4. WEITERGABEN

##### 4.1.4.1. EIN NEUER DATENSCHUTZ-TEST

85. Wenn eine zuständige Behörde beabsichtigt, personenbezogene Daten, die gemäß Teil 3 des DPA 2018 verarbeitet wurden, an Strafverfolgungsbehörden eines Drittlandes weiterzugeben, gelten besondere Anforderungen. Solche Übermittlungen können insbesondere dann erfolgen, wenn sie durch Verordnungen des Secretary of State genehmigt wurden oder, falls solche Verordnungen nicht bestehen, auf geeigneten Garantien beruhen. Wenn eine Übermittlung weder auf einer Verordnung noch auf angemessenen Garantien beruhen kann, ist sie nur unter bestimmten, genau festgelegten Umständen möglich, die als „besondere Umstände“ bezeichnet werden und den Situationen und Bedingungen entsprechen, die gemäß Artikel 38 der Datenschutz-Grundverordnung als „Ausnahmen“ gelten.
86. Während die Kommission feststellt, dass „die Regelung für die internationale Übermittlung personenbezogener Daten aus dem Vereinigten Königreich nach wie vor sehr nahe an den Vorschriften in Kapitel V der Richtlinie (EU) 2016/680 liegt“, wird im Beschlussentwurf auch darauf hingewiesen, dass der rechtliche Standard für Verordnungen zur Genehmigung von Übermittlungen, die in dem früheren Abschnitt 74A des Datenschutzgesetzes 2018 als Angemessenheitsverordnungen bezeichnet wurden, sowie geeignete Garantien umformuliert wurden. Anstatt sich auf ein angemessenes Schutzniveau zu beziehen, verlangt der neue „Datenschutz-Test“ gemäß Abschnitt 74AB des Datenschutzgesetzes von 2028, dass das Schutzniveau für betroffene Personen in Empfänger-Drittländern oder internationalen Organisationen „nicht wesentlich niedriger“ ist als das Schutzniveau, das für betroffene Personen gemäß den einschlägigen Datenschutzgesetzen des Vereinigten Königreichs vorgesehen ist.

---

<sup>69</sup> So könnte beispielsweise argumentiert werden, dass dies bei der Suche nach beschlagnahmten Geräten der Fall ist, die noch nicht analysiert oder entschlüsselt wurden.

87. In diesem Zusammenhang stellt der EDSA fest, dass die Elemente, die der Secretary of State bei der Bewertung gemäß Abschnitt 74 AB(2) des DPA 2018 zu berücksichtigen hat, im Vergleich zur vorherigen Bewertung der Angemessenheitsvorschriften offenbar reduziert wurden.<sup>70</sup> Der EDSA weist auf die Streichung bestimmter Faktoren hin, die seiner Ansicht nach eine wichtige Rolle bei der Beurteilung spielen, ob ein Drittland ein im Wesentlichen gleichwertiges Schutzniveau für personenbezogene Daten bietet, und verweist auf die Analyse und die Schlussfolgerungen in den Absätzen 42 und 43 dieser Stellungnahme. Insbesondere fordert der EDSA i) die Kommission auf, sich speziell mit den Änderungen zu befassen und ihre Bewertung des neuen Datenschutztests weiter auszuarbeiten. Der EDSA geht davon aus, dass die neuen Vorschriften für die Übermittlung personenbezogener Daten an Drittländer zusätzliche Flexibilität bieten sollen. Gleichzeitig fordert der EDSA die Kommission auf, die praktische Anwendung dieser Vorschriften im Bereich der Strafverfolgung und der justiziellen Zusammenarbeit in Strafsachen zu überwachen. Dies ist besonders relevant im Hinblick auf die neue Befugnis des Secretary of State, Vorschriften zu erlassen, die eine Übermittlung auf der Grundlage des neuen Datenschutztests identifizieren und genehmigen, und zwar mit allen Mitteln, einschließlich unter Bezugnahme auf geografische Sektoren innerhalb eines Landes, Verantwortliche oder Auftragsverarbeiter, Empfänger der Daten, Arten von Daten, Übermittlungswege und Rechtsinstrumente. Es bleibt beispielsweise unklar, wie ein bestimmter Verantwortlicher oder Auftragsverarbeiter mit Sitz in einem Drittland, das nicht als angemessen angesehen wird, die Datenschutzerfordernisse erfüllen würde, wenn es um wirksame Rechtsbehelfe oder Rechte der betroffenen Personen geht, die im Rechtsrahmen dieses Drittlandes noch nicht festgelegt sind.
88. Darüber hinaus erinnert der EDSA an die in Absatz 41 dargelegten Schlussfolgerungen in Bezug auf die Verwendung des Kriteriums der „Zweckmäßigkeit der Erleichterung der Übermittlung personenbezogener Daten nach und aus dem Vereinigten Königreich“ (Abschnitt 74 AA(3) des Datenschutzgesetzes von 2018) und fordert die Kommission auf, in ihrer Entscheidung klarzustellen, dass dieses Kriterium kein Bestandteil der Datenschutzprüfung ist, sondern lediglich ein zusätzlicher Faktor, den der Secretary of State berücksichtigen kann, wenn die Kriterien der Prüfung vollständig erfüllt sind, da dies aus dem Gesetzestext nicht ganz klar hervorgeht. In diesem Zusammenhang fordert der EDSA die Kommission auf, die praktischen Auswirkungen von Abschnitt 74AA(3) des Datenschutzgesetzes von 2018 zu beobachten, da noch abzuwarten bleibt, welche Rolle die „Zweckmäßigkeit der Erleichterung der Übermittlung personenbezogener Daten nach und aus dem Vereinigten Königreich“ in diesem Zusammenhang spielen wird.

---

<sup>70</sup> Die Bestimmung von Abschnitt 74A Absatz 4 des DPA 018, die vom DUAA ausgelassen wurde, enthielt eine Liste von Kriterien, die mit Artikel 36 Absatz 3 der Richtlinie zum Datenschutz bei der Strafverfolgung identisch waren.

#### 4.1.4.2. DAS CLOUD-ACT-ABKOMMEN ZWISCHEN DEM VEREINIGTEN KÖNIGREICH UND DEN USA

89. Eine weitere wichtige Entwicklung im Bereich der Weiterübermittlung ist das im Oktober 2022 in Kraft getretene „Abkommen zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugang zu elektronischen Daten für die Zwecke der Bekämpfung schwerer Kriminalität“ („UK-USA-Cloud Act Agreement“). Wie die Kommission zu Recht hervorhebt, könnten personenbezogene Daten, die aus der EU an Dienstleister im Vereinigten Königreich übermittelt werden, gemäß diesem Abkommen Gegenstand von Beweismaßnahmen sein, die von den zuständigen US-Strafverfolgungsbehörden erlassen werden.<sup>71</sup>
90. Da zum Zeitpunkt der Annahme der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich das Abkommen zwar geschlossen, aber noch nicht in Kraft getreten war, betonte die Kommission, dass alle Informationen und künftigen Klarstellungen hinsichtlich der Art und Weise, wie die USA ihren Verpflichtungen aus dem Abkommen nachkommen werden, vom Vereinigten Königreich an die Kommission weitergeleitet werden sollten, um eine ordnungsgemäße Überwachung der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich gemäß Artikel 45 Absatz 4 der DSGVO zu gewährleisten. Die Kommission wies darauf hin, dass der Anwendung und Anpassung der im Rahmenabkommen zwischen der EU und den USA festgelegten Schutzvorkehrungen auf die spezifischen Arten von Übermittlungen,<sup>72</sup> die unter das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den USA fallen, besondere Aufmerksamkeit gewidmet werden sollte.<sup>73</sup> Im Anschluss an diese Erklärung verweist die Kommission in ihrem Beschlussentwurf auf mehrere Klarstellungen, die zwischen dem Vereinigten Königreich und den USA im Zusammenhang mit der Anwendung des Rahmenabkommens zwischen der EU und den USA auf das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den USA erzielt wurden. Der EDSA begrüßt diese Klarstellungen, die für mehr Rechtssicherheit sorgen. Gleichzeitig ist darauf hinzuweisen, dass das Rahmenabkommen zwischen der EU und den USA noch nicht überprüft wurde, wodurch die Schlussfolgerungen, die hinsichtlich der Auswirkungen und der Wirksamkeit seiner Anwendung auf das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den USA gezogen werden können, in gewissem Maße eingeschränkt werden.<sup>74</sup> Darüber hinaus möchte der EDSA mit Blick auf das Rahmenabkommen zwischen der EU und den USA daran erinnern, dass die in diesem Abkommen vorgesehenen Garantien verbessert werden müssen. Dies gilt insbesondere für die Verfügbarkeit gerichtlicher Rechtsbehelfe. Betroffene Personen in der EU, die keine EU-Bürger sind, haben nach dem Gesetz über den gerichtlichen Rechtsbehelf keine Rechtsgrundlage für die Einlegung von Rechtsbehelfen. Darüber hinaus enthält das Datenschutzgesetz Ausnahmen, die durch das Gesetz über

<sup>71</sup> Siehe Erwägungsgrund 87 des Beschlussentwurfs.

<sup>72</sup> Siehe Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten.

Informationen im Zusammenhang mit der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, ABl.

L 336, 10.12.2016, S. 3–13, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)).

<sup>73</sup> Siehe Erwägungsgrund 155 des Durchführungsbeschlusses 2021/1772. Gemäß Artikel 9 Absatz 1 des Cloud-Act-Abkommens zwischen dem Vereinigten Königreich und den Vereinigten Staaten gilt das Rahmenabkommen zwischen der EU und den Vereinigten Staaten sinngemäß für das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den Vereinigten Staaten. Es kann nur sinngemäß angewendet werden, da das Rahmenabkommen grenzüberschreitende Übermittlungen zwischen Strafverfolgungsbehörden und nicht die direkte Zusammenarbeit zwischen einem Diensteanbieter und einer Strafverfolgungsbehörde regelt.

<sup>74</sup> Siehe Artikel 23 des Rahmenabkommens zwischen der EU und den USA, der vorsieht, dass die Parteien regelmäßige gemeinsame Überprüfungen der Strategien und Verfahren zur Umsetzung des Abkommens durchführen, wobei die erste Überprüfung spätestens drei Jahre nach Inkrafttreten des Abkommens stattfindet. Das Rahmenabkommen zwischen der EU und den USA trat im Februar 2017 in Kraft.

den Rechtsbehelf nicht geändert wurden und die die Möglichkeiten von Einzelpersonen einschränken, in bestimmten Situationen der Strafverfolgung und der nationalen Sicherheit Rechtsbehelf einzulegen. Die Kommission stellt zwar fest, dass das Gesetz über den Rechtsbehelf (Judicial Redress Act) nicht der einzige Mechanismus zur Erlangung eines Rechtsbehelfs ist, doch heißt es im Beschlussentwurf lediglich, dass „je nach den Umständen und dem Kontext des jeweiligen Einzelfalls andere anwendbare US-Gesetze alternative Wege für die Erlangung eines Rechtsbehelfs bieten“<sup>75</sup>. Damit bleibt unklar, ob allen EU-Personen, deren Daten unter das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den USA fallen können, Rechtsbehelfe in den USA gewährt werden.

91. Der EDSA stellt ferner fest, dass eine spezifische gegenseitige Garantie, die im Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den USA festgelegt ist, wonach beide Parteien die möglichen Auswirkungen des Abkommens auf Personen im Vereinigten Königreich bzw. in den USA begrenzen, naturgemäß nicht für Personen in der EU gilt.<sup>76</sup> Der EDSA stellt fest, dass aus diesem Grund robuste Datenschutzgarantien unerlässlich sind, um sicherzustellen, dass die Rechte der betroffenen Personen in der EU angemessen geschützt werden, wenn ihre Daten im Rahmen dieses Abkommens verarbeitet werden. Daher fordert der EDSA die Kommission auf, das Cloud-Act-Abkommen zwischen dem Vereinigten Königreich und den Vereinigten Staaten auch weiterhin in ihre künftigen Bewertungen und Überprüfungen der Angemessenheitsentscheidung einzubeziehen.
92. Insgesamt sieht der EDSA Klärungsbedarf hinsichtlich der Bewertung des Cloud-Act-Abkommens zwischen dem Vereinigten Königreich und den Vereinigten Staaten durch die Kommission und hinsichtlich möglicher Auswirkungen des Abkommens auf das Schutzniveau, wie es in der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich bewertet wurde. Die Ergebnisse der ersten Überprüfung des Cloud-Act-Abkommens zwischen dem Vereinigten Königreich und den Vereinigten Staaten, die gemäß Artikel 12 Absatz 1 des Abkommens innerhalb eines Jahres nach Inkrafttreten des Abkommens durchgeführt werden soll, könnten für eine solche weitere Analyse besonders aufschlussreich sein.

#### 4.1.5. AUFSICHT UND RECHTSSCHUTZ

93. Der EDSA stellt fest, dass das System zur Überwachung der Strafverfolgungsbehörden gemäß dem Datenschutzgesetz von 2018 und dem IPA von 2016 sowie die Rechtsbehelfsmechanismen gemäß Teil 3 des DPA von 2018, des IPA von 2016 und des Menschenrechtsgesetzes von 1998 weitgehend unverändert bleiben. Insbesondere wird die Aufsicht im Vereinigten Königreich neben dem ICO weiterhin durch eine Kombination verschiedener Kommissionsmitglieder gewährleistet, nämlich den Kommissar für Untersuchungsbefugnisse (Investigative Powers Commissioner, IPC), der von anderen Justizkommissaren unterstützt wird, sowie den Kommissar für Biometrie und Surveillance-Kamera.
94. Wie die Kommission in Erwägungsgrund 97 des Beschlussentwurfs erläutert, wurden mit dem Investigatory Powers Amendment Act 2024 nur begrenzte Änderungen vorgenommen, insbesondere durch die Einführung von stellvertretenden IPCs, denen die IPC bestimmte Befugnisse übertragen kann, wenn sie ihre Aufgaben nicht wahrnehmen können oder nicht verfügbar sind. Bei diesen stellvertretenden IPC muss es sich um Justizkommissare handeln, die von der IPC ernannt werden.

---

<sup>75</sup> Siehe Erwägungsgrund 93 des Beschlussentwurfs.

<sup>76</sup> Siehe Artikel 4 Absatz 3 und Artikel 7 Absatz 1 des Abkommens, die Zielbeschränkungen vorsehen und festlegen, dass Aufträge, die unter das Abkommen fallen, nicht absichtlich auf eine „empfangende Partei“ ausgerichtet sein dürfen. Daher können die USA nicht vorsätzlich gegen eine Person vorgehen, die sich im Hoheitsgebiet des Vereinigten Königreichs befindet, und das Vereinigte Königreich muss eine ähnliche Beschränkung einhalten.

95. Der EDSA begrüßt, dass die früheren Vorschläge im Rahmen des Gesetzes über Datenschutz und digitale Informationen, die dem DUUA vorausgegangen waren, nämlich die Abschaffung des Kommissars für Biometrie und Überwachungskamera und die Übertragung der Rolle auf den Kommissar für Untersuchungsbefugnisse, verworfen wurden.<sup>77</sup> In diesem Zusammenhang fordert der EDSA die Kommission auf, der Rolle des Beauftragten für Biometrie und Überwachungskameras im Rahmen des Aufsichtssystems während der Überwachung und künftigen Überprüfungen des Beschlussentwurfs mehr Aufmerksamkeit zu widmen und eine detailliertere Bewertung vorzunehmen.
96. Wie der EDSA bereits in seiner Stellungnahme 14/2021 betont hat, verfügt das ICO zwar über die erforderlichen Befugnisse, die weitgehend den Befugnissen der Aufsichtsbehörden der EU-Mitgliedstaaten gemäß Artikel 58 der DSGVO entsprechen, doch spielen wirksame Sanktionen eine wichtige Rolle bei der Gewährleistung der Einhaltung der Vorschriften<sup>78</sup>.
97. Der EDSA begrüßt die Transparenzpolitik des ICO und die Verfügbarkeit statistischer und analytischer Daten, einschließlich Beispielen, über die Durchsetzungstätigkeiten des ICO gegenüber Strafverfolgungsbehörden.<sup>79</sup> In diesem Zusammenhang hält der EDSA eine Präferenz der britischen Aufsichtsbehörde für Verwarnungen im Falle von Verstößen gegen die Datenschutzvorschriften durch die Polizei fest. Eine bemerkenswerte Ausnahme ist die im Januar 2024 an die Staatsanwaltschaft des Vereinigten Königreichs gerichtete Durchsetzungsmitteilung<sup>80</sup>. Der EDSA hält es auch für positiv, dass das ICO zahlreiche Verhaltenskodizes, Leitlinien, Stellungnahmen und andere Leitfäden für die betroffenen Parteien veröffentlicht hat.
98. Vor diesem Hintergrund und insbesondere angesichts der bevorstehenden wesentlichen Änderungen in der Struktur und Organisation der Aufsichtsbehörde des Vereinigten Königreichs, wie bereits in Nummer 68 dieser Stellungnahme analysiert, fordert der EDSA die Europäische Kommission auf, die Wirksamkeit von Sanktionen und einschlägigen Rechtsbehelfen im Rahmen des Datenschutzrahmens des Vereinigten Königreichs weiterhin zu überwachen.

#### 4.2. ZUGANG VON UND VERWENDUNG DURCH BEHÖRDEN DES VEREINIGTEN KÖNIGREICHS ZU KOMMUNIKATIONSDATEN FÜR ZWECKE DER NATIONALEN SICHERHEIT

99. Der Beschlussentwurf enthält nur begrenzte Einzelheiten über den Zugang zu personenbezogenen Daten und deren Verwendung durch Behörden des Vereinigten Königreichs für Zwecke der nationalen Sicherheit. Die Kommission erklärt, dass im DUUA nur geringfügige Änderungen am Rahmen für die Datenverarbeitung durch Nachrichtendienste des Vereinigten Königreichs vorgenommen wurden<sup>81</sup>, von denen einige auch in die Strafverfolgungsregelung des Datenschutzgesetzes 2018 aufgenommen wurden. Diese Änderungen werden in Erwägungsgrund 75 des Beschlussentwurfs kurz erwähnt. Darüber hinaus werden die seit der Annahme der vorherigen Angemessenheitsentscheidung für das Vereinigte Königreich vorgenommenen Änderungen am IPA 2016 bereits in Abschnitt 3.2 des Beschlussentwurfs behandelt, wo sie sowohl die Datenverarbeitung zu Strafverfolgungszwecken als

---

<sup>77</sup> Siehe <https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner>.

<sup>78</sup> Vgl. EDSA, Stellungnahme 14/2021, Randnummer 112.

<sup>79</sup> Siehe z. B. die detaillierten Datensätze zu Datenschutzbeschwerden, abrufbar unter <https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-protection-complaints/>.

<sup>80</sup> Siehe <https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/>.

<sup>81</sup> Siehe Erwägungsgrund 75 des Beschlussentwurfs.

auch zu Zwecken der nationalen Sicherheit betreffen.<sup>82</sup> Dementsprechend gelten die in den Abschnitten und 4.1.1.1 oben dargelegten Ersuchen um Klarstellung 4.1.3 und Überwachung gleichermaßen für den Zugang zu personenbezogenen Daten und deren Verwendung für Zwecke der nationalen Sicherheit.

#### 4.2.1. DIE VERWENDUNG VON HINWEISEN ÜBER DIE TECHNISCHE LEISTUNGSFÄHIGKEIT

100. Anfang dieses Jahres wurde in Medienberichten bekannt, dass die Regierung des Vereinigten Königreichs angeblich gemäß Abschnitt 253 des IPA 2016 eine Technical Capability Notice („TCN“) an ein großes Technologieunternehmen herausgegeben hatte, in der der Anbieter aufgefordert wurde, den Zugriff auf die verschlüsselten Daten seiner Nutzer in entschlüsselter Form aufrechtzuerhalten.<sup>83</sup> In der Praxis würde dies angeblich bedeuten, die End-to-End-Verschlüsselung zu umgehen, die der Anbieter für seine Cloud-Speicherlösung anbietet. Diese Maßnahme wurde daher als „Hintertür-Nachfrage“ bezeichnet.
101. Obwohl die Rechtsgrundlage für TCNs bereits zum Zeitpunkt der Verabschiedung der vorherigen Angemessenheitsentscheidung des Vereinigten Königreichs bestand, scheint dieser gemeldete Fall der erste bekannte Fall einer Anwendung dieser Art zu sein. Als solche stellt sie eine wesentliche Entwicklung dar, die besondere Aufmerksamkeit verdient, insbesondere im Hinblick auf Artikel 45 Absatz 2 Buchstabe a DSGVO, der nicht nur eine Bewertung des rechtlichen Rahmens auf dem Papier, sondern auch eine Bewertung seiner Umsetzung erfordert.<sup>84</sup> Der EDSA hätte daher erwartet, dass der Beschlussentwurf diese Frage ausdrücklich behandelt, und fordert die Kommission auf, die Entscheidung entsprechend zu ergänzen.
102. Obwohl die Einzelheiten dieses Falls der Öffentlichkeit aufgrund des vertraulichen Charakters von Drittstaatsangehörigen nicht vollständig bekannt sind, geht aus der öffentlichen Auflistung des Antrags auf eine Verhandlung unter Ausschluss der Öffentlichkeit auf der Website des Gerichts für Untersuchungsbefugnisse sowie aus dem öffentlich zugänglichen Auszug aus dem privaten Urteil über eine solche Anhörung hervor, dass es nicht um Medienspekulationen geht.<sup>85</sup> Die Angelegenheit verdient Erwähnung, und die angebliche Anwendung von Abschnitt 253 des IPA 2016 zur Ausstellung einer „Hintertürforderung“ sollte zur künftigen Überwachung markiert werden.
103. Wie kürzlich in der Erklärung 05/2024 dargelegt, hält der EDSA die Verschlüsselung für unerlässlich, um die Sicherheit und Vertraulichkeit personenbezogener Daten und der elektronischen Kommunikation zu gewährleisten. Insbesondere eine echte End-to-End-Verschlüsselung, die die Endgeräte und die darin enthaltenen Daten abdeckt und bei der die Entschlüsselungscodes ausschließlich beim Nutzer liegen, ist ein entscheidendes Instrument zur Gewährleistung der Vertraulichkeit der elektronischen Kommunikation.<sup>86</sup> Drittstaatsangehörige, die Unternehmen dazu verpflichten, auf Ersuchen der Regierung die Möglichkeit zur Entfernung von Verschlüsselung zur

---

<sup>82</sup> Siehe Erwägungsgrund 98 des Beschlussentwurfs. Die fraglichen Ermittlungsbefugnisse können nicht nur von nationalen Nachrichtendiensten, sondern auch von bestimmten Strafverfolgungsbehörden ausgeübt werden.

<sup>83</sup> Siehe „Großbritannien verpflichtet Apple, verschlüsselte Konten von Nutzern zu überwachen“ (Washington Post, 7. Februar 2025), <https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/>.

<sup>84</sup> Darüber hinaus ist in Artikel 45 Absatz 3 DSGVO festgelegt, dass die Kommission bei der regelmäßigen Überprüfung ihrer Angemessenheitsfeststellungen alle relevanten Entwicklungen in dem Drittland berücksichtigt.

<sup>85</sup> Siehe <https://www.judiciary.uk/judgments/apple-inc-v-secretary-of-state-for-the-home-department/>.

<sup>86</sup> Siehe Erklärung 5/2024 zu den Empfehlungen der hochrangigen Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung, angenommen am 4. November 2024, S. 4, 5.

Verfügung zu stellen, schaffen systemische Schwachstellen und stellen eine direkte Bedrohung für die Integrität und Vertraulichkeit der elektronischen Kommunikation dar. In diesem Zusammenhang verweist der EDSA auf den Fall PODCHASOV gegen RUSSLAND, in dem der EGMR feststellte, dass eine „Verpflichtung zur Entschlüsselung von Ende-zu-Ende-verschlüsselten Kommunikationen die Gefahr birgt, dass Anbieter solcher Dienste den Verschlüsselungsmechanismus für alle Nutzer schwächen müssen; dies steht daher in keinem angemessenen Verhältnis zu den verfolgten legitimen Zielen“.<sup>87</sup>

104. Es wird zwar davon ausgegangen, dass die Regierung des Vereinigten Königreichs in erster Linie versuchen würde, auf unverschlüsselte Nutzerdaten zuzugreifen, wenn ein Risiko für die nationale Sicherheit bestünde, doch ist der EDSA der Auffassung, dass das Ersuchen um eine Bewertung der Nutzung von Drittstaatsangehörigen, wie oben erörtert, im Zusammenhang mit dem Zugang staatlicher Stellen zu Strafverfolgungszwecken gleichermaßen relevant ist.

#### 4.2.2. RECHTSGRUNDLAGEN UND ANWENDBARE GARANTIE

105. Mit der Änderung der Ermittlungsbefugnisse von 2024 wurde eine spezifische Regelung für die Speicherung und Prüfung großer Mengen personenbezogener Datensätze eingeführt, bei denen die Personen, auf die sich die personenbezogenen Daten beziehen, „keine oder nur geringe begründete Erwartungen an die Privatsphäre haben können“, wie es im Gesetz heißt.<sup>88</sup> Für die Aufbewahrung und Überprüfung solcher spezifischer Teilmengen von personenbezogenen Massendatensätzen sieht die IPA 2016 nun die Möglichkeit von „Einzelgenehmigungen“ und „Kategoriegenehmigungen“ vor.<sup>89</sup>
106. Der Begriff „große personenbezogene Datensätze“ ist weit gefasst und kann eine Vielzahl von Datensätzen umfassen.<sup>90</sup> Sie kann sich auf sensible Informationen beziehen, kann aber auch öffentlich und kommerziell verfügbare Daten umfassen. Vor diesem Hintergrund hielt es die Regierung des Vereinigten Königreichs für notwendig, die bisherige Regelung, die für alle personenbezogenen Massendatenbestände das gleiche Schutzniveau vorsah, zu überarbeiten und stattdessen unterschiedliche Schutzmaßnahmen für die Speicherung und Auswertung von personenbezogenen Massendatenbeständen vorzusehen, je nach Sensibilität oder öffentlicher Zugänglichkeit ihrer Inhalte oder dem Ausmaß der Eingriffe, die mit der Speicherung und Auswertung durch die Nachrichtendienste verbunden sind.<sup>91</sup> Nach Auffassung des EDSA führten diese Überlegungen letztendlich zur Schaffung einer gesonderten Regelung für personenbezogene Massendatenbestände, bei denen nur eine geringe oder keine angemessene Erwartung auf Privatsphäre besteht.

---

<sup>87</sup> Siehe EGMR, Urteil vom 13. Februar 2024, 33696/19, Rn. 79.

<sup>88</sup> Siehe Abschnitt 226A Absatz 1 IPA 2016.

<sup>89</sup> Siehe Abschnitte 226A und 226BA des IPA 2016 in der durch Abschnitt 2 der Änderung über Untersuchungsbefugnisse eingeführten Fassung.  
Gesetz 2024.

<sup>90</sup> Siehe Abschnitt 199 des IPA 2016, der festlegt, dass ein „Nachrichtendienst einen personenbezogenen Massendatensatz aufbewahrt, wenn (a) der Nachrichtendienst eine Reihe von Informationen erhält, die personenbezogene Daten zu einer Reihe von Personen enthalten, (b) die Art des Datensatzes derart ist, dass die Mehrheit der Personen für den Nachrichtendienst bei der Ausübung seiner Aufgaben nicht von Interesse ist und wahrscheinlich auch nicht von Interesse werden wird, (c) der Nachrichtendienst den Datensatz nach einer ersten Prüfung des Inhalts zum Zwecke der Ausübung seiner Aufgaben aufbewahrt und (d) der Datensatz zur Analyse im Rahmen der Ausübung dieser Aufgaben elektronisch gespeichert wird oder gespeichert werden soll“.

<sup>91</sup> Siehe Home Office, Policy paper Investigatory Powers (Amendment) Bill: Bulk Personal Datasets und Third Party Bulk Personal Datasets, <https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-bulk-personal-datasets-and-third-party-bulk-personal-datasets>.

107. Während die Kommission das neue Konzept einer „Kategoriegenehmigung“ kurz erörtert, heißt es im Beschlussentwurf, dass „für die Speicherung und Prüfung großer Mengen personenbezogener Datensätze die in den Erwägungsgründen 239 und 240 des Durchführungsbeschlusses (EU) 2021/1772 bewertete Regelung weiterhin gilt, insbesondere die Notwendigkeit einer Anordnung, die zunächst vom Secretary of State und dann vom Justizkommissar vorbehaltlich der Anforderungen der Notwendigkeit und Verhältnismäßigkeit der Maßnahme gebilligt wird, wie in Teil 7 des IPA 2016 vorgesehen“<sup>92</sup>. Diese Analyse scheint jedoch unvollständig zu sein. Der EDSA stellt fest, dass nicht nur die Einführung von „Kategorisierungsgenehmigungen“, sondern auch von „Einzelgenehmigungen“ eine relevante Änderung darstellt, die durch das Investigatory Powers Amendment Act 2024 in Bezug auf den oben genannten spezifischen Datensatz umgesetzt wurde: Eine „Einzelgenehmigung“, die vom Leiter eines Nachrichtendienstes oder einer in dessen Namen handelnden Person erteilt werden kann, ersetzt die Notwendigkeit, einen Durchsuchungsbefehl einzuholen, um personenbezogene Massendatensätze, für die nur eine geringe oder keine angemessene Erwartung auf Privatsphäre besteht, aufzubewahren oder aufzubewahren und zu prüfen.<sup>93</sup> Die Begriffe „Berechtigung“ und „individuelle Bewilligung“ sollten daher nicht verwechselt werden und können nicht synonym verwendet werden.<sup>94</sup> Dies gilt insbesondere, weil sich die gerichtliche Genehmigung, die für Einzelgenehmigungen erforderlich ist, auf die Frage beschränkt, ob der spezifische Datensatz die Kriterien für eine Einstufung als Bedrohung nur einer geringen oder gar keiner vernünftigen Erwartung eines Schutzes der Privatsphäre gemäß Abschnitt 226A des IPA 2016 erfüllt.<sup>95</sup> Eine „Kategoriegenehmigung“ unterscheidet sich von einer „Einzelgenehmigung“ und entzieht – gemäß Abschnitt 226B Absatz 6 Buchstabe a des IPA 2016 – das Erfordernis einer solchen gerichtlichen Genehmigung einer Einzelgenehmigung, wenn sie sich auf einen Datensatz bezieht, der unter eine Kategoriegenehmigung fällt. Der Grund dafür ist, dass bereits eine Entscheidung getroffen und von einem Justizkommissar genehmigt wurde, dass jeder Datensatz, der unter die Beschreibung in der Kategoriegenehmigung fällt, tatsächlich ein Datensatz ist, auf den Abschnitt 226A Anwendung findet.
108. Obwohl diese Änderungen die Speicherung und Überprüfung von personenbezogenen Massendaten betreffen und nicht deren ursprüngliche Erfassung oder Erhebung, möchte der EDSA die Bedeutung hervorheben, die der EGMR einer vorherigen unabhängigen Genehmigung im Zusammenhang mit der Verarbeitung personenbezogener Massendaten beimisst. Der Gerichtshof befand: „Um das Risiko eines Missbrauchs der Befugnis zur Sammelüberwachung so gering wie möglich zu halten, [...] muss das Verfahren durchgängigen Garantien unterliegen, was bedeutet, dass auf nationaler Ebene in jeder Phase des Verfahrens die Notwendigkeit und Verhältnismäßigkeit der ergriffenen Maßnahmen bewertet werden sollten; dass die Sammelüberwachung von Anfang an einer unabhängigen Genehmigung unterliegen sollte, wenn Ziel und Umfang des Vorgangs festgelegt werden; und dass der Vorgang einer Überwachung und unabhängigen nachträglichen Überprüfung unterzogen werden sollte.“<sup>96</sup> Vor diesem Hintergrund und auf der Grundlage eines ganzheitlichen Ansatzes und unter Berücksichtigung aller Umstände des Falles bei der Beurteilung der Angemessenheit sollte die Speicherung und Prüfung von personenbezogenen Datensätzen zumindest entweder einer vorherigen Genehmigung durch eine unabhängige Behörde oder einer systematischen unabhängigen Ex-post-

---

<sup>92</sup> Siehe Erwägungsgrund 99 des Beschlussentwurfs.

<sup>93</sup> Abschnitt 200 Absätze 1 und 2 des IPA 2016.

<sup>94</sup> Dies scheint jedoch in den Erwägungsgründen 99 und 100 des Beschlussentwurfs der Fall zu sein.

<sup>95</sup> Abschnitt 226BB(1) des IPA 2016 legt fest, dass bei der Entscheidung über die Genehmigung einer Einzelgenehmigung oder einer Kategoriegenehmigung ein Justizkommissar die Schlussfolgerungen der Person, die die Genehmigung erteilt hat, überprüfen muss, um festzustellen, ob Abschnitt 226A auf den in der Genehmigung beschriebenen personenbezogenen Massendatensatz oder ob Abschnitt 226A auf einen Datensatz Anwendung findet, der unter die in der Genehmigung beschriebene Kategorie von Datensätzen fällt.

<sup>96</sup> EGMR, Big Brother Watch u. a. gegen Vereinigtes Königreich, 25. Mai 2021, Rn. 350.

Überprüfung durch ein Gericht oder eine gleichwertige Stelle, d. h. eine unabhängige Stelle, die verbindliche Entscheidungen erlassen kann, unterliegen.

109. Angesichts der verbleibenden erforderlichen Klarstellungen fordert der EDSA die Kommission nachdrücklich auf, die Begriffe „Einzelzulassungen“ und „Kategoriegenehmigungen“ im Rahmen der Änderung der Untersuchungsbefugnisse 2024 weiter zu prüfen. Darüber hinaus fordert der EDSA die Kommission auf, die Umsetzung des Begriffs „geringe oder keine berechtigten Erwartungen an den Schutz der Privatsphäre“ in der Praxis genau zu überwachen. Obwohl Abschnitt 226A des IPA 2016 eine Reihe von Kriterien für eine solche Feststellung festlegt, hält es der EDSA für wichtig, deren Anwendung zu beobachten, da sie potenziell weit ausgelegt werden können.<sup>97</sup>

#### 4.2.3. AUFSICHT UND RECHTSSCHUTZ

110. Wie im Beschlussentwurf angegeben und bereits in der Stellungnahme 14/2021 analysiert, spielen der Kommissar für Untersuchungsbefugnisse (Investigative Powers Commissioner, IPC) und sein Büro (Investigative Powers Commissioner, IPCO) eine zentrale Rolle bei der Überwachung der Ausübung von Untersuchungsbefugnissen durch die Geheimdienste des Vereinigten Königreichs. Darüber hinaus ist das Gericht für Untersuchungsbefugnisse (Investigative Powers Tribunal, IPT) das zuständige Gericht, das in dieser Hinsicht für Rechtsbehelfe zuständig ist. Wie bereits in Abschnitt 3.1.5. zur Aufsicht im Bereich der Strafverfolgung dargelegt, wurden durch das Gesetz zur Änderung der Ermittlungsbefugnisse von 2024 nur begrenzte Änderungen vorgenommen, insbesondere durch die Einführung von stellvertretenden IPCs. Daher behalten die Anmerkungen des EDSA in seiner Stellungnahme 14/2021 ihre volle Gültigkeit<sup>98</sup>.
111. Der EDSA begrüßt die transparente jährliche Berichterstattung der IPCO, einschließlich der Verfügbarkeit detaillierter Statistiken für den Zeitraum 2019–2023, unter anderem über die Nutzung von Massenbefugnissen durch die britischen Nachrichtendienste sowie über die Zielauswahlentscheidungen und die gezielten Genehmigungen zum Zweck der Datenerfassung gemäß dem Datenzugriffsabkommen zwischen dem Vereinigten Königreich und den Vereinigten Staaten. Der EDSA nimmt auch ausdrücklich die Überwachungstätigkeiten der IPCO hinsichtlich der massenhaften Überwachung von Daten durch das Government Communications Headquarters (GCHQ) zur Kenntnis, die von der Kommission in Erwägungsgrund 102 des Beschlussentwurfs hervorgehoben wurden. In diesem Zusammenhang fordert der EDSA die Kommission auf, die Wirksamkeit des Aufsichtssystems in diesem Bereich weiterhin genau zu überwachen, insbesondere im Hinblick auf die Verhältnismäßigkeit der Sammelüberwachungsersuchen.<sup>99</sup>
112. Darüber hinaus stellt der EDSA fest, dass das Gericht für Untersuchungsbefugnisse auch einen öffentlichen Bericht über seine Tätigkeiten und seine Rechtsprechung für den Zeitraum 2021-2023 herausgegeben hat.<sup>100</sup> In dem Bericht werden unter anderem wichtige und relevante Entwicklungen hervorgehoben, wie das Urteil des Europäischen Gerichtshofs für Menschenrechte in der Rechtssache *Wieder und Guarnieri / Vereinigtes Königreich*, in dem entschieden wurde, dass Einzelpersonen überall auf der Welt einen Anspruch im IPT geltend machen können, wenn das Verhalten von einer

<sup>97</sup> Abschnitt 226A des IPA 2016 bezieht sich beispielsweise auf die Art der Daten, den Umfang, in dem die Daten veröffentlicht wurden, oder den Umfang, in dem die Daten allgemein bekannt sind.

<sup>98</sup> Siehe Stellungnahme 14/2021, Absätze 200 bis 215.

<sup>99</sup> Weitere Informationen sind dem Jahresbericht 2023 des Kommissars für Untersuchungsbefugnisse zu entnehmen, der unter folgendem Link abrufbar ist: [https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC\\_603-IPCO-Annual-Report-2023-Web\\_Accessible.pdf](https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf), Seite 31, Abschnitt 6.41.

<sup>100</sup> <https://investigatorypowertribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf>

öffentlichen Einrichtung des Vereinigten Königreichs begangen wurde und im Vereinigten Königreich stattfand. Der EDSA fordert die Kommission daher auf, auch die Tätigkeiten des IPT in ihre Bewertung und in künftige Überprüfungen des Beschlussentwurfs einzubeziehen.

## 5. ÜBERPRÜFUNG, DAUER UND VERLÄNGERUNG DES BESCHLUSSENTWURFS

113. Der EDSA stellt fest, dass der endgültige Angemessenheitsbeschluss für sechs Jahre gelten würde, d. h. bis zum 27. Dezember 2031. Es wäre somit weiterhin das einzige Drittland, dessen Angemessenheitsentscheidung eine Auslaufklausel enthält, die mit der in Artikel 45 Absatz 3 DSGVO vorgesehenen obligatorischen regelmäßigen Überprüfung verbunden ist. Der EDSA ist sich bewusst, dass der neue Rechtsrahmen des Vereinigten Königreichs besondere Aufmerksamkeit verdient, und fordert die Kommission auf, die Umsetzung der DUAA, einschließlich der in dieser Stellungnahme hervorgehobenen Schwerpunktbereiche, sowie alle anderen relevanten Entwicklungen im Vereinigten Königreich in dieser Hinsicht sorgfältig zu überwachen.
114. Der EDSA begrüßt, dass in Erwägungsgrund 68 des Beschlussentwurfs auf die Rolle des EDSA (und zivilgesellschaftlicher Gruppen) im Rahmen des Mechanismus zur regelmäßigen Überprüfung gemäß der Empfehlung 01/2021 des EDSA<sup>101</sup> hingewiesen wird. Was die praktische Einbeziehung des EDSA und seiner Vertreter in die Vorbereitung und Durchführung der künftigen Überprüfung betrifft, wiederholt der EDSA, dass alle einschlägigen Unterlagen dem EDSA rechtzeitig vor den Überprüfungen schriftlich mitgeteilt werden sollten.
115. Aus den zusätzlichen Erläuterungen der Kommission zu Erwägungsgrund 113 geht nach Auffassung des EDSA hervor, dass beabsichtigt ist, nach Ablauf der vier Jahre eine Überprüfung durchzuführen, auf deren Grundlage die Kommission einen öffentlichen Bericht erstellen wird<sup>102</sup>. Diese Überprüfung wird der Kommission Aufschluss darüber geben, ob sie spätestens sechs Monate vor Ablauf des Beschlussentwurfs das Verfahren zur Verlängerung der Laufzeit des Beschlussentwurfs einleiten soll<sup>103</sup>.
116. Der EDSA begrüßt diese Absicht und stellt fest, dass die Überprüfung einem anderen Zweck dient als die Verfallsklausel und eine wichtige Rolle bei der Überwachung des Rechtsrahmens spielt. Der EDSA geht daher davon aus, dass die Überprüfung in vier Jahren stattfinden wird, und fordert die Kommission auf, diese zu gegebener Zeit durchzuführen.

---

<sup>101</sup> Siehe Erwägungsgrund 19 der Empfehlung 01/2021 des EDSA.

<sup>102</sup> Siehe Erwägungsgrund 110 des Beschlussentwurfs.

<sup>103</sup> Siehe Erwägungsgrund 113 des Beschlussentwurfs.

117. Der EDSA geht davon aus, dass bei dieser künftigen Überprüfung die im Durchführungsbeschluss 2021/1772 der Kommission dargelegten Elemente berücksichtigt werden und dass die Erwägungsgründe über die Aussetzung und Aufhebung des Beschlusses nach wie vor gültig sind<sup>104</sup>. Aus Gründen der Rechtssicherheit ist der EDSA der Auffassung, dass eine solche Klarstellung im endgültigen Angemessenheitsbeschluss enthalten sein könnte.

Für den Europäischen Datenschutzausschuss

Der Vorsitz

(Anu Talus)

---

<sup>104</sup> Siehe Erwägungsgründe 168 bis 171 des Durchführungsbeschlusses 2021/1173 der Kommission.