Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2574

23.12.2025

DURCHFÜHRUNGSBESCHLUSS (EU) 2025/2574 DER KOMMISSION

vom 19. Dezember 2025

zur Änderung des Durchführungsbeschlusses (EU) 2021/1772 der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich

(Bekannt gegeben unter Aktenzeichen C(2025) 8771)

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ([1]), insbesondere auf Artikel 45 Absatz 3,

in Erwägung nachstehender Gründe:

1. EINFÜHRUNG

(1) Im Durchführungsbeschluss (EU) 2021/1772 der Kommission ([2]) wird der Schluss gezogen, dass das Vereinigte Königreich für die Zwecke des Artikels 45 der Verordnung (EU) 2016/679 ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die im Rahmen des Anwendungsbereichs der genannten Verordnung aus der Europäischen Union an das Vereinigte Königreich übermittelt werden ([3]).

(2) Bei der Annahme des Durchführungsbeschlusses (EU) 2021/1772 berücksichtigte die Kommission, dass das Vereinigte Königreich nach dem Ende des im Abkommen über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft ([4]) vorgesehenen Übergangszeitraums und nach dem Außerkrafttreten der Übergangsbestimmung gemäß Artikel 782 des Abkommens über Handel und Zusammenarbeit zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits ([5]) eine neue Datenschutzregelung erlassen, anwenden und durchsetzen würde, die sich von der Regelung unterscheidet, die galt, als das Vereinigte Königreich noch durch Unionsrecht gebunden war.

(3) Da dies Änderungen des im Durchführungsbeschluss (EU) 2021/1772 bewerteten Datenschutzrahmens oder andere einschlägige Entwicklungen zur Folge haben könnte, erschien es angebracht vorzusehen, dass der genannte Beschluss für einen Zeitraum von vier Jahren ab seinem Inkrafttreten gilt. Die Geltungsdauer des Durchführungsbeschlusses (EU) 2021/1772 endete daher am 27. Juni 2025, sofern er nicht nach dem in Artikel 93 Absatz 2 der Verordnung (EU) 2016/679 genannten Verfahren verlängert wurde.

([1]) ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Durchführungsbeschluss (EU) 2021/1772 der Kommission vom 28. Juni 2021 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (ABl. L 360 vom 11.10.2021, S. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).
([3]) Siehe Artikel 1 Absatz 1 des Durchführungsbeschlusses (EU) 2021/1772. Gemäß Artikel 1 Absatz 2 des Beschlusses gilt der Beschluss nicht für personenbezogene Daten, die für die Zwecke der Einwanderungskontrolle im Vereinigten Königreich übermittelt werden oder anderweitig in den Anwendungsbereich der Ausnahme von bestimmten Rechten betroffener Personen für die Zwecke der Aufrechterhaltung einer wirksamen Einwanderungskontrolle gemäß dem Anhang 2 Paragraf 4 Absatz 1 des britischen Gesetzes über den Datenschutz von 2018 (UK Data Protection Act 2018) fallen.
([4]) ABl C 384 I vom 12.11.2019, S. 1.
([5]) ABl. L 149 vom 30.4.2021, S. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) Um über eine mögliche Verlängerung des Durchführungsbeschlusses (EU) 2021/1772 zu entscheiden, muss die Kommission beurteilen, ob die Feststellung, dass das Vereinigte Königreich ein angemessenes Schutzniveau gewährleistet, im Hinblick auf die seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 eingetretenen Entwicklungen in Bezug auf die in Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 aufgezählten Elemente weiterhin sachlich und rechtlich gerechtfertigt ist.

(5) Insbesondere hat die Regierung des Vereinigten Königreichs am 23. Oktober 2024 den Data (Use and Access) Bill ([6]) (Gesetzentwurf zur Nutzung von und zum Zugang zu Daten) in das Parlament des Vereinigten Königreichs eingebracht, in dem Änderungen an der britischen Datenschutz-Grundverordnung (United Kingdom General Data Protection Regulation, im Folgenden „UK GDPR“) und am Data Protection Act 2018 (Gesetz über den Datenschutz von 2018, im Folgenden „DPA 2018“) vorgeschlagen werden, die im Durchführungsbeschluss (EU) 2021/1772 bewertet werden. Am 24. Juni 2025 erließ die Kommission den Durchführungsbeschluss (EU) 2025/1226 ([7]), mit dem die Geltungsdauer des Durchführungsbeschlusses (EU) 2021/1772 um sechs Monate bis zum 27. Dezember 2025 verlängert wurde. Diese zeitlich begrenzte technische Verlängerung ermöglichte es der Kommission, ihre Bewertung des angemessenen Schutzniveaus für personenbezogene Daten durch das Vereinigte Königreich auf der Grundlage eines stabilen Rechtsrahmens, d. h. nach Abschluss des einschlägigen Gesetzgebungsverfahrens, abzuschließen ([8]).

(6) Seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 überwachte die Kommission fortlaufend die einschlägigen Entwicklungen im Vereinigten Königreich ([9]). Im Einklang mit Erwägungsgrund 281 des Durchführungsbeschlusses (EU) 2021/1772 galt die besondere Aufmerksamkeit der praktischen Anwendung der Vorschriften des Vereinigten Königreichs über die Übermittlung personenbezogener Daten an Drittländer und deren möglichen Auswirkungen auf das Schutzniveau für die im Rahmen des Durchführungsbeschlusses (EU) 2021/1772 übermittelten Daten, auf der Wirksamkeit der Ausübung individueller Rechte, einschließlich einschlägiger rechtlicher und praktischer Entwicklungen in Bezug auf Ausnahmen oder Beschränkungen dieser Rechte (insbesondere im Zusammenhang mit der Aufrechterhaltung einer wirksamen Einwanderungskontrolle), sowie auf der Einhaltung der Beschränkungen und Garantien in Bezug auf den Zugang der Regierung. Unter anderem flossen Entwicklungen in der Rechtsprechung sowie die Aufsichtstätigkeit des Information Commissioner's Office (ICO) und anderer unabhängiger Stellen in die Überwachung der Kommission ein.

(7) Auf der Grundlage der Bewertung dieser Entwicklungen, einschließlich der mit dem Data (Use and Access) Act eingeführten Änderungen am UK GDPR und am DPA 2018, kommt die Kommission zu dem Schluss, dass das Vereinigte Königreich weiterhin ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die im Rahmen des Anwendungsbereichs der Verordnung (EU) 2016/679 aus der Europäischen Union in das Vereinigte Königreich übermittelt werden.

(8) Die Kommission kommt ferner zu dem Schluss, dass angesichts der Änderungen der einschlägigen Bestimmungen des Rechts des Vereinigten Königreichs ([10]) der Ausschluss personenbezogener Daten, die für die Zwecke der Einwanderungskontrolle des Vereinigten Königreichs übermittelt werden oder anderweitig in den Anwendungsbereich der Ausnahme von bestimmten Rechten betroffener Personen für die Zwecke der Aufrechterhaltung einer wirksamen Einwanderungskontrolle (im Folgenden „Ausnahme im Bereich der Einwanderung“) gemäß dem Anhang 2 Artikel 4 Absatz 1 des britischen Datenschutzgesetzes fallen, vom Anwendungsbereich des Durchführungsbeschlusses (EU) 2021/1772 nicht mehr gerechtfertigt ist, wie in Erwägungsgrund 37 des vorliegenden Beschlusses erläutert.

([6]) Abrufbar unter folgendem Link: https://bills.parliament.uk/bills/3825/news.

([7]) Durchführungsbeschluss (EU) 2025/1226 der Kommission vom 24. Juni 2025 zur Änderung des Durchführungsbeschlusses (EU) 2021/1772 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (ABl. L, 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) Der Data (Use and Access) Act erhielt am 19. Juni 2025 die Königliche Zustimmung.

([9]) Artikel 45 Absatz 4 der Verordnung (EU) 2016/679.

([10]) Im Mai 2021 hatte der Court of Appeal von England und Wales die damals in Anhang 2 Paragraf 4 Absatz 1 des britischen Data Protection Act formulierte Ausnahme im Bereich der Einwanderung für unvereinbar mit den Rechtsvorschriften des Vereinigten Königreichs befunden, da die Gesetzgebungsmaßnahme keine spezifischen Bestimmungen über die in Artikel 23 Absatz 2 UK GDPR aufgeführten Garantien enthielt. Um dem Urteil nachzukommen, überarbeitete die Regierung des Vereinigten Königreichs die Ausnahme im Bereich der Einwanderung durch die Verabschiedung der Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022. Die überarbeitete Ausnahme wurde jedoch erneut mit der Begründung angefochten, dass sie nicht alle Anforderungen von Artikel 23 Absatz 2 UK GDPR erfülle. In einem Urteil vom 11. Dezember 2023 erklärte der Court of Appeal die überarbeitete Ausnahme im Bereich der Einwanderung erneut für unvereinbar mit Artikel 23 Absatz 2 UK GDPR. Zum Zweck der Einhaltung verabschiedete die Regierung des Vereinigten Königreichs dann die Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024, die am 8. März 2024 in Kraft getreten sind.

2. EINSCHLÄGIGE ENTWICKLUNGEN IN BEZUG AUF DIE VORSCHRIFTEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

2.1. Der Datenschutzrechtsrahmen des Vereinigten Königreichs

(9) Bei Erlass des Durchführungsbeschlusses (EU) 2021/1772 bestand der Rechtsrahmen für den Schutz personenbezogener Daten im Vereinigten Königreich aus folgenden Rechtsakten:

— Die UK GDPR ([11]), wie sie durch den European Union (Withdrawal) Act 2018 ([12]) in das Recht des Vereinigten Königreichs übernommen und durch die Data Protection, Privacy and Electronic Communications (Amendments usw.) (EU Exit) Regulations 2019 (DPPEC Regulations) ([13]) geändert wurde,

— der DPA 2018 ([14]), wie er durch die DPPEC Regulations geändert wurde.

(10) Diese beiden Gesetze, die die entsprechenden in der Europäischen Union geltenden Vorschriften genau wiedergaben, bilden zwar weiterhin die Datenschutzvorschriften des Vereinigten Königreichs, wurden seither jedoch nur in begrenztem Umfang geändert, worin sich der Umstand niederschlägt, dass das Vereinigte Königreich nicht mehr dem Recht der Europäischen Union unterliegt.

(11) Erstens wurde im Retained EU Law (Revocation and Reform) Act 2023 (REUL Act) ([15]) klargestellt, dass die allgemeinen Grundsätze des EU-Rechts nach Ende 2023 nicht mehr Teil des innerstaatlichen Rechts des Vereinigten Königreichs sind ([16]). Darüber hinaus sind die Gerichte des Vereinigten Königreichs nicht mehr verpflichtet, unverändertes „assimiliertes Recht", das zuvor als „beibehaltenes EU-Recht" bezeichnet wurde, im Einklang mit den allgemeinen Grundsätzen des EU-Rechts auszulegen, sondern dieses Recht ist vielmehr im Einklang mit dem innerstaatlichen Recht des Vereinigten Königreichs auszulegen ([17]). Unverändertes „übernommenes Recht" ist jedoch weiterhin von den zuständigen Gerichten des Vereinigten Königreichs im Einklang mit der einschlägigen Rechtsprechung des Europäischen Gerichtshofs auszulegen, die vor dem Ende des Übergangszeitraums ([18]) erlassen wurde, wie auch in Erwägungsgrund 13 des Durchführungsbeschlusses (EU) 2021/1772 ausgeführt. Der DPA 2018 wurde durch den Data (Use and Access) Act geändert, um die Auswirkungen des REUL Act auf die Datenschutzvorschriften des Vereinigten Königreichs klarzustellen. Beispielsweise sieht Paragraf 183A Absatz 1 des DPA 2018 als allgemeine Regel vor, dass alle neuen Rechtsvorschriften, die am oder nach dem 20. August 2025 erlassen werden und neue Pflichten oder Befugnisse zur Verarbeitung personenbezogener Daten einführen, als den Datenschutzvorschriften des Vereinigten Königreichs unterliegend gelten. Dies bedeutet, dass der Datenschutzrahmen des Vereinigten Königreichs weiterhin anderen Rechtsvorschriften vorgeht. Gemäß

([11]) General Data Protection Regulation, abrufbar unter folgendem Link: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) The European Union (Withdrawal) Act 2018, abrufbar unter dem Link https://www.legislation.gov.uk/ukpga/2018/16/contents, aufgenommen in die Rechtsvorschriften der Union, die am Ende der Übergangszeit durch Aufnahme in das Recht des Vereinigten Königreichs unmittelbar gültig wurden. Dieses beibehaltene Unionsrecht („retained EU law") umfasste die Verordnung (EU) 2016/679 in allen ihren Teilen, einschließlich ihrer Erwägungsgründe (siehe Explanatory Notes to the European Union (Withdrawal) Act 2018, Nummer 83, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Im Einklang mit diesem Gesetz muss das unverändert beibehaltene Unionsrecht von den Gerichten des Vereinigten Königreichs gemäß der einschlägigen Rechtsprechung des Gerichtshofs der Europäischen Union und den allgemeinen Grundsätzen des Unionsrechts ausgelegt werden, so wie sie unmittelbar vor dem Ende des Übergangszeitraums gegolten haben (bezeichnet als „beibehaltene EU-Rechtsprechung" („retained EU case law") bzw. als „beibehaltene allgemeine Grundsätze des EU-Rechts" („retained general principles of EU law").

([13]) The Data Protection, Privacy and Electronic Communications (Amendments usw.) (EU Exit) Regulations 2019, abrufbar unter dem Link https://www.legislation.gov.uk/uksi/2019/419/contents/made, geändert durch die DPPEC Regulations 2020, abrufbar unter dem Link https://www.legislation.gov.uk/ukdsi/2020/9780348213522. Durch die DPPEC Regulations wird die Verordnung (EU) 2016/679 geändert, die durch den European Union (Withdrawal) Act 2018, den DPA 2018 und andere Datenschutzvorschriften in das britische Recht übernommen wurde, um sie an den nationalen Kontext anzupassen.

([14]) Data Protection Act 2018, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/12/contents. Vor dem Austritt des Vereinigten Königreichs aus der Europäischen Union und während des Übergangszeitraums erließ der DPA Im Jahr 2018, soweit nach der Verordnung (EU) 2016/679 zulässig, nationale Vorschriften zur Präzisierung und Beschränkung der Anwendung der Vorschriften der Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([15]) Abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) Paragraf 5 des European Union (Withdrawal) Act 2018 in der durch den REUL Act geänderten Fassung.

([17]) Paragraf 5 Absatz A2 des European Union (Withdrawal) Act 2018 in der durch das REUL-Gesetz geänderten Fassung.

([18]) Paragraf 6 Absätze 3 und 7 des European Union (Withdrawal) Act 2018 in der durch den REUL Act geänderten Fassung.

Paragraf 183A Absatz 2 Buchstabe b DPA 2018 kann diese Vermutung unangewendet bleiben, wenn das Parlament des Vereinigten Königreichs dies unter Wahrung der parlamentarischen Souveränität bewusst und ausdrücklich in einer Rechtsvorschrift festlegt. Darüber hinaus stellt Paragraf 186 Absatz 2A des DPA 2018 klar, dass die in Paragraf 186 Absatz 3 des DPA 2018 aufgeführten Beschränkungen der Rechte der betroffenen Person nicht durch Paragraf 186 Absatz 1 des DPA 2018 außer Kraft gesetzt werden, der vorsieht, dass Rechtsvorschriften, die die Offenlegung von Informationen verbieten oder einschränken, bestimmte Datenschutzrechte nicht außer Kraft setzen. Dadurch wird sichergestellt, dass beispielsweise die im DPA 2018 festgelegten Beschränkungen der Rechte betroffener Personen nicht selbst unter die allgemeine Vorrangregelung in Paragraf 186 Absatz 1 des DPA 2018 fallen.

(12) Zweitens wurden die Datenschutzvorschriften des Vereinigten Königreichs seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 durch die Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023 geändert ([19]). In diesen Regulations werden Verweise auf Grundrechte oder Grundfreiheiten in der UK GDPR und im DPA 2018 (die zuvor so definiert wurden, dass sie die Grundrechte und Grundfreiheiten der EU abdecken ([20])) als Bezugnahmen auf Rechte im Rahmen der Europäischen Menschenrechtskonvention definiert, die im Rahmen des Human Rights Act 1998 im innerstaatlichen Recht des Vereinigten Königreichs umgesetzt wurden ([21]). Mit dem Human Rights Act 1998 wurden die in der Europäischen Menschenrechtskonvention verbürgten Rechte in das Recht des Vereinigten Königreichs übernommen. Durch den Human Rights Act werden jeder Person die Grundrechte und -freiheiten gewährt, die in den Artikeln 2 bis 12 und 14 der Europäischen Menschenrechtskonvention, in den Artikeln 1, 2 und 3 ihres Ersten Protokolls und in Artikel 1 ihres Dreizehnten Protokolls in Verbindung mit den Artikeln 16, 17 und 18 dieser Konvention vorgesehen sind. Dazu zählen das Recht auf Achtung des Privat- und Familienlebens (einschließlich des Schutzes personenbezogener Daten als Teil dieses Rechts) sowie das Recht auf ein faires Verfahren ([22]).

(13) Schließlich wurden die UK GDPR und der DPA 2018 gezielten Reformen unterzogen, die in den Teilen 5 und 6 des Data (Use and Access) Act festgehalten sind. Während der Anwendungsbereich des Data (Use and Access) Act weit über den Schutz personenbezogener Daten hinaus geht, sind für mehrere Aspekte der Datenschutzregelung begrenzte Änderungen vorgesehen, darunter die Vorschriften für eine Datenverarbeitung zum Zwecke wissenschaftlicher Forschung, die Rechtsgrundlagen für eine Datenverarbeitung, die Vorschriften zum Zweckbindungsprinzip und die Bedingungen für eine automatisierte Entscheidungsfindung. Darüber hinaus werden mit dem Data (Use and Access) Act Änderungen an der Leitungsstruktur des ICO vorgenommen. Sobald diese Maßnahmen umgesetzt sind, werden sie das ICO durch eine neue Einrichtung, die Informationskommission, ersetzen. Die Rolle und die Aufgaben der Regulierungsbehörde als unabhängige Datenschutzaufsichtsbehörde im Vereinigten Königreich bleiben unverändert. Mit dem Gesetz werden auch neue Durchsetzungsbefugnisse für die Regulierungsbehörde eingeführt.

(14) Mit diesem Beschluss werden legislative, regulatorische und sonstige Entwicklungen bewertet, die für die Schlussfolgerung zum Schutzniveau des Vereinigten Königreichs gemäß dem Durchführungsbeschluss (EU) 2021/1772 maßgeblich sind. Die Bewertung im Durchführungsbeschluss (EU) 2021/1772 gilt weiterhin für diejenigen Aspekte des Datenschutzrahmens des Vereinigten Königreichs, die seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 nicht geändert oder von anderen Entwicklungen beeinflusst wurden.

(15) Die legislativen, regulatorischen und sonstigen relevanten Entwicklungen werden in den folgenden Abschnitten auf der Grundlage des Angemessenheitsstandards eingehend analysiert, wonach die Kommission feststellen muss, ob das betreffende Drittland ein Schutzniveau gewährleistet, das dem in der Europäischen Union gewährleisteten Schutzniveau „der Sache nach gleichwertig" ist ([23]). Der Gerichtshof der Europäischen Union hat klargestellt, dass es dazu keines identischen Schutzniveaus bedarf ([24]). Insbesondere können sich die Mittel, auf die das betreffende Drittland für den Schutz personenbezogener Daten zurückgreift, von denen unterscheiden, die in der Union herangezogen werden, sofern sie sich in der Praxis als wirksam erweisen, um ein angemessenes Schutzniveau zu gewährleisten ([25]). Daher erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den Vorschriften der Union. Maßgeblich ist vielmehr, ob das ausländische Rechtssystem insgesamt durch den materiellen Gehalt der Datenschutzrechte sowie deren wirksame Umsetzung, Überwachung und Durchsetzung das erforderliche Schutzniveau gewährleistet ([26]).

([19]) Abrufbar unter folgendem Link: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) Die Grundrechte und Grundfreiheiten der EU waren durch Paragraf 4 des European Union (Withdrawal) Act 2018, der Ende 2023 durch den REUL Act aufgehoben wurde, im Recht des Vereinigten Königreichs beibehalten worden.

([21]) Paragraf 2 Absatz 3 der Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023.

([22]) Artikel 6, 8, 10 und 13 EMRK (siehe auch Anhang 1 des Human Rights Act 1998).

([23]) Erwägungsgrund 104 der Verordnung (EU) 2016/679.

([24]) Rechtssache C-362/14, *Schrems* (im Folgenden „*Schrems I*"), ECLI:EU:C:2015:650, Rn. 73.

([25]) *Schrems I*, Rn. 74.

([26]) Siehe Mitteilung der Kommission an das Europäische Parlament und den Rat „Austausch und Schutz personenbezogener Daten in einer globalisierten Welt" COM(2017) 7 vom 10.1.2017, Paragraf 3.1, S. 6-7, abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017DC0007&from=DE.

2.1.1. *Begriffsbestimmungen*

(16) Grundlegende Datenschutzkonzepte, die die Terminologie der Richtlinie (EU) 2016/679 wiedergeben, gelten in der Datenschutzregelung des Vereinigten Königreichs weiterhin. Diese Konzepte wurden im Erwägungsgrund 23 des Durchführungsbeschlusses (EU) 2021/1772 bewertet.

(17) Während der Data (Use and Access) Act die überwiegende Mehrheit der Begriffsbestimmungen unverändert lässt, wurden in Artikel 4 Absätze 2, 3, 4 und 5 der UK GDPR spezifische Begriffsbestimmungen für die Verarbeitung personenbezogener Daten für wissenschaftliche, historische und statistische Zwecke eingeführt. Absatz 2 definiert die „Verarbeitung für wissenschaftliche Zwecke" als die Verarbeitung personenbezogener Daten für Zwecke der Forschung, die vernünftigerweise als wissenschaftlich beschrieben werden kann. Diese Forschungsarbeiten können öffentlich oder privat finanziert und entweder als gewerbliche oder nichtgewerbliche Tätigkeit durchgeführt werden. Entsprechend dem Inhalt von Erwägungsgrund 159 der Verordnung (EU) 2016/679 enthält Absatz 3 eine nicht erschöpfende Liste von Beispielen für Forschungstätigkeiten, die wissenschaftlichen Zwecken dienen, einschließlich technologischer Entwicklung, Demonstration, Grundlagenforschung und angewandter Forschung. In Absatz 4 wird klargestellt, dass „historische Forschung" auch genealogische Forschung umfasst, was in Erwägungsgrund 160 der Verordnung (EU) 2016/679 ebenfalls als historischer Zweck anerkannt wird. Schließlich ist in Absatz 5 die Verarbeitung zu statistischen Zwecken als die Verarbeitung von Daten für statistische Erhebungen oder zur Erstellung statistischer Ergebnisse definiert, wobei die Daten so aggregiert werden, dass sie keine personenbezogenen Daten mehr darstellen. Darüber hinaus dürfen die verarbeiteten Daten oder daraus resultierenden Informationen nicht dazu verwendet werden, Entscheidungen zu treffen oder Maßnahmen zu ergreifen, die sich gegen eine bestimmte Person richten. Diese Definition steht im Einklang mit dem in Erwägungsgrund 162 der Verordnung (EU) 2016/679 dargelegten Verständnis der statistischen Zwecke.

(18) Zusammenfassend lässt sich festhalten, dass mit den Änderungen an Artikel 4 der UK GDPR zwar spezifische Definitionen der Datenverarbeitung für wissenschaftliche, historische und statistische Zwecke hinzugefügt werden, diese Begriffsbestimmungen jedoch mit Wortlaut und Geist der Verordnung (EU) 2016/679 im Einklang stehen, wie aus den oben genannten Erwägungsgründen 159, 160 und 162 hervorgeht.

(19) Mit der Einfügung von Absatz 6 in Artikel 4 der UK GDPR hat der Data (Use and Access) Act zudem einen spezifischen Rahmen für die Einholung der Einwilligung der betroffenen Person zur Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke geschaffen. In sehr ähnlichem Wortlaut wie Erwägungsgrund 33 der Verordnung (EU) 2016/679, in dem eingeräumt wird, dass im Bereich der wissenschaftlichen Forschung nicht immer eine Einwilligung für einen bestimmten Verarbeitungszweck eingeholt werden kann, ermöglicht die neue Bestimmung umfassendere Formen der Einwilligung, indem darin vorgesehen ist, dass betroffene Personen auch dann eine gültige Einwilligung erteilen können, wenn die genauen Zwecke der Forschung zum Zeitpunkt der Datenerhebung nicht vollständig identifiziert werden können, sofern die Einholung der Einwilligung mit den allgemein anerkannten ethischen Standards für den jeweiligen Forschungsbereich im Einklang steht. In jedem Fall müssen betroffene Personen die Möglichkeit haben, in die Verarbeitung personenbezogener Daten nur für bestimmte Teile der Forschung einzuwilligen, sofern dies möglich ist.

(20) Schließlich wurden im Data (Use and Access) Act die zuvor in Artikel 89 UK GDPR und Paragraf 19 DPA 2018 enthaltenen Garantien für die Datenverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche, historische oder statistische Forschungszwecke in einem neuen Kapitel 8A der UK GDPR näher ausgeführt ([27]). Diese Garantien ähneln den in Artikel 89 der Verordnung (EU) 2016/679 vorgeschriebenen Garantien und umfassen die Anforderung, technische und organisatorische Maßnahmen zu ergreifen, um die Einhaltung des Grundsatzes der Datenminimierung sicherzustellen.

2.2. **Garantien, Rechte und Pflichten**

2.2.1. *Rechtmäßigkeit der Verarbeitung und Verarbeitung nach Treu und Glauben*

(21) Wie in den Erwägungsgründen 24 bis 26 des Durchführungsbeschlusses (EU) 2021/1772 bewertet, schreibt der Datenschutzrahmen des Vereinigten Königreichs weiterhin vor, dass die Verarbeitung von Daten rechtmäßig und nach Treu und Glauben erfolgen muss.

([27]) Artikel 84A bis 84D UK GDPR, eingeführt durch Paragraf 86 des Data (Use and Access) Act.

(22) Die Grundsätze der Rechtmäßigkeit und der Verarbeitung nach Treu und Glauben sowie die Gründe für eine rechtmäßige Verarbeitung werden im Recht des Vereinigten Königreichs weiterhin durch Artikel 5 Absatz 1 Buchstabe a und Artikel 6 Absatz 1 UK GDPR gewährleistet, wie im Durchführungsbeschluss (EU) 2021/1772 bewertet. Während diese Bestimmungen weitgehend mit den entsprechenden Bestimmungen der Verordnung (EU) 2016/679 übereinstimmen ([28]), wird mit dem Data (Use and Access) Act zunächst Artikel 6 Absatz 1 UK GDPR geändert, indem ein zusätzlicher rechtmäßiger Grund für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe ea eingeführt wird ([29]). Nach dieser Bestimmung ist die Verarbeitung rechtmäßig, wenn und soweit sie „für die Zwecke eines anerkannten berechtigten Interesses erforderlich ist". Anders als beim Rechtmäßigkeitsgrund des berechtigten Interesses gemäß Artikel 6 Absatz 1 Buchstabe f der UK GDPR erfordert der neu eingeführte Rechtmäßigkeitsgrund des anerkannten berechtigten Interesses keine einzelfallbezogene Abwägung zwischen den berechtigten Interessen des Verantwortlichen und den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person. Ziel ist es, Verantwortlichen, die keine öffentlichen Stellen sind, eine größere Rechtssicherheit zu bieten. Stattdessen legt der neu eingeführte Artikel 6 Absatz 5 UK GDPR fest, dass die Verarbeitung nur dann für die Zwecke eines anerkannten berechtigten Interesses erforderlich ist, wenn eine Bedingung in Anhang 1 erfüllt ist ([30]), in dem die Situationen aufgeführt sind, in denen die Verarbeitung für die Zwecke eines anerkannten berechtigten Interesses als notwendig gilt, beispielsweise wenn sie auf Ersuchen einer Behörde erfolgt, die die Daten zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe benötigt, für die eine Rechtsgrundlage gemäß Artikel 6 Absatz 3 UK GDPR besteht, oder wenn die Verarbeitung erforderlich ist, um die nationale Sicherheit, den Schutz der öffentlichen Sicherheit oder die Verteidigung zu gewährleisten, auf einen Notfall zu reagieren, Straftaten aufzudecken, zu untersuchen oder zu verhindern oder schutzbedürftige Personen zu schützen ([31]).

(23) Während mit dem Data (Use and Access) Act somit die Liste der Rechtsgrundlagen für die Verarbeitung personenbezogener Daten, die dem Verantwortlichen zur Verfügung stehen, erweitert wird, unterliegt die neu eingeführte Rechtsgrundlage eines anerkannten berechtigten Interesses mehreren wichtigen Beschränkungen. Erstens sind die anerkannten berechtigten Interessen auf bestimmte, im Gesetz abschließend aufgeführte Sachverhalte beschränkt. Zweitens können sich öffentliche Stellen bei der Erfüllung ihrer Aufgaben nicht auf diese Rechtsgrundlage berufen ([32]). Drittens betrifft sie nur Bereiche, in denen ein eindeutiges öffentliches Interesse an der Verarbeitungstätigkeit besteht (gemäß den in Anhang 1 festgelegten Bedingungen), das heißt, wenn die Verarbeitung den in Artikel 23 UK GDPR aufgeführten Zwecken dient (entsprechend Artikel 23 der Verordnung (EU) 2016/679) und sich somit nicht für kommerzielle Zwecke stützen lässt. Viertens räumt der Data (Use and Access) Act dem Secretary of State zwar das Recht ein, die Liste in Anhang 1 mittels Verordnung ([33]) zu ändern, doch darf der

([28]) Zur Klarstellung wird mit dem Data (Use and Access) Act in Artikel 6 UK GDPR auch ein neuer Absatz eingeführt, der Beispiele für Arten der Verarbeitung enthält, die als für die Zwecke des berechtigten Interesses im Sinne von Artikel 6 Absatz 1 Buchstabe f UK GDPR erforderlich angesehen werden können. Diese Beispiele (Direktwerbung, Übermittlung von Daten innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke und die Sicherheit von Netzen und Informationssystemen) werden auch in den Erwägungsgründen 47 und 48 der Verordnung (EU) 2016/679 als Situationen genannt, in denen die Verarbeitung als im berechtigten Interesse des Verantwortlichen liegend betrachtet würde.

([29]) Paragraf 70 Absatz 2 Buchstabe b des Data (Use and Access) Act Paragraf 70 Absatz 5 des Data (Use and Access) Act hat das Widerspruchsrecht nach Artikel 21 UK GDPR auf den neuen Artikel 6 Absatz 1 Buchstabe ea UK GDPR ausgeweitet.

([30]) Paragraf 70 Absatz 4 des Data (Use and Access) Act.

([31]) Siehe Anhang 4 des Data (Use and Access) Act. Nach Angaben der britischen Behörden gehören zu den Beispielsituationen, in denen nicht-öffentliche Stellen personenbezogene Daten verarbeiten müssen, um Straftaten zu verhindern oder aufzudecken, etwa ein Unternehmen, das von Versuchen erfährt, unrechtmäßig in seine Computersysteme einzudringen, oder eine Bank bzw. ein Finanzinstitut, das von betrügerischen Versuchen erfährt, ein Konto zu eröffnen. Die Verarbeitung personenbezogener Daten durch eine nichtöffentliche Stelle kann beispielsweise zum Schutz der nationalen Sicherheit oder Verteidigung erforderlich sein, wenn eine gewerbliche Organisation den Verdacht hat, dass die Online-Aktivität eines Kunden auf eine Beteiligung an terroristischen Aktivitäten hindeutet. Das ICO arbeitet derzeit an spezifischen Leitlinien zu diesem Thema, einschließlich einer Definition der einschlägigen Begriffe. Beispielsweise wird darin ausgeführt, dass unter „nationale Sicherheit" wahrscheinlich die Sicherheit und das Wohlergehen des gesamten Vereinigten Königreichs, seiner Bevölkerung, seiner Institutionen und seines Regierungssystems zu verstehen ist. Siehe den Entwurf der ICO-Leitlinien zum anerkannten berechtigten Interesse, der zur öffentlichen Konsultation veröffentlicht wurde und unter folgendem Link abrufbar ist: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Artikel 6 Absatz 1 letzter Unterabsatz, geändert durch Paragraf 70 Absatz 2 Buchstabe c des Data (Use and Access) Act.

([33]) Vor dem Erlass von Verordnungen muss der Secretary of State die Auswirkungen etwaiger Änderungen auf die Interessen, Grundrechte und Freiheiten der betroffenen Personen sowie die Tatsache berücksichtigen, dass Kinder (gegebenenfalls) besonderen Schutz in Bezug auf ihre personenbezogenen Daten benötigen. Die Verordnungen müssen durch von Verordnungen abgeleitete Rechtsvorschriften erlassen werden und unterliegen dem positiven Abstimmungsverfahren, was bedeutet, dass sie vom Parlament des Vereinigten Königreichs aktiv gebilligt werden müssen. Paragraf 70 Absatz 4 Unterabsatz 8 des Data (Use and Access) Act.

Secretary of State eine solche Verordnung nur nach Anhörung der ICO ([34])erlassen und ein anerkanntes berechtigtes Interesse nur dann in diese Liste aufnehmen, wenn diese Verarbeitung erneut erforderlich ist, um ein in Artikel 23 Absatz 1 Buchstaben c bis j der UK GDPR aufgeführtes Ziel des öffentlichen Interesses zu wahren ([35]). Schließlich müssen, wie auch in den Leitlinien des ICO bestätigt wird ([36]), Verantwortliche, die sich auf ein anerkanntes berechtigtes Interesse als Rechtsgrundlage stützen, alle anderen Anforderungen der UK GDPR erfüllen, einschließlich der Gewährleistung, dass die Verarbeitung zur Erreichung des berechtigten Interesses erforderlich und verhältnismäßig ist.

(24) Zweitens wird im Data (Use and Access) Act in Artikel 6 Absatz 3, Artikel 9 Absatz 2 Buchstabe g und Artikel 10 Absatz 1 UK GDPR, die den jeweiligen Bestimmungen der Verordnung (EU) 2016/679 entsprechen, klargestellt, dass die Grundlage für die Verarbeitung personenbezogener Daten, besonderer Kategorien personenbezogener Daten und personenbezogener Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten im Einklang mit einer rechtlichen Verpflichtung oder für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe nicht nur auf das innerstaatliche Recht, sondern auch auf das einschlägige Völkerrecht gestützt werden kann ([37]). Das einschlägige Völkerrecht wird dann durch den neu eingeführten Artikel 9A UK GDPR in Verbindung mit Anhang A1 auf ein einziges Abkommen beschränkt, nämlich auf das am 3. Oktober 2019 unterzeichnete Abkommen zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugang zu elektronischen Daten zur Bekämpfung von schwerer Kriminalität (im Folgenden das „Abkommen zwischen dem Vereinigten Königreich und den USA“) ([38]). Die in diesem Abkommen vorgesehenen Garantien wurden in den Erwägungsgründen 153 bis 155 des Durchführungsbeschlusses (EU) 2021/1772 bewertet und ihre Umsetzung wird in den Erwägungsgründen 87 bis 93 des vorliegenden Beschlusses analysiert.

2.2.2. *Verarbeitung besonderer Kategorien personenbezogener Daten*

(25) Wie in den Erwägungsgründen 27 bis 42 des Durchführungsbeschlusses (EU) 2021/1772 bewertet, bietet der Datenschutzrahmen des Vereinigten Königreichs weiterhin spezifische Garantien für besondere Datenkategorien.

(26) Sowohl die Begriffsbestimmungen besonderer Kategorien personenbezogener Daten als auch die spezifischen Vorschriften für die Verarbeitung dieser Datenkategorien in der UK GDPR und im DPA 2018 behalten ihre Gültigkeit. Gleichzeitig überträgt der Data (Use and Access) Act dem Secretary of State neue Regelungsbefugnisse, um besondere Kategorien von Daten hinzuzufügen, die Bedingungen für ihre Nutzung anzupassen und erforderlichenfalls neue Begriffsbestimmungen hinzuzufügen ([39]). Wichtig ist, dass es dem Secretary of State nicht gestattet ist, bestehende besondere Kategorien von Daten zu streichen oder abzuändern oder die Bedingungen für die Verarbeitung dieser Kategorien zu ändern ([40]). Die neu eingeführte Regelungsbefugnis ermöglicht es der Regierung somit lediglich, neue Kategorien sensibler Daten hinzuzufügen und die Bedingungen für die Verarbeitung dieser Kategorien festzulegen, damit die Regierung bei Bedarf auf künftige technologische und gesellschaftliche Entwicklungen reagieren kann.

(27) Daher berühren diese Änderungen nicht das Schutzniveau für besondere Kategorien personenbezogener Daten, das im Durchführungsbeschluss (EU) 2021/1772 als der Sache nach gleichwertig mit dem Schutzniveau innerhalb der EU angesehen wird.

([34]) Paragraf 182 Absatz 2 DPA 2018.
([35]) Paragraf 70 Absatz 4 Unterabsatz 9 des Data (Use and Access) Act.
([36]) Siehe die ICO-Leitlinien zu berechtigten Interessen, abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.
([37]) Paragraf 72 des Data (Use and Access) Act.
([38]) Abkommen zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugang zu elektronischen Daten zur Bekämpfung von schwerer Kriminalität, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.
([39]) Paragraf 74 des Data (Use and Access) Act. Solche Regelungen unterliegen dem positiven Abstimmungsverfahren, d. h., es ist dafür eine aktive Zustimmung des Parlaments des Vereinigten Königreichs erforderlich.
([40]) Siehe den neuen Artikel 11A Absatz 1 Buchstabe b und Absatz 2 UK GDPR sowie die Erläuterungen zum Data (Use and Access) Bill, Paragraf 571, abrufbar unter folgendem Link: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3. *Zweckbindung*

(28) Durch die Regelung des Vereinigten Königreichs zum Schutz personenbezogener Daten wird weiterhin verlangt, dass Daten für einen bestimmten Zweck verarbeitet und anschließend nur insoweit verwendet werden, als dies mit dem ursprünglichen Zweck der Verarbeitung vereinbar ist, wie in den Erwägungsgründen 43 bis 48 des Durchführungsbeschlusses (EU) 2021/1772 bewertet.

(29) Erstens werden mit dem Data (Use and Access) Act nur wenige gezielte Änderungen des Grundsatzes der Zweckbindung gemäß Artikel 5 Absatz 1 Buchstabe b UK GDPR vorgenommen. Mit diesen Änderungen wird die Anwendung dieses Grundsatzes präzisiert, ohne dass der Inhalt geändert wird. Paragraf 71 Absätze 1, 2 und 3 des Data (Use and Access) Act stellen klar, dass der Grundsatz der Zweckbindung gilt, unabhängig davon, ob die Daten bei der betroffenen Person oder auf andere Weise erhoben wurden, dass er nur Anwendung findet, wenn personenbezogene Daten durch oder im Auftrag desselben Verantwortlichen weiterverarbeitet werden (d. h. nicht bei einem Wechsel des Verantwortlichen), und dass eine Verarbeitung nicht allein deshalb rechtmäßig ist, weil sie mit den ursprünglichen Erhebungszwecken vereinbar ist.

(30) Zweitens werden im Data (Use and Access) Act die Vorschriften für die Weiterverarbeitung personenbezogener Daten präzisiert, indem sie in dem neu hinzugefügten Artikel 8A der UK GDPR zusammengefasst werden, in dem die vollständige Regelung für die Weiterverarbeitung personenbezogener Daten festgelegt ist. In Artikel 8A Absatz 2 UK GDPR sind die Elemente aufgeführt, die bei der Feststellung zu berücksichtigen sind, ob ein neuer Verarbeitungszweck mit dem ursprünglichen Zweck vereinbar ist. Diese Elemente wurden zuvor in Artikel 6 Absatz 4 UK GDPR aufgeführt, der Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 ([41]) entspricht. In Artikel 8A Absatz 3 UK GDPR sind in einer Bestimmung die Fälle zusammengefasst, in denen die Verarbeitung personenbezogener Daten für einen neuen Zweck als mit dem ursprünglichen Zweck vereinbar zu behandeln ist. Diese Fälle umfassen Situationen, in denen die betroffene Person in die Verarbeitung personenbezogener Daten für den neuen Zweck einwilligt oder die Verarbeitung zur Wahrung eines in Artikel 23 Absatz 1 genannten Ziels erforderlich ist ([42]), wenn die Verarbeitung zu Zwecken der wissenschaftlichen oder historischen Forschung, der Archivierung im öffentlichen Interesse oder zu statistischen Zwecken erfolgt ([43]). Schließlich wird im Data (Use and Access) Act klargestellt, dass jede Verarbeitung, mit der sichergestellt werden soll, dass die Verarbeitung den in Artikel 5 Absatz 1 der UK GDPR festgelegten Datenschutzgrundsätzen entspricht, oder der Nachweis, dass dies der Fall ist, als mit dem ursprünglichen Zweck vereinbar angesehen wird. Die oben genannten Situationen entsprechen weiterhin der Weiterverarbeitung, die auch in der Verordnung (EU) 2016/679 als vereinbar erachtet wird.

(31) Drittens werden mit dem Data (Use and Access) Act in Artikel 8A Absatz 3 Buchstabe d UK GDPR auch neue zusätzliche Situationen eingeführt, in denen die Weiterverarbeitung personenbezogener Daten für einen neuen Zweck als mit dem ursprünglichen Zweck vereinbar angesehen wird. Diese Situationen sind in Anhang 2 UK GDPR ([44]) aufgeführt und umfassen beispielsweise den Fall, dass die Verarbeitung als Reaktion auf ein Ersuchen einer Behörde erfolgt, die die Daten zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe benötigt, für die eine Rechtsgrundlage gemäß Artikel 6 Absatz 3 UK DSGVO besteht, sofern die Verarbeitung für den Schutz der öffentlichen Sicherheit, die Reaktion auf einen Notfall, die Aufdeckung, Untersuchung oder Verhütung von Straftaten, den Schutz der lebenswichtigen Interessen der betroffenen Person oder anderer Personen, den Schutz schutzbedürftiger Personen oder für steuerliche Zwecke bzw. zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist ([45]).

(32) Während durch den Data (Use and Access) Act somit die Liste der Fälle erweitert wird, in denen die Weiterverarbeitung für einen anderen Zweck als mit dem ursprünglichen Verarbeitungszweck vereinbar angesehen wird, unterliegt diese Ausweitung erheblichen Beschränkungen. Erstens ist sie auf bestimmte Sachverhalte beschränkt, die im Gesetz erschöpfend aufgezählt sind. Zweitens betrifft sie nur Bereiche, in denen ein eindeutiges öffentliches Interesse an der Verarbeitung besteht, d. h., in denen die Weiterverarbeitung den in Artikel 23 UK GDPR (der

([41]) Wie in der Verordnung (EU) 2016/679 umfassen diese Elemente jede Verbindung zwischen dem ursprünglichen und dem neuen Zweck, den Kontext, in dem die personenbezogenen Daten erhoben wurden, einschließlich der Beziehung zwischen der betroffenen Person und dem Verantwortlichen, die Art der Verarbeitung und möglicherweise enthaltene besondere Kategorien von Daten, die möglichen Folgen der beabsichtigten Verarbeitung für die betroffene Person und das Vorhandensein geeigneter Garantien.

([42]) Siehe auch Artikel 6 Absatz 4 der Verordnung (EU) 2016/679.

([43]) Erwägungsgrund 50 der Verordnung (EU) 2016/679.

([44]) Anhang 2 wird durch Anhang 5 des Data (Use and Access) Act in die UK GDPR eingefügt, siehe Paragraf 71 Absatz 6 dieses Gesetzes.

([45]) Siehe Anhang 5 des Data (Use and Access) Act.

Artikel 23 der Verordnung (EU) 2016/679 entspricht) aufgeführten Zielen dient. Daher kann sie nicht für kommerzielle Zwecke geltend gemacht werden. Drittens räumt der Data (Use and Access) Act dem Secretary of State zwar das Recht ein, die Liste in Anhang 2 mittels Verordnung zu ändern ([46]), doch darf der Secretary of State dieser Liste nur dann ein anerkanntes berechtigtes Interesse hinzufügen, wenn diese Verarbeitung erneut erforderlich ist, um ein in Artikel 23 Absatz 1 Buchstaben c bis j der UK GDPR aufgeführtes Ziel des öffentlichen Interesses zu wahren ([47]). Viertens gilt, wenn die Erhebung personenbezogener Daten durch den Verantwortlichen auf der Einwilligung der betroffenen Person beruht, die Verarbeitung für einen neuen Zweck in den in Anhang 2 aufgeführten Fällen nur dann als mit dem ursprünglichen Zweck vereinbar, wenn von dem Verantwortlichen nach vernünftigem Ermessen nicht erwartet werden kann, dass er eine neue Einwilligung der betroffenen Person einholt ([48]).

2.2.4. *Rechte des Einzelnen*

(33) Gemäß dem Rahmen des Vereinigten Königreichs für den Schutz personenbezogener Daten genießen die betroffenen Personen weiterhin ohne wesentliche Änderungen dieselben individuellen Rechte wie nach der Verordnung (EU) 2016/679 ([49]), die gegen den Verantwortlichen oder den Auftragsverarbeiter durchgesetzt werden können, insbesondere das Recht auf Auskunft über die Daten, das Recht auf Widerspruch gegen die Verarbeitung und das Recht auf Berichtigung und Löschung von Daten, wie in den Erwägungsgründen 51 bis 54 des Durchführungsbeschlusses (EU) 2021/1772 bewertet.

(34) Erstens werden im Data (Use and Access) Act bestimmte Modalitäten festgelegt, unter denen diese Rechte ausgeübt werden können. Einerseits werden darin durch eine Änderung von Artikel 12 und die Einführung eines neuen Artikels 12A der UK GDPR die Fristen festgelegt ([50]), innerhalb deren die Verantwortlichen auf die Anträge der betroffenen Person reagieren müssen. Insbesondere wird Artikel 12 UK GDPR dahin gehend geändert, dass der Verantwortliche nicht mehr verpflichtet ist, gemäß den Artikeln 15 bis 22 UK GDPR „innerhalb eines Monats nach Eingang des Antrags“ Informationen über die auf einen Antrag der betroffenen Person hin ergriffenen Maßnahmen (oder über die Gründe, aus denen keine Maßnahmen ergriffen wurden) vorzulegen, sondern „vor Ablauf der geltenden Frist“. Die geltende Frist wird in dem neu eingeführten Artikel 12A UK GDPR definiert als ein Zeitraum von einem Monat ab dem maßgeblichen Zeitpunkt, d. h. dem Zeitpunkt, zu dem der Verantwortliche den Antrag erhält, wenn der Verantwortliche Informationen erhält, die im Zusammenhang mit einem Ersuchen nach Artikel 12 Absatz 6 UK GDPR angefordert werden, oder wenn eine Gebühr entrichtet wurde, die im Zusammenhang mit dem Ersuchen nach Artikel 12 Absatz 5 UK GDPR erhoben wurde, je nachdem, welcher Zeitpunkt der spätere ist ([51]). Artikel 12A Absatz 3 ermöglicht es dem Verantwortlichen ferner, die geltende Frist um zwei weitere Monate zu verlängern, wenn dies aufgrund der Komplexität der Anträge der betroffenen Person oder der Anzahl solcher Anträge erforderlich ist. Andererseits wird Artikel 15 UK GDPR durch den Data (Use and Access) Act ausschließlich in Bezug auf das Recht auf Zugang zu Informationen und personenbezogenen Daten geändert, indem klargestellt wird, dass die Verantwortlichen nur angemessene und verhältnismäßige Nachforschungen zu den angeforderten Informationen und personenbezogenen Daten durchführen müssen ([52]). Es wird erwartet, dass die neue Bestimmung im Einklang mit der bestehenden Rechtsprechung ausgelegt wird, in der es heißt: „[…] was bei der Verhältnismäßigkeitsprüfung abgewogen wird, ist das Endziel der Suche, nämlich der potenzielle Nutzen, den die Bereitstellung der Informationen für die betroffene Person mit sich bringen könnte, im Vergleich zu den Mitteln, mit denen diese Informationen erlangt werden. Es wird in jedem Einzelfall zu prüfen sein, ob ein unverhältnismäßiger Aufwand erforderlich ist, um die Informationen zu finden und bereitzustellen, im Vergleich zu dem Nutzen, den sie der betroffenen Person bringen könnten“ ([53]).

([46]) Artikel 8A Absatz 5 Buchstabe b UK GDPR, eingeführt durch Paragraf 71 Absatz 1 des Data (Use and Access) Act.

([47]) Artikel 8A Absatz 6 Buchstabe b UK GDPR, eingeführt durch Paragraf 71 Absatz 1 des Data (Use and Access) Act.

([48]) Artikel 8A Absatz 4 Buchstabe b UK GDPR, eingeführt durch Paragraf 71 Absatz 1 des Data (Use and Access) Act.

([49]) Mit Paragraf 31 des Victims and Prisoners Act 2024 (VAP Act) wurde ein zusätzlicher Grund in das Recht auf Löschung gemäß Artikel 17 UK GDPR eingefügt, wonach betroffene Personen das Recht haben, von den Verantwortlichen die Löschung ihrer personenbezogenen Daten zu verlangen, wenn diese aufgrund einer unbegründeten Behauptung einer böswilligen Person über die betroffene Person verarbeitet wurden. Eine Person gilt als „böswillig“, wenn sie wegen einer Straftat nach Paragraf 31 Absatz 3 VAP Act (wie Belästigung) verurteilt wurde oder einer Stalking-Schutzanordnung unterliegt. Der VAP Act ist unter folgendem Link abrufbar: https://www.legislation.gov.uk/ukpga/2024/21/contents. Darüber hinaus wird mit Paragraf 77 des Data (Use and Access) Act das Recht auf Information gemäß Artikel 13 UK GDPR so geändert, dass der Verantwortliche die betroffene Person nicht mehr über die Weiterverarbeitung ihrer personenbezogenen Daten für einen neuen Zweck informieren muss, wenn es sich bei diesem Zweck um wissenschaftliche oder historische Forschung, Archivierung im öffentlichen Interesse oder einen statistischen Zweck handelt, die Verarbeitung gemäß den besonderen Schutzvorkehrungen des neuen Artikels 84B UK GDPR erfolgt und die Bereitstellung der Informationen unmöglich oder unverhältnismäßig wäre.

([50]) Paragraf 76 des Data (Use and Access) Act.

([51]) Artikel 12A Absätze 1 und 2 UK GDPR, eingeführt durch Paragraf 76 des Data (Use and Access) Act.

([52]) Artikel 15 Absatz 1A UK GDPR, eingeführt durch Paragraf 78 des Data (Use and Access) Bill.

([53]) Dawson-Dammer gegen Taylor Wessing LLP [2017] EWCA Civ 74.

(35) Während die Fristen für die Beantwortung von Anträgen der betroffenen Personen und die besonderen Pflichten der für die Verarbeitung Verantwortlichen in Bezug auf das Auskunftsrecht genauer geregelt sind, stellt das System des Vereinigten Königreichs weiterhin sicher, dass Anträge betroffener Personen innerhalb angemessener Fristen bearbeitet werden müssen, die auf der Grundlage objektiver Faktoren festgelegt werden. Darüber hinaus basieren die wesentlichen Pflichten des Verantwortlichen bei der Beantwortung von Auskunftsersuchen auf festgelegten Rechtsnormen, die auch die Interessen der betroffenen Person berücksichtigen. Schließlich ist bereits in den geltenden ICO-Leitlinien festgelegt, dass ein Verantwortlicher nicht verpflichtet ist, Suchmaßnahmen durchzuführen, die unangemessen oder im Verhältnis zur Bedeutung der Gewährung des Zugangs zu den Informationen unverhältnismäßig wären ([54]).

(36) Die Beschränkungen dieser Rechte des Einzelnen, die im DPA 2018 festgelegt sind und sich in den Rahmen von Artikel 23 UK GDPR einfügen, sowie die Beschränkungen und Garantien, die für die Anwendung dieser Beschränkungen maßgeblich sind, bestehen im Rechtsrahmen des Vereinigten Königreichs ([55]) weiterhin, wie in den Erwägungsgründen 55 bis 67 des Durchführungsbeschlusses (EU) 2021/1772 ausführlich beschrieben wird.

(37) Speziell in Bezug auf die Beschränkung personenbezogener Daten, die zum Zwecke der Aufrechterhaltung einer wirksamen Einwanderungskontrolle oder der Ermittlung oder Aufdeckung von Tätigkeiten verarbeitet werden, die die Aufrechterhaltung einer wirksamen Einwanderungskontrolle untergraben würden, soweit die Anwendung dieser Bestimmungen diese Angelegenheiten beeinträchtigen könnte (Ausnahme im Bereich der Einwanderung) ([56]), hat die Regierung des Vereinigten Königreichs Anhang 2 Absatz 4 des DPA 2018 durch die Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022 ([57]) und die The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024 ([58]), die die Regulations von 2022 ergänzen, geändert ([59]). Mit den Änderungen werden in Anhang 2 Paragraf 4A und 4B des DPA 2018 die nach Artikel 23 Absatz 2 UK GDPR erforderlichen Garantien für die Ausübung der Ausnahme im Bereich der Einwanderung aufgenommen. Es wird insbesondere vorgeschrieben, dass i) die Ausnahme im Bereich der Einwanderung von Fall zu Fall, getrennt für jede der einschlägigen Bestimmungen der UK GDPR und jeweils erneut geltend gemacht werden muss, wenn der Secretary of State erwägt, die Anwendung einer der einschlägigen Bestimmungen der UK GDPR außer Kraft zu setzen oder einzuschränken ([60]), ii) die Rechte und Freiheiten der betroffenen Person sowie deren potenzielle Verwundbarkeiten bei der Anwendung der Ausnahme berücksichtigt werden ([61]), iii) der Secretary of State Aufzeichnungen über die Inanspruchnahme der Ausnahme im Bereich der Einwanderung führt und die betroffene Person über deren Verwendung informiert (außer in bestimmten Fällen, in denen die Informationen das Ziel der Ausnahme beeinträchtigen würden) ([62]), und iv) klargestellt wird, dass die Anwendung der Ausnahme im Bereich der Einwanderung auf die Verarbeitung personenbezogener Daten durch den Secretary of State beschränkt ist ([63]), das heißt in der Praxis durch das Home Office für seine Funktionen gemäß Absatz 4(1) von Anhang 2 der DPA 2018. Darüber hinaus wird damit auch die Abwägung erläutert, die vorzunehmen ist, wenn festgestellt wird, ob die Ausübung der Rechte betroffener Personen eine wirksame Einwanderungskontrolle beeinträchtigen kann und ob es notwendig und verhältnismäßig ist, diese Rechte dadurch einzuschränken.

([54]) Abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([55]) Paragraf 88 Absatz 2 des Data (Use and Access) Act enthält eine geringfügige Änderung von Paragraf 26 Absatz 2 Buchstabe f DPA 2018 (Ausnahme für die nationale Sicherheit und Verteidigung), mit der klargestellt wird, dass das Recht auf Beschwerde beim Commissioner gemäß Artikel 77 UK GDPR nicht Teil der Bestimmungen ist, deren Anwendung aus Gründen der nationalen Sicherheit oder Verteidigung eingeschränkt werden kann.

([56]) Zum Zeitpunkt des Erlasses des Durchführungsbeschlusses (EU) 2021/1772 waren die Gültigkeit und Auslegung der Ausnahme im Bereich der Einwanderung nach dem Recht des Vereinigten Königreichs noch nicht geklärt, nachdem der Court of Appeal of England and Wales am 26. Mai 2021 entschieden hatte, dass die Ausnahme im Bereich der Einwanderung, wie sie damals im DPA 2018 vorgesehen war, mit dem Recht des Vereinigten Königreichs unvereinbar sei, da es an spezifischen Bestimmungen zur Festlegung der in Artikel 23 Absatz 2 der UK GDPR aufgeführten Garantien fehle, der Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 entspricht. Aus diesem Grund waren personenbezogene Daten, die zu Zwecken der Einwanderungskontrolle des Vereinigten Königreichs übermittelt wurden oder anderweitig in den Anwendungsbereich der Ausnahme im Bereich der Einwanderung fallen, vom Anwendungsbereich des Durchführungsbeschlusses (EU) 2021/1772 ausgenommen worden.

([57]) Die Regulations traten am 31. Januar 2022 in Kraft und sind unter folgendem Link abrufbar: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) Die Regulations traten am 8. März 2024 in Kraft und sind unter folgendem Link abrufbar: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) Die mit den Verordnungen 2022 überarbeitete Ausnahme im Bereich der Einwanderung wurde erneut im Wege einer gerichtlichen Überprüfung mit der Begründung angefochten, dass sie noch nicht alle Anforderungen von Artikel 23 Absatz 2 UK GDPR erfülle. Der Court of Appeal stellte im Dezember 2023 fest, dass sie nicht mit den Anforderungen des Artikels 23 Absatz 2 UK GDPR vereinbar sei. Infolge dieses Urteils ergänzen die Verordnungen 2024 die Verordnungen 2022 und nehmen weitere Änderungen an der Ausnahme im Bereich der Einwanderung vor.

([60]) Paragraf 2 Absatz 4A Unterabsatz 2 des DPA 2018.

([61]) Paragraf 2 Absatz 4AB Unterabsätze 3 und 4 des DPA 2018. Das Büro des Information Commissioner wurde zu den Entwürfen der Verordnungen 2024 konsultiert und erklärte öffentlich, dass es mit der Verordnung einverstanden sei. Das als Antwort auf die Konsultation veröffentlichte Schreiben zur Bestätigung seiner Ansicht ist unter folgendem Link abrufbar: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) Anhang 2 Paragraf 4B Absätze 1 und 2 des DPA 2018.

([63]) Anhang 2 Paragraf 4 Absatz 1 des DPA 2018.

(38) Darüber hinaus hat die britische ICO detaillierte Leitlinien zur Anwendung dieser spezifischen Einschränkung veröffentlicht ([64]). Darin heißt es insbesondere: „Die Ausnahme im Bereich der Einwanderung sollte nicht als pauschale Ausnahmeregelung angewendet werden, um die Rechte in Bezug auf alle im Besitz befindlichen Daten einzuschränken. Der Geltungsbereich der Ausnahme ist auf die Rechte beschränkt, die, würden sie im Hinblick auf die im Besitz befindlichen Daten ausgeübt, die ermittelten Zwecke im Bereich der Einwanderung beeinträchtigen würden. […] Daher sollte der Standpunkt des Verantwortlichen standardmäßig darin bestehen, die Anforderungen der Verordnung (EU) 2016/679 und des DPA so weit wie möglich zu erfüllen. […] Der Maßstab für eine Beeinträchtigung ist hoch, und die Ausnahme sollte nicht pauschal angewendet werden. […] Sie müssen prüfen, ob die Anwendung der Ausnahme eine verhältnismäßige Antwort auf den Datenschutzantrag der betreffenden Person darstellt. Man könnte der Ansicht sein, dass ein zwingender gesellschaftlicher Grund für die Anwendung der Ausnahme im Bereich der Einwanderung besteht, dennoch ist auch zu berücksichtigen, ob dieser Grund schwerer wiegt als die Verpflichtung gegenüber dem Einzelnen gemäß der Verordnung (EU) 2016/679. Der Einzelne besitzt Rechte bezüglich seiner personenbezogenen Daten, die unter allen Umständen zu berücksichtigen sind, insbesondere das Recht auf Auskunft. Daher muss in jedem Fall beurteilt werden, ob die Datenschutzrechte des Einzelnen das festgestellte Risiko einer Beeinträchtigung überwiegen. Die Anwendung der Ausnahme muss in einem angemessenen Verhältnis zu den Umständen stehen, und jeder Fall muss sorgfältig geprüft und dokumentiert werden."

(39) Insgesamt unterliegt die Einwanderungsbeschränkung gemäß Anhang 2 Nummer 4 des DPA 2018 in der von der Regierung des Vereinigten Königreichs 2022 und 2024 überarbeiteten Fassung und in der Auslegung durch die Rechtsprechung ([65]) und die Leitlinien des ICO einer Reihe strenger Bedingungen, die ihre Anwendung bestimmen und den Bedingungen sehr ähnlich sind, die im Unionsrecht, insbesondere in Artikel 23 der Verordnung (EU) 2016/679, für die Beschränkung der Datenschutzrechte und -pflichten für wichtige Ziele des öffentlichen Interesses wie die Kontrolle der Einwanderung festgelegt sind.

2.2.5. *Beschränkungen für Weiterübermittlungen*

(40) Das Schutzniveau für personenbezogene Daten, die aus der Europäischen Union an Verantwortliche oder Auftragsverarbeiter im Vereinigten Königreich übermittelt werden, ist nach wie vor nicht durch die Weiterübermittlung dieser Daten an Empfänger in einem Drittland beeinträchtigt. Wie in den Erwägungsgründen 74 bis 82 des Durchführungsbeschlusses (EU) 2021/1772 bewertet, ähnelt die Regelung für die internationale Übermittlung personenbezogener Daten aus dem Vereinigten Königreich nach wie vor sehr stark den Regelungen in Kapitel V der Verordnung (EU) 2016/679.

(41) Mit dem Data (Use and Access) Act wurde Kapitel 5 der UK GDPR über die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen zwar geändert, jedoch wird die Kernanforderung beibehalten, dass personenbezogene Daten nur dann an ein Drittland oder eine internationale Organisation übermittelt werden dürfen, wenn die Übermittlung auf i) Verordnungen zur Genehmigung der Übermittlung (neue Terminologie für die früheren „Angemessenheitsvorschriften"), ii) geeigneten Garantien oder iii) einer Ausnahme für bestimmte Situationen beruht. Diese allgemeinen Grundsätze für Datenübermittlungen werden in dem neuen Artikel 44A übernommen, der Artikel 44 UK GDPR ersetzt ([66]) und in dem auch festgelegt ist, dass die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation nur zulässig ist, wenn die Übermittlung im Einklang mit den anderen Bestimmungen der UK GDPR erfolgt.

(42) Speziell in Bezug auf die Verordnungen zur Genehmigung einer Übermittlung ist in Artikel 45A Absatz 2 UK GDPR festgelegt, dass der Secretary of State solche Verordnungen nur erlassen darf, wenn er der Auffassung ist, dass die Datenschutzprüfung erfüllt ist. Dies bedeutet, dass die in Artikel 45A Absatz 3 UK GDPR eingeführte Möglichkeit für den Secretary of State, die Erwünschtheit der Erleichterung des Datenverkehrs beim Erlass solcher Vorschriften zu berücksichtigen, stets an die Bedingung geknüpft ist, dass die Datenschutzprüfung erfüllt ist. Der rechtliche Standard für die zu erfüllende Datenschutzprüfung ist im neuen Artikel 45B Absatz 1 UK GDPR festgelegt, wonach der Schutzstandard für betroffene Personen in Empfängerländern oder in internationalen Organisationen nicht wesentlich niedriger sein darf als der Standard, der für betroffene Personen nach den einschlägigen Datenschutzvorschriften des Vereinigten Königreichs vorgesehen ist. Artikel 45B Absatz 2 UK GDPR enthält ferner eine nicht abschließende Liste von Elementen, die bei der Beurteilung, ob dieser Test erfüllt ist, zu berücksichtigen sind, wie die Achtung der Rechtsstaatlichkeit und der Menschenrechte, die Existenz und Befugnisse einer Datenschutzbehörde, die Regelungen für gerichtliche oder außergerichtliche Rechtsbehelfe, die Vorschriften über die Übermittlung personenbezogener Daten aus dem Land oder durch die Organisation an andere Länder oder

([64]) Abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

([65]) *Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor*, [2019] EWHC 2562 (Admin), Rn. 40 und 41.

([66]) Paragraf 85 und Anhang 7 des Data (Use and Access) Act.

internationale Organisationen, die einschlägigen internationalen Verpflichtungen des Landes oder der Organisation sowie die Verfassung, Traditionen und Kultur des Landes oder der Organisation. Während die Liste der relevanten Elemente aus dem früheren Artikel 45 UK GDPR neu gefasst wurde, behält der neue Artikel 45B Absatz 2 die Kernelemente dieser Liste bei und bleibt damit eng an den Vorgaben von Kapitel V der Verordnung (EU) 2016/679 angelehnt. Darüber hinaus haben die Behörden des Vereinigten Königreichs bestätigt, dass der Secretary of State Elemente berücksichtigen wird, die nicht in Artikel 45B Absatz 2 aufgeführt sind, wie z. B. die Rechtsvorschriften und Gepflogenheiten in einem Drittland in Bezug auf den Zugang von Behörden zu personenbezogenen Daten für Zwecke wie die nationale Sicherheit oder die Strafverfolgung, soweit sie den allgemeinen Schutzstandard beeinträchtigen. Darüber hinaus sind die Behörden des Vereinigten Königreichs der Auffassung, dass die einschlägige Rechtsprechung in dem Drittland ein wesentlicher Bestandteil bei der Prüfung der in Artikel 45B Absatz 2 UK GDPR nicht erschöpfend aufgeführten Angelegenheiten sein wird.

(43) Verordnungen zur Genehmigung einer Übermittlung unterliegen weiterhin den „allgemeinen" Verfahrensanforderungen, die in Paragraf 182 der DPA 2018 vorgesehen sind, wie in Erwägungsgrund 77 des Durchführungsbeschlusses (EU) 2021/1772 dargelegt. Im Rahmen dieses Verfahrens muss der Secretary of State den Information Commissioner konsultieren, wenn er beabsichtigt, britische Angemessenheitsverordnungen zu erlassen ([67]). Nach ihrer Verabschiedung durch den Secretary of State werden diese Verordnungen dem Parlament vorgelegt und unterliegen dem „Negative Resolution"-Verfahren, nach dem beide Parlamentskammern die Verordnungen prüfen und innerhalb von 40 Tagen einen Beschluss zur Aufhebung der Verordnungen fassen können ([68]).

(44) In Bezug auf geeignete Garantien sieht der neue Artikel 46 Absatz 1A UK GDPR vor, dass solche Übermittlungen nur erfolgen dürfen, wenn in den nach Artikel 46 Absätze 2 und 3 ([69]) der UK GDPR verfügbaren Instrumenten einschlägige Garantien vorgesehen sind und der Verantwortliche, der Auftragsverarbeiter oder die zuständigen öffentlichen Stellen, die nach vernünftigem Ermessen und verhältnismäßig handeln, der Auffassung sind, dass die Datenschutzprüfung erfüllt ist. In den neu eingefügten Absätzen 6 und 7 wird klargestellt, dass die Datenschutzprüfung erfüllt ist, wenn der für betroffene Personen vorgesehene Schutzstandard aufgrund der erforderlichen Garantien nach der Übermittlung nicht wesentlich niedriger ist als der Standard nach den einschlägigen Datenschutzvorschriften des Vereinigten Königreichs, d. h., ebenso wie dies nach der Verordnung (EU) 2016/679 der Fall ist, gelten dieselben rechtlichen Standards sowohl für Verordnungen zur Genehmigung einer Übermittlung als auch für geeignete Garantien. Laut demselben Absatz ist das, was als angemessen und verhältnismäßig gilt, unter Berücksichtigung aller Umstände oder voraussichtlicher Umstände der Übermittlung bzw. des Übermittlungstyps zu bestimmen, einschließlich der Art und des Umfangs der übermittelten personenbezogenen Daten.

(45) In Bezug auf Ausnahmen für bestimmte Situationen wird in Artikel 49 UK GDPR zu den Bedingungen, unter denen Ausnahmen für bestimmte Situationen angewandt werden können, eine Reihe technischer Änderungen vorgenommen, mit denen die Bestimmung an Änderungen anderer Bestimmungen angepasst wird, das Schutzniveau für personenbezogene Daten im Vereinigten Königreich jedoch nicht beeinträchtigt wird. Darüber hinaus wird ein neuer Absatz 4A eingefügt, um die Wirkung von Paragraf 18 Absatz 1 der DPA 2018 wiederzugeben, der dem Secretary of State die Befugnis verleiht, durch Verordnungen die Umstände festzulegen, unter denen Datenübermittlungen aus Gründen des öffentlichen Interesses als erforderlich gelten. Schließlich übernimmt ein neuer Artikel 49A die Wirkung von Paragraf 18 Absatz 2 der DPA 2018, der es dem Secretary of State ermöglicht, durch Verordnungen Beschränkungen für Datenübermittlungen vorzuschreiben, wenn diese nicht gemäß Artikel 45A (durch Verordnungen genehmigte Übermittlungen) genehmigt sind und aus wichtigen Gründen des öffentlichen Interesses für notwendig erachtet werden.

(46) Bei der Umsetzung der internationalen Übermittlungsregeln des Vereinigten Königreichs gab es seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 mehrere Entwicklungen.

([67]) Siehe Vereinbarung zwischen dem Secretary of State des Ministeriums für Digitales, Kultur, Medien und Sport (Department for Digital, Culture, Media and Sport) und dem Büro des Information Commissioner über die Rolle des ICO im Zusammenhang mit der neuen britischen Angemessenheitsbewertung, abrufbar unter folgenden Link: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([68]) Im Falle eines solchen Votums verlieren die Vorschriften endgültig jede Rechtswirkung.

([69]) Bei dem nach Artikel 46 Absätze 2 und 3 UK GDPR zur Verfügung stehenden Übermittlungsinstrument handelt es sich um rechtsverbindliche und durchsetzbare Instrumente zwischen Behörden oder öffentlichen Stellen, um verbindliche unternehmensinterne Vorschriften gemäß Artikel 47 UK GDPR, um Standarddatenschutzklauseln, die in Verordnungen des Secretary of State oder in einem von der Information Commission herausgegebenen Dokument festgelegt sind, um einen genehmigten Verhaltenskodex und einen genehmigten Zertifizierungsmechanismus.

(47) In Bezug auf Verordnungen zur Genehmigung von Datenübermittlungen wurden bislang zwei neue Verordnungen erlassen, die im Einklang mit den Angemessenheitsbeschlüssen stehen, die auch in der Union gelten, d. h. für Übermittlungen an die Republik Korea und für Übermittlungen an gewerbliche Einrichtungen, die sich der Erweiterung des EU-US-Datenschutzrahmens auf das Vereinigte Königreich angeschlossen haben. Die Angemessenheitsvorschriften für die Republik Korea ([70]) traten am 19. Dezember 2022 in Kraft und ermöglichen die Übermittlung personenbezogener Daten aus dem Vereinigten Königreich an die Republik Korea. Die Erweiterung des EU-US-Datenschutzrahmens auf das Vereinigte Königreich, für die die einschlägigen Verordnungen ([71]) am 12. Oktober 2023 in Kraft getreten sind, ermöglicht den freien Verkehr personenbezogener Daten an zertifizierte US-Organisationen.

(48) In Bezug auf geeignete Garantien hat das Vereinigte Königreich seine eigenen Standard-Datenschutzvertragsklauseln, das International Data Transfer Agreement (IDTA) ([72]) und ein Addendum zu den Standardvertragsklauseln der EU, veröffentlicht, die beide im März 2022 in Kraft getreten sind. Das IDTA bietet einen spezifischen Mechanismus für das Vereinigte Königreich zur Gewährleistung geeigneter Garantien für die Übermittlung personenbezogener Daten und ist den Standardvertragsklauseln der EU in verschiedenen Punkten ähnlich. Das vom ICO herausgegebene Addendum ermöglicht es Verantwortlichen und Auftragsverarbeitern im Vereinigten Königreich, sich für internationale Übermittlungen auf EU-Standardvertragsklauseln im Rahmen der UK GDPR zu stützen. Das ICO hat außerdem ein Instrument zur Risikobewertung von Datenübermittlungen herausgegeben, um Organisationen im Vereinigten Königreich bei der Bewertung der mit internationalen Datenübermittlungen verbundenen Risiken zu unterstützen.

(49) Das Vereinigte Königreich hat außerdem das Genehmigungsverfahren für verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, im Folgenden „BCR“) durch neue Leitlinien und neue Optionen für die Genehmigung verbindlicher interner Datenschutzvorschriften optimiert. Im Juli 2022 veröffentlichte die ICO Leitlinien und Bezugstabellen, um den Ansatz des Vereinigten Königreichs zu BCRs nach dem Brexit zu erläutern, und im Dezember 2023 wurde ein Addendum zu den EU-BCRs veröffentlicht, um sicherzustellen, dass unter dem Unionsrahmen genehmigte BCRs im Vereinigten Königreich durchsetzbar sind ([73]).

(50) Schließlich wurde das Vereinigte Königreich im Juli 2023 assoziiertes Mitglied des Forums „Global Cross-Border Privacy Rules“ (CBPR) ([74]). Wichtig ist dabei, dass diese Mitgliedschaft keine Erleichterung der Datenübermittlung aus dem Vereinigten Königreich an andere Mitglieder des CBPR-Forums mit sich bringt. Das Vereinigte Königreich hat klargestellt, dass jede Übermittlung personenbezogener Daten aus dem Vereinigten Königreich an Drittländer oder internationale Organisationen die in den Rechtsvorschriften des Vereinigten Königreichs festgelegten Bedingungen, wie oben beschrieben, erfüllen muss, insbesondere die Datenschutzprüfung, wonach die gewährten Schutzstandards „nicht wesentlich niedriger“ sein dürfen als die nach der UK GDPR.

(51) Wie die Kommission bereits erläutert hat, gewährleisten CBPRs kein ausreichendes Schutzniveau für personenbezogene Daten aus der EU. Insbesondere sieht es keine durchsetzbaren Rechte des Einzelnen vor ([75]). Daher ist es besonders wichtig, dass das CBPR, selbst wenn das Vereinigte Königreich assoziiertes Mitglied des Global CBPR-Forum ist, keinen gültigen Übermittlungsmechanismus nach dem Datenschutzrecht des Vereinigten Königreichs darstellen kann. Sollte sich dies ändern, würde dadurch das derzeit gewährleistete Schutzniveau für personenbezogene Daten, die aus der EU in das Vereinigte Königreich übermittelt werden, beeinträchtigt. Daher wird die Kommission die weiteren Entwicklungen in dieser Hinsicht weiterhin aufmerksam verfolgen.

([70]) Abrufbar unter folgendem Link: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Abrufbar unter folgendem Link: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) Nach dem Brexit gingen beim ICO zahlreiche BCR-Anträge des Vereinigten Königreichs ein. Viele zuvor genehmigte BCRs konnten nicht mehr verwendet werden, da nur BCRs, bei denen das ICO in das Genehmigungsverfahren eingebunden war, auch nach dem Brexit weiterhin genutzt werden konnten; diese BCR-Inhaber waren jedoch verpflichtet, dem ICO aktualisierte, mit der UK GDPR konforme BCR-Dokumente vorzulegen.

([74]) Das CBPR-Forum setzt sich aus den Vereinigten Staaten von Amerika, Kanada, Japan, der Republik Korea, den Philippinen, Singapur, Taiwan und Australien zusammen, während Mauritius, das Dubai International Financial Centre und Bermuda wie das Vereinigte Königreich assoziierte Mitglieder sind.

([75]) Siehe beispielsweise die von den G7-Datenschutzbehörden durchgeführte vergleichende Analyse der Kernelemente des DSGVO-Zertifizierungssystems und des CBPR-Systems, die „erhebliche Unterschiede“ zwischen den Systemen ergab, einschließlich der „Durchsetzbarkeit und des Rechtsschutzes, der Vorschriften über die unabhängige Aufsicht und den Zugang der Regierung“). Abrufbar unter folgendem Link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165.
Siehe Erwägungsgrund 79 des Durchführungsbeschlusses (EU) 2019/419 der Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen (ABl. L 76 vom 19.3.2019, S. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Siehe auch Artikel-29-Datenschutzgruppe, Stellungnahme 02/2014 zu einer Referenzgrundlage für Anforderungen an verbindliche interne Datenschutzvorschriften, die den nationalen Datenschutzbehörden in der EU vorgelegt wurden, sowie grenzüberschreitende Vorschriften zur Wahrung der Privatsphäre, die den CBPR-Rechenschaftspflichtigen der APEC vorgelegt wurden, 6. März 2014.

2.2.6. *Automatisierte Entscheidungsfindung*

(52) Unter Beibehaltung mehrerer Elemente der Vorschriften über die automatisierte Entscheidungsfindung, die in Erwägungsgrund 54 des Durchführungsbeschlusses (EU) 2021/1772 bewertet wurden, wurden einige Aspekte dieser Vorschriften durch den Data (Use and Access) Act geändert.

(53) Zunächst enthält der neu eingeführte Artikel 22B UK GDPR ein allgemeines Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten (gemäß Artikel 9 Absatz 1 UK GDPR) für wichtige Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen und rechtliche oder ähnlich bedeutende Auswirkungen auf die betroffene Person haben. Es sind darin jedoch drei Ausnahmen von diesem Verbot vorgesehen: die betroffene Person hat ausdrücklich in diese Verarbeitung eingewilligt; oder die Entscheidung ist für den Abschluss oder die Erfüllung eines Vertrags zwischen dem für die Verarbeitung Verantwortlichen und der betroffenen Person erforderlich; oder die Verarbeitung ist gesetzlich vorgeschrieben oder zulässig. In den beiden letztgenannten Ausnahmen muss die automatisierte Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich sein ([76]). Das allgemeine Verbot gilt nicht für wichtige Entscheidungen, die auf einer automatisierten Verarbeitung nicht besonderer Datenkategorien beruhen.

(54) Darüber hinaus wird in dem neuen Artikel 22A UK GDPR die Definition einer Entscheidung präzisiert, die „ausschließlich auf einer automatisierten Verarbeitung beruht“, indem festgelegt wird, dass eine solche Entscheidung eine Entscheidung ist, bei der keine wesentliche menschliche Beteiligung am Entscheidungsprozess vorliegt. Wichtig ist, dass die Verantwortlichen beurteilen müssen, inwieweit Profiling zu einer Entscheidung beiträgt, um festzustellen, ob die menschliche Beteiligung wesentlich war. In Artikel 22A UK GDPR wird außerdem klargestellt, dass eine „bedeutende Entscheidung“ eine Entscheidung ist, die eine nachteilige Rechtswirkung für die betroffene Person haben oder sie erheblich beeinträchtigen würde ([77]).

(55) Zweitens schreibt der neu eingeführte Artikel 22C der UK GDPR vor, dass Verantwortliche Maßnahmen ergreifen müssen, um die einschlägigen Garantien für alle wesentlichen Entscheidungen zu bieten, die ganz oder teilweise auf personenbezogenen Daten und ausschließlich auf einer automatisierten Verarbeitung beruhen (einschließlich nicht besonderer Kategorien personenbezogener Daten). Diese Garantien müssen die Unterrichtung der betroffenen Person über den Entscheidungsprozess umfassen, es der betroffenen Person ermöglichen, die Entscheidung anzufechten und Erklärungen abzugeben, und sicherstellen, dass die betroffene Person das Eingreifen einer Person in den Entscheidungsprozess erwirken kann ([78]).

(56) Schließlich verleiht der neu eingeführte Artikel 22D der UK GDPR dem Secretary of State die Befugnis, abgeleitete Rechtsvorschriften zu erlassen, um zu beschreiben, was eine sinnvolle menschliche Beteiligung darstellt und was nicht und welche Entscheidung als ähnlich erhebliche Auswirkungen auf die betroffenen Personen anzusehen ist und was nicht. Er ermöglicht es dem Secretary of State auch, sekundäre Rechtsvorschriften zu erlassen, um i) neue Schutzvorkehrungen hinzuzufügen, ii) Anforderungen festzulegen, die die bestehenden Garantien ergänzen; und iii) Maßnahmen zu definieren, die die Schutzvorkehrungen nicht erfüllen ([79]). Wichtig ist, dass der Secretary of State vor dem Erlass von Verordnungen gemäß Artikel 22D UK GDPR das ICO konsultieren muss ([80]), dass mit den Verordnungen Artikel 22C UK GDPR nicht geändert werden darf ([81]) und dass Verordnungen dem positiven Abstimmungsverfahren unterliegen ([82]), was bedeutet, dass sie von beiden Kammern des Parlaments des Vereinigten Königreichs gebilligt werden müssen, bevor sie erlassen werden können.

(57) Mit dem Data (Use and Access) Act wurde zwar der Rahmen für die automatisierte Entscheidungsfindung geändert, es ist jedoch darauf hinzuweisen, dass die automatisierte Entscheidungsfindung nach dem Rechtsrahmen des Vereinigten Königreichs weiterhin den wichtigsten Garantien unterliegt, durch die das Recht auf das Eingreifen einer Person in allen Fällen bedeutender Entscheidungen vorgeschrieben ist, die ausschließlich auf automatisierter Verarbeitung beruhen, d. h. auf der Grundlage der Verarbeitung sensibler und nicht sensibler personenbezogener

([76]) Artikel 22B der UK GDPR, eingeführt durch Paragraf 80 Absatz 1 des Data (Use and Access) Act.
([77]) Artikel 22A UK GDPR, eingeführt durch Paragraf 80 Absatz 1 des Data (Use and Access) Act.
([78]) Artikel 22C der UK GDPR, eingeführt durch Paragraf 80 Absatz 1 des Data (Use and Access) Act.
([79]) Artikel 22D der UK GDPR, eingeführt durch Paragraf 80 Absatz 1 des Data (Use and Access) Act. Alle Verordnungen, die im Rahmen dieser Befugnisse erlassen werden, unterliegen dem positiven Abstimmungsverfahren, durch das die parlamentarische Kontrolle sichergestellt ist. Die Anforderungen des Artikels 22C können mit den Verordnungen nicht geändert werden.
([80]) Paragraf 182 Absatz 2 DPA 2018.
([81]) Artikel 22D Absatz 4 UK GDPR.
([82]) Artikel 22D Absatz 5 UK GDPR.

Daten ([83]). Darüber hinaus ist es, wie die Kommission in früheren Angemessenheitsbeschlüssen festgestellt hat ([84]), unwahrscheinlich, dass sich die spezifischen Vorschriften für die automatisierte Entscheidungsfindung in der UK GDPR auf das Schutzniveau für personenbezogene Daten auswirken, die aus der Union in das Vereinigte Königreich übermittelt werden. Bei personenbezogenen Daten, die in der Union erhoben wurden, wird jede Entscheidung, die auf einer automatisierten Verarbeitung beruht, typischerweise vom Verantwortlichen in der Union getroffen (der eine direkte Beziehung zu der betroffenen Person unterhält) und unterliegt somit den Bestimmungen der Verordnung (EU) 2016/679.

2.3. **Aufsicht und Durchsetzung**

2.3.1. *Unabhängige Aufsicht*

(58) Im Vereinigten Königreich wird die Überwachung und Durchsetzung der Einhaltung des Datenschutzrahmens weiterhin von einer unabhängigen Datenschutzaufsichtsbehörde durchgeführt, wie in den Erwägungsgründen 85 bis 91 des Durchführungsbeschlusses (EU) 2021/1772 analysiert. Mit dem Data (Use and Access) Act wird die Leitungsstruktur dieser Behörde reformiert, indem mit der Information Commission eine Körperschaft geschaffen wird, die das ICO ersetzt, das zuvor als Corporation Sole organisiert war.

(59) Konkret werden die im Daten-(Nutzungs- und Zugriffs-)Gesetz festgelegten Governance-Maßnahmen, sobald sie umgesetzt sind, das Amt des Informationsbeauftragten abschaffen und die Funktionen, das Personal und das Eigentum vom ICO auf die neue Stelle, die Informationskommission, übertragen. Die Information Commission setzt sich aus geschäftsführenden und nicht geschäftsführenden Mitgliedern zusammen ([85]). Im Gesetz ist auch vorgesehen, dass der Information Commissioner den Vorsitz der Information Commission übernimmt, also zu einem nicht geschäftsführenden Mitglied wird ([86]). Im Data (Use and Access) Act ist ferner vorgesehen, dass, soweit dies aufgrund der Übertragung von Aufgaben angemessen ist, Verweise auf den Information Commissioner in allen Rechtsvorschriften oder sonstigen Dokumenten (unabhängig davon, wann diese verabschiedet oder erstellt wurden) als Verweise auf die Information Commission zu behandeln sind. Zur Erfüllung ihrer Aufgaben kann die Kommission Ausschüsse einsetzen und Aufgaben an Mitglieder, Mitarbeitende oder Ausschüsse der Kommission ([87]) delegieren sowie Vorkehrungen zur Regelung ihrer Verfahren und der Verfahren der Ausschüsse treffen, unter anderem in Bezug auf die Beschlussfähigkeit und die Beschlussfassung mit Stimmenmehrheit. Diese Verfahren müssen veröffentlicht werden ([88]).

(60) Wichtig ist, dass die Unabhängigkeit der Information Commission denselben Garantien unterliegt, auch in Bezug auf die Vorschriften für die Ernennung und Abberufung der vorsitzenden Person, wie sie in den Erwägungsgründen 87 bis 90 des Durchführungsbeschlusses (EU) 2021/1772 ([89]) bewertet. Ähnliche Schutzmaßnahmen gelten auch für die anderen nicht geschäftsführenden Mitglieder der Information Commission Insbesondere wird die vorsitzende Person der Information Commission auf Empfehlung des Secretary of State von Seiner Majestät ernannt. Er/sie wird aufgrund seiner/ihrer Verdienste und auf der Grundlage eines fairen und offenen Auswahlverfahrens ausgewählt ([90]). Die übrigen nicht geschäftsführenden Mitglieder werden vom Secretary of State nach Rücksprache mit der vorsitzenden Person ernannt. Bewerber/innen können nur dann für eine Ernennung empfohlen oder ernannt werden, wenn sie auf der Grundlage ihrer Leistungen im Rahmen eines fairen und offenen Auswahlverfahrens ausgewählt wurden und wenn der Secretary of State davon überzeugt ist, dass sie sich nicht in einem Interessenkonflikt befinden ([91]). Die geschäftsführenden Mitglieder sind Bedienstete der Information Commission, die zu von den nicht geschäftsführenden Mitgliedern festgelegten Bedingungen beschäftigt werden ([92]). Die anderen nicht geschäftsführenden Mitglieder werden vom Secretary of State nach Konsultation der vorsitzenden Person ernannt. Die Ernennung der geschäftsführenden Mitglieder unterliegt auch einer Auswahl nach Verdiensten auf der Grundlage eines fairen und offenen Auswahlverfahrens ([93]).

(61) Die vorsitzende Person kann von Seiner Majestät nur nach einer Meinungsäußerung beider Kammern des Parlaments ihres Amtes enthoben werden und nur dann, wenn der Secretary of State der betreffenden Kammer einen Bericht vorgelegt hat, in dem er erklärt, dass sich die vorsitzende Person seiner Überzeugung nach eines schweren Fehlverhaltens schuldig gemacht hat, in einem Interessenkonflikt steht, besonderen Informationspflichten

([83]) Artikel 22C Absatz 2 der UK GDPR, eingeführt durch Paragraf 80 Absatz 1 des Data (Use and Access) Act.
([84]) Siehe beispielsweise Erwägungsgrund 94 des Durchführungsbeschlusses (EU) 2019/419 und Erwägungsgrund 81 des Durchführungsbeschlusses (EU) 2022/254 der Kommission vom 17. Dezember 2021 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten durch die Republik Korea im Rahmen des Gesetzes über den Schutz personenbezogener Informationen (ABl. L 44 vom 24.2.2022, S. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).
([85]) Absatz 3(1) von Anhang 12A zum DPA 2018.
([86]) Paragrafen 117, 118, 119 und 120 in Verbindung mit Anhang 14 des Data (Use and Access) Act.
([87]) Absätze 13 und 14 von Anhang 12A zum DPA 2018.
([88]) Absatz 16 von Anhang 12A zum DPA 2018.
([89]) Artikel 52 UK GDPR sowie Anhang 12A des DPA 2018, eingeführt durch Paragraf 114A des Data (Use and Access) Bill.
([90]) Anhang 12A Paragraf 5 Absatz 1 und Paragraf 3 Absatz 2 des DPA 2018.
([91]) Anhang 12A Paragrafen 3 Absatz 2, 5 und 6 des DPA 2018.
([92]) Absatz 11 von Anhang 12A zum DPA 2018.
([93]) Absatz 5(2) von Anhang 12A zum DPA 2018.

in Bezug auf potenzielle Interessenkonflikte nicht nachgekommen ist oder nicht in der Lage, ungeeignet oder willens ist, die Funktionen der vorsitzenden Person auszuüben ([94]). Nicht geschäftsführende Mitglieder können vom Secretary of State nur dann ihres Amtes enthoben werden, wenn er sich davon überzeugt hat, dass die in den Rechtsvorschriften festgelegten besonderen Bedingungen erfüllt sind. Dazu gehören Interessenkonflikte, schwere Verfehlungen oder die Unfähigkeit, Bereitschaft oder Unfähigkeit, ihre Aufgaben zu erfüllen. In Bezug auf zusätzliche Garantien ist der Secretary of State verpflichtet, die Entscheidung, dies zu tun, zu veröffentlichen und dem Mitglied eine Begründung für die Abberufung zu übermitteln ([95]).

(62) Die Hauptaufgabe der Information Commission besteht weiterhin in der Überwachung und Durchsetzung des Datenschutzrahmens im Vereinigten Königreich „zum Schutz der Grundrechte und Grundfreiheiten" der Einzelnen ([96]). Im Hinblick auf die Aufgabe der Information Commission, ein angemessenes Schutzniveau für personenbezogene Daten sicherzustellen, ist im Data (Use and Access) Act ausdrücklich vorgeschrieben, dass die Information Commission neben den Interessen der betroffenen Personen, der für die Verarbeitung Verantwortlichen und anderer Personen auch Fragen von allgemeinem öffentlichem Interesse und die Förderung des Vertrauens der Öffentlichkeit in die Verarbeitung personenbezogener Daten berücksichtigt ([97]). Diese Ziele werden auch in Erwägungsgrund 7 der Verordnung (EU) 2016/679 genannt.

(63) Darüber hinaus ist im Data (Use and Access) Act festgelegt, dass die Information Commission bei der Wahrnehmung ihrer Aufgaben im Rahmen der Datenschutzvorschriften die Förderung von Innovation und Wettbewerb, die Bedeutung der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, die Notwendigkeit des Schutzes der öffentlichen Sicherheit und der nationalen Sicherheit sowie die besonderen Bedürfnisse im Zusammenhang mit dem Schutz von Kindern berücksichtigt ([98]). Im EU-Datenschutzrecht wird auch die Notwendigkeit anerkannt, den Schutz personenbezogener Daten mit mehreren anderen Grundrechten und Zielen in Einklang zu bringen, wie z. B. wirtschaftlicher und sozialer Fortschritt, Sicherheit und Gerechtigkeit sowie die Freiheit der unternehmerischen Tätigkeit ([99]).

2.3.2. *Durchsetzung, einschließlich Sanktionen*

(64) Die Befugnisse und Aufgaben der Information Commission entsprechen weiterhin denen der Datenschutzaufsichtsbehörden der Mitgliedstaaten gemäß den einschlägigen Artikeln der Verordnung (EU) 2016/679 ([100]), wie in den Erwägungsgründen 91 bis 95 des Durchführungsbeschlusses (EU) 2021/1772 bewertet.

(65) Mit dem Data (Use and Access) Act wurden einige Klarstellungen bezüglich der Ausübung verschiedener Befugnisse eingeführt.

(66) Einerseits kann die Kommission nach dem Data (Use and Access) Act bestimmte „Dokumente" und „Informationen" verlangen, wenn sie von der Befugnis Gebrauch macht, diese mittels eines Informationsbescheides anzufordern ([101]). Andererseits werden mit dem Data (Use and Access) Act zwei neue Befugnisse für die Information Commission eingeführt: eine neue Befugnis, einen Bericht zu verlangen ([102]), und eine neue Befugnis, im Falle eines mutmaßlichen Verstoßes gegen die UK GDPR oder den DPA 2018 „Anhörungsmitteilungen" an die Verantwortlichen zu richten ([103]).

([94]) Anhang 12A Paragraf 7 Absatz 6 und 7 des DPA 2018.

([95]) Anhang 12A Paragraf 9 Absatz 6, 7, 8 und 9 des DPA 2018.

([96]) Artikel 51 UK GDPR.

([97]) Paragraf 91 des Data (Use and Access) Act, mit dem Paragraf 120A des DPA 2018 eingeführt wird.

([98]) Paragraf 91 des Data (Use and Access) Act, mit dem Paragraf 120B des DPA 2018 eingeführt wird. Mit dem Data (Use and Access) Act wird ferner ein neuer Paragraf 120C im DPA 2018 eingeführt, wonach die Information Commission eine Strategie ausarbeiten und veröffentlichen muss, in der sich unter anderem die Art und Weise niederschlägt, in der sie die oben genannten Fragen sowie die Förderung des Wirtschaftswachstums bei der Wahrnehmung ihrer Regulierungsaufgaben berücksichtigt hat.

([99]) Siehe insbesondere die Erwägungsgründe 2 und 4 sowie Artikel 23 der Verordnung (EU) 2016/679.

([100]) Artikel 57 und 58 UK GDPR.

([101]) Paragraf 97 des Data (Use and Access) Act zur Änderung von Paragraf 142 DPA 2018. Die Überlegungen zu den Auswirkungen der Technologie und zur Rolle des Datenschutzes bei der Schaffung von Vertrauen in die digitale Wirtschaft sind sowohl im Vereinigten Königreich als auch in der EU Teil der Tätigkeiten der Datenschutzregulierungsbehörden. Siehe z. B. Jahresbericht 2024 des Europäischen Datenschutzausschusses, S. 12: „Der EDSA ist ein dynamisches und kooperatives Gremium, das eine zentrale Rolle bei der Sicherstellung der einheitlichen Anwendung der Datenschutzvorschriften in ganz Europa spielt. Aus meiner Sicht als stellvertretender Vorsitzender sehe ich ihn als Hüter der Rechte des Einzelnen auf Privatsphäre, der die Bedürfnisse von Innovation und Wirtschaftswachstum sachgemäß gegeneinander abwägt."

([102]) Paragraf 98 des Data (Use and Access) Act zur Änderung von Paragraf 146 DPA 2018.

([103]) Paragraf 100 des Data (Use and Access) Act zur Einführung von Paragraf 148A des DPA 2018.

(67) In Bezug auf die Ausübung dieser Befugnisse durch die Information Commission hat der Information Commissioner seit dem Inkrafttreten des Durchführungsbeschlusses (EU) 2021/1772 jährlich etwa 40 000 Beschwerden betroffener Personen bearbeitet, was in etwa der Zahl der Beschwerden entspricht, die bearbeitet wurden, als das Vereinigte Königreich noch Teil der Union war und die Verordnung (EU) 2016/679 anwandte ([104]). Das ICO führte auch Untersuchungen von Amts wegen durch, die ein breites Spektrum von Bereichen und Fragen der Einhaltung der Vorschriften, einschließlich der Rechte betroffener Personen, abdeckten ([105]).

(68) Was Durchsetzungsmaßnahmen betrifft, so hat der Commissioner seit dem Inkrafttreten des Durchführungsbeschlusses (EU) 2021/1772 120 Verweise, 32 Informationsbescheide, 3 Bewertungsbescheide, 12 Durchsetzungsbescheide, 2 Verwarnungen und 12 Geldbußen erlassen ([106]). Hierzu zählen mehrere beträchtliche Geldbußen, die im Rahmen der UK GDPR und des DPA 2018 verhängt wurden. So verhängte der Information Commissioner im April 2023 eine Geldbuße in Höhe von 12,7 Mio. GBP gegen eine Social-Media-Plattform wegen missbräuchlicher Verwendung der Daten von Kindern ([107]). Im März 2025 wurde gegen ein Softwareunternehmen wegen Sicherheitsmängeln, durch die die personenbezogenen Daten von mehr als 70 000 Personen gefährdet wurden, eine Geldbuße in Höhe von 3,07 Mio. GBP verhängt ([108]). Erst kürzlich, im Juni 2025, verhängte der Information Commissioner eine Geldbuße in Höhe von 2,31 Mio. GBP gegen ein Gentestunternehmen, weil es nach einem groß angelegten Cyberangriff im Jahr 2023 keine angemessenen Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten von Nutzern im Vereinigten Königreich umgesetzt hatte ([109]).

(69) Seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 hat das Büro des Information Commissioner auch eine beträchtliche Zahl von Leitlinien, Stellungnahmen und anderen Leitfäden ausgearbeitet und veröffentlicht, in denen die Anwendung der Datenschutzvorschriften in wichtigen Bereichen wie Gesichtserkennung, Fairness bei künstlicher Intelligenz, Daten von Kindern, Direktwerbung, Videoüberwachung, Recht auf Auskunft, Transparenz in der Gesundheits- und Sozialfürsorge usw. für verschiedene Zielgruppen, darunter kleine und mittlere Unternehmen, bestimmte Einrichtungen wie Schulen, Kindergärten oder kleine Behörden, sowie für Unternehmen im Allgemeinen, die breite Öffentlichkeit oder betroffene Personen präzisiert wird ([110]).

3. EINSCHLÄGIGE ENTWICKLUNGEN IN BEZUG AUF DEN ZUGANG ZU UND DIE VERWENDUNG VON AUS DER EUROPÄISCHEN UNION ÜBERMITTELTEN PERSONENBEZOGENEN DATEN DURCH BEHÖRDEN IM VEREINIGTEN KÖNIGREICH

3.1. Allgemeiner Rechtsrahmen

(70) Das Vereinigte Königreich ist weiterhin Mitglied des Europarats, beachtet weiterhin die Europäische Menschenrechtskonvention und untersteht weiterhin der Gerichtsbarkeit des Europäischen Gerichtshofs für Menschenrechte. Daher unterliegt es nach wie vor den völkerrechtlich verankerten Verpflichtungen, wie sie in den Erwägungsgründen 116 bis 119 des Durchführungsbeschlusses (EU) 2021/1772 beschrieben sind und die den Rahmen für sein System des staatlichen Zugriffs bilden, und zwar auf der Grundlage von Grundsätzen, Garantien und individuellen Rechten, die mit denen identisch sind, die für die 27 Mitgliedstaaten als Vertragspartei der EMRK gelten und die sich weitgehend in der einschlägigen Rechtsprechung des Gerichtshofs der Europäischen Union niederschlagen.

(71) Wie in den Erwägungsgründen 121 bis 132 des Durchführungsbeschlusses (EU) 2021/1772 analysiert, werden im DPA 2018 weiterhin besondere Datenschutzgarantien und -rechte für Fälle gewährt, in denen Daten durch Behörden, einschließlich Strafverfolgungsbehörden und nationaler Sicherheitsorgane, verarbeitet werden. Mit dem Data (Use and Access) Act wurden nur begrenzte und gezielte Änderungen an denjenigen Teilen des DPA 2018 vorgenommen, die die Vorschriften für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Strafverfolgung (Teil 3 DPA 2018) und der nationalen Sicherheit (Teil 4 DPA 2018) enthalten.

([104]) Jahresbericht und Jahresabschluss 2021-2022, 2022-2023 und 2023-2024 des Information Commissioner. Siehe auch Durchführungsbeschluss (EU) 2021/1772, Erwägungsgrund 96.

([105]) Jahresbericht 2023-2024 des Information Commissioner, Seite 41.

([106]) Jahresbericht und Jahresabschluss 2021-2022, 2022-2023 und 2023-2024 des Information Commissioner.

([107]) Weitere Informationen zu diesen und weiteren Durchsetzungsmaßnahmen finden Sie auf der ICO-Website unter folgendem Link: https://ico.org.uk/action-weve-taken/enforcement/.

([108]) Weitere Informationen finden Sie unter folgendem Link: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.

([109]) Weitere Informationen finden Sie unter folgendem Link: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.

([110]) Abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) In Bezug auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sind in Teil 3 des DPA 2018 weiterhin Grundsätze, Rechte und Pflichten vorgesehen, die denen der Richtlinie (EU) 2016/680 ähnlich sind ([111]).

(73) Insbesondere hat die Kommission am Tag der Annahme dieses Beschlusses einen weiteren Beschluss auf der Grundlage von Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 angenommen, nach dem die Datenschutzregelung, die für die Verarbeitung durch Strafverfolgungsbehörden des Vereinigten Königreichs zum Zwecke der Strafverfolgung gilt, für ein Schutzniveau sorgt, das der Sache nach dem durch die Richtlinie (EU) 2016/680 garantierten Schutzniveau gleichwertig ist.

(74) Mit dem Data (Use and Access) Act wurden bestehende Ausnahmen in Teil 3 des DPA 2018, die den zuständigen Behörden für Zwecke der nationalen Sicherheit zur Verfügung stehen, geändert und konsolidiert. Die Ausnahme aus Gründen der nationalen Sicherheit ermöglicht es den zuständigen Behörden, bestimmte Bestimmungen von Teil 3 des DPA 2018 nicht anzuwenden, wenn eine Ausnahme von dieser Bestimmung zum Schutz der nationalen Sicherheit erforderlich ist ([112]). Sie entspricht den Ausnahmen für die Verarbeitung personenbezogener Daten im Bereich der nationalen Sicherheit, wie sie unter der UK GDPR (Paragraf 26 der DPA 2018) und unter Teil 4 der DPA 2018 (Paragraf 110 der DPA 2018) vorgesehen sind.

(75) Die Ausnahme aus Gründen der nationalen Sicherheit unterliegt denselben Beschränkungen und Garantien wie die Ausnahmen gemäß der UK GDPR und Teil 4 des DPA 2018, wie in den Erwägungsgründen 64 bis 67 und 126 des Durchführungsbeschlusses (EU) 2021/1772 analysiert. Insbesondere kann die Ausnahme nur angewendet werden, wenn und soweit sie zum Schutz der nationalen Sicherheit erforderlich ist. Sie stellt keine pauschale Ausnahme dar und muss vom Verantwortlichen von Fall zu Fall geprüft und in Anspruch genommen werden ([113]). Darüber hinaus muss jede Anwendung der Ausnahme mit den Menschenrechtsstandards in Einklang stehen (gestützt auf den Human Rights Act 1998 und die Europäische Menschenrechtskonvention), nach denen jeder Eingriff in das Recht auf Privatsphäre notwendig und verhältnismäßig in einer demokratischen Gesellschaft sein muss ([114]). Dies wird auch in den Leitlinien der ICO zur Anwendung von Ausnahmen im Bereich der nationalen Sicherheit bestätigt ([115]).

(76) Auf der Grundlage der mit dem Data (Use and Access) Act eingeführten Änderungen ([116]) kann eine bestimmte Verarbeitungstätigkeit durch die für die Strafverfolgung zuständigen Behörden auch durch die Bestimmungen von Teil 4 des DPA 2018 geregelt werden, der normalerweise nur für die Verarbeitung von Daten durch nationale Sicherheitsbehörden gilt.

([111]) Mit Paragraf 69 des Data (Use and Access) Act werden die Definition des Begriffs „Einwilligung" und die Bedingungen für die Berufung auf die Einwilligung gemäß Artikel 4 Absatz 11 und Artikel 7 UK GDPR (welche die entsprechenden Bestimmungen der Verordnung (EU) 2016/679 widerspiegeln) als neue Paragrafen 33 Absatz 1A und 40A in den DPA 2018 aufgenommen, wodurch der Begriff der Einwilligung und die Bedingungen für die Berufung auf die Einwilligung präzisiert werden, wenn sie als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Strafverfolgung verwendet werden. Darüber hinaus wird in Paragraf 71 Absätze 7 und 8 des Data (Use and Access) Act der Wortlaut von Paragraf 36 Absatz 1 DPA 2018 leicht präzisiert. Schließlich werden gegebenenfalls Änderungen an der UK GDPR durch den Data (Use and Access) Act, wie in Paragraf 2 beschrieben, auch in Teil 3 des DPA 2018 berücksichtigt, siehe beispielsweise Paragraf 74 Absätze 2 bis 5 über die Verarbeitung sensibler Daten, Paragraf 76 Absätze 4 bis 6 in Bezug auf die Fristen für die Beantwortung von Anträgen der betroffenen Person, Paragraf 78 Absätze 2 und 3 in Bezug auf Abfragen auf Ersuchen betroffener Personen und Paragraf 80 Absätze 3 bis 5 über die automatisierte Entscheidungsfindung.

([112]) Paragraf 78A Absatz 1 des DPA 2018, eingeführt durch Paragraf 88 des Data (Use and Access) Act. Gemäß Paragraf 78A Absätze 2 bis 4 der DPA 2018 erlaubt die Ausnahme, die Datenschutzgrundsätze (außer dem Grundsatz der Rechtmäßigkeit sowie den Bedingungen und Schutzvorkehrungen für die Verarbeitung sensibler Daten), die Rechte der Betroffenen, die Pflichten der Verantwortlichen und Auftragsverarbeiter in Bezug auf Datenschutzverletzungen, bestimmte Teile der Vorschriften zu internationalen Datenübermittlungen sowie einige Befugnisse der Information Commissioner zur Durchführung von Inspektionen und zur Durchsetzung außer Kraft zu setzen.

([113]) Siehe Baker v Secretary of State for the Home Department [2001] UKIT NSA2 („Baker v Secretary of State").

([114]) Siehe auch *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), Rn. 45; Lin/Commissioner of the Police for the Metropolis, [2015] EWHC 2484 (QB), Rn. 80.

([115]) Siehe Leitfaden des ICO über die Ausnahme zum Schutz der nationalen Sicherheit oder für Verteidigungszwecke, abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Paragrafen 89 bis 90 des Data (Use and Access) Act.

(77) Während die Datenschutzregelung für die Verarbeitung zu Zwecken der nationalen Sicherheit somit in bestimmten Fällen auch auf die Datenverarbeitung durch Strafverfolgungsbehörden ausgeweitet wird, ist dies nur unter bestimmten Umständen und unter strengen Bedingungen und Garantien der Fall, d. h. wenn i) eine zuständige Behörde in den vom Secretary of State erlassenen Verordnungen, die der Zustimmung des Parlaments bedürfen, als „qualifizierte zuständige Behörde" bezeichnet wird ([117]) und ii) der Secretary of State mittels eines Bescheids eine bestimmte Verarbeitungstätigkeit der qualifizierten zuständigen Behörde benennt. Wichtig ist, dass eine solche Benennung nur erfolgen kann, wenn der Secretary of State der Auffassung ist, dass die Benennung der Verarbeitungstätigkeit zum Schutz der nationalen Sicherheit erforderlich ist, d. h., wenn eine Strafverfolgungsbehörde aus Gründen der nationalen Sicherheit handelt und die Verarbeitungstätigkeit von der qualifizierten zuständigen Behörde als gemeinsam Verantwortlicher mit mindestens einem Nachrichtendienst durchgeführt wird ([118]). Als weitere Garantien muss der Secretary of State den Commissioner konsultieren, bevor er eine Benennungsmitteilung abgibt ([119]), der Wortlaut der Bekanntmachung muss grundsätzlich veröffentlicht werden ([120]), und eine Person, die von einer Benennungsmitteilung unmittelbar betroffen ist, kann eine gerichtliche Überprüfung beantragen ([121]). Daher soll mit dieser Änderung im Wesentlichen klargestellt werden, dass in Fällen, in denen die Behörden des Vereinigten Königreichs sowohl für die Strafverfolgung als auch für die nationale Sicherheit zuständig sind und Daten im Rahmen ihrer letztgenannten Zuständigkeiten verarbeiten, die Datenschutzregelung für nationale Sicherheitsdienste gilt.

(78) Teil 4 des DPA 2018 regelt die Datenverarbeitung durch Nachrichtendienste des Vereinigten Königreichs. Wie in den Erwägungsgründen 125 bis 132 des Durchführungsbeschlusses (EU) 2021/1772 beschrieben, werden weiterhin die wichtigsten Datenschutzgrundsätze, Bedingungen für die Verarbeitung besonderer Kategorien von Daten, die Rechte betroffener Personen, Datenschutz durch Technikgestaltung sowie die Übermittlung personenbezogener Daten geregelt.

(79) Die Änderungen an dieser Regelung, die durch den Data (Use and Access) Act eingeführt wurden, sind begrenzt. In Bezug auf das Auskunftsrecht der betroffenen Personen nach Paragraf 94 DPA 2018 wird mit dem Data (Use and Access) Act ein neuer Unterabsatz 2A eingeführt, in dem klargestellt wird, dass die betroffene Person nur insoweit Anspruch auf die einschlägigen Informationen hat, als die verantwortliche Person in der Lage ist, sie auf der Grundlage einer angemessenen und verhältnismäßigen Suche zur Verfügung zu stellen ([122]). Wie in Erwägungsgrund 35 erläutert, bildet diese Änderung den Rahmen für das Auskunftsrecht auf der Grundlage etablierter rechtlicher Standards, die auch die Interessen der betroffenen Person berücksichtigen. Im Bereich der automatisierten Entscheidungsfindung ist es den Verantwortlichen weiterhin untersagt, eine Entscheidung zu treffen, die eine betroffene Person erheblich beeinträchtigt und ausschließlich auf einer automatisierten Verarbeitung der sie betreffenden personenbezogenen Daten beruht, es sei denn, eine solche Entscheidung ist gesetzlich vorgeschrieben oder zulässig, die betroffene Person hat in die auf dieser Grundlage getroffene Entscheidung eingewilligt oder die Entscheidung wird im Zusammenhang mit einem Vertrag getroffen ([123]); mit dem Data (Use and Access) Act wird in Teil 4 des DPA 2018 ([124]) dieselbe Definition des Begriffs „ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungen" eingeführt, wie sie in Artikel 22A UK GDPR enthalten ist und in Erwägungsgrund 53 dieses Beschlusses analysiert wird.

3.2. **Einschlägige Entwicklungen in Bezug auf den Zugriff und die Verwendung durch Behörden des Vereinigten Königreichs für Strafverfolgungszwecke**

(80) Das Recht des Vereinigten Königreichs umfasst weiterhin eine Reihe von wichtigen Beschränkungen für den Zugang zu und die Verwendung von personenbezogenen Daten für Zwecke der Strafverfolgung; ferner sieht es für diesen Bereich Aufsichtsmechanismen und Rechtsbehelfe vor, die in den Erwägungsgründen 134 bis 174 des Durchsetzungsbeschlusses (EU) 2021/1772 analysiert werden.

([117]) Paragraf 82 Absätze A1, 2A und 4 DPA 2018, eingeführt durch Paragraf 89 Absatz 2 des Data (Use and Access) Act.

([118]) Paragraf 82A Absätze 1 und 2, eingeführt durch Paragraf 89 Absatz 3 des Data (Use and Access) Act. Als weitere Garantien muss der Secretary of State den Commissioner konsultieren, bevor er einen Benennungsbescheid herausgibt, siehe den neuen Paragraf 82A Absatz 8 DPA 2018, muss der Wortlaut des Bescheids grundsätzlich veröffentlicht werden, siehe den neuen Paragraf 82D Absatz 1 vorbehaltlich der in dem neuen Paragraf 82D Absatz 3 DPA 2018 festgelegten Ausnahmen, und kann eine von einem Benennungsbescheid unmittelbar betroffene Person eine gerichtliche Überprüfung beantragen, siehe neuer Paragraf 82E des DPA 2018.

([119]) Paragraf 82A Absatz 8 des DPA 2018.

([120]) Paragraf 82D Absatz 1 DPA 2018, vorbehaltlich der in dem neuen Paragrafen 82D Absatz 3 DPA 2018 festgelegten Ausnahmen.

([121]) Paragraf 82E des DPA 2018.

([122]) Paragraf 78 Absatz 4 des Data (Use and Access) Act.

([123]) Paragraf 96 DPA 2018.

([124]) Nach dem neuen Paragraf 96 Absatz 4 DPA 2018 beruht eine Entscheidung auf einer vollständig automatisierten Verarbeitung, wenn der Entscheidungsprozess keine Möglichkeit für einen Menschen umfasst, die Entscheidung anzunehmen, abzulehnen oder zu beeinflussen. Siehe Paragraf 80 Absatz 4 Buchstabe c des Data (Use and Access) Act.

3.2.1. *Rechtsgrundlagen und anwendbare Beschränkungen/Garantien*

(81) Vorbehaltlich der in den Erwägungsgründen 135 bis 138 des Durchführungsbeschlusses (EU) 2021/1772 beschriebenen Bedingungen und Garantien ist die Erhebung personenbezogener Daten von Unternehmern im Vereinigten Königreich zum Zwecke der Strafverfolgung in der Rechtsordnung des Vereinigten Königreichs auf der Grundlage von Durchsuchungsanordnungen und Herausgabeanordnungen weiterhin zulässig.

(82) Darüber hinaus hat der National Security Act 2023 ([125]), mit dem Bedrohungen der nationalen Sicherheit durch Spionage, Sabotage und Personen, die für ausländische Mächte handeln, bekämpft werden sollen, der britischen Polizei neue Befugnisse zum Zugang, zur Durchsuchung und zur Beschlagnahme eingeräumt, einschließlich der Möglichkeit, personenbezogene Daten zu erlangen, wenn der begründete Verdacht besteht, dass Material beschafft werden kann, das wahrscheinlich als Beweis dafür dient, dass eine der schwerwiegenderen Straftaten oder Aktivitäten zur Bedrohung durch ausländische Mächte gemäß dem National Security Act 2023 begangen wurde oder kurz vor der Begehung steht ([126]). Diese Befugnisse unterliegen ähnlichen Bedingungen und Garantien wie denen, die im Durchführungsbeschluss (EU) 2021/1772 für die zu diesem Zeitpunkt bestehenden Befugnisse analysiert wurden. Insbesondere muss ihre Verwendung durch einen Beschluss, eine Vorlageverfügung oder eine Auskunftsverfügung einer unabhängigen Justizbehörde auf Antrag der Polizei/Ermittlungsbehörde genehmigt werden ([127]). Für vertrauliches Material wie journalistisches Material und Gegenstände, die einem Rechtsprivileg unterliegen, gibt es einen besonderen Schutz ([128]). Ebenso muss der Erlass von Offenlegungsanordnungen („disclosure orders") ([129]), Kundeninformationsanordnungen („customer information orders") ([130]) und Kontoüberwachungsanordnungen („account monitoring orders") ([131]), der auch im National Security Act 2023 vorgesehen ist, von einem Richter auf Antrag eines zuständigen Beamten genehmigt werden und unterliegt bestimmten Bedingungen und Garantien, darunter, dass die Anordnung in Bezug auf eine bestimmte Person zum Zwecke der Untersuchung von Aktivitäten ausländischer Mächte beantragt wird, dass die Anordnung die Wirksamkeit der Untersuchung erhöht und dass sie nicht dazu verwendet wird, um Informationen zu erhalten, die gesetzlich geschützt oder anderweitig ausgeschlossen sind, wie z. B. journalistisches Material und bestimmte Gesundheitsakten ([132]).

(83) Wie in den Erwägungsgründen 139 bis 141 des Durchführungsbeschlusses (EU) 2021/1772 beschrieben, können im Rechtsrahmen des Vereinigten Königreichs bestimmte Strafverfolgungsbehörden, z. B. die National Crime Agency oder der Metropolitan Police Service, auch gezielte Ermittlungsbefugnisse im Rahmen des Gesetzes über Ermittlungsbefugnisse 2016 (Investigatory Powers Act, IPA 2016) ([133]) nutzen, um schwere Straftaten zu verhüten oder aufzudecken. Die spezifischen Ermittlungsbefugnisse, auf die sich diese Strafverfolgungsbehörden stützen können, sind das gezielte Abfangen von Informationen (Teil 2 des IPA 2016), die Erfassung von Kommunikationsdaten (Teil 3 des IPA 2016) und gezielte Geräteüberwachung (Teil 5 des IPA 2016). Werden Vorratsspeicherungsanordnungen vom Secretary of State nach Teil 4 des IPA 2016 erlassen, kann die Strafverfolgung auch davon profitieren, wenn sie über die Befugnisse zur Erhebung von Kommunikationsdaten nach Teil 3 des IPA 2016 auf die auf Vorrat gespeicherten Kommunikationsdaten zugreifen kann.

([125]) Abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) Anhang 2 des National Security Act 2023. Relevante Straftaten nach dem National Security Act 2023 sind beispielsweise die Erlangung oder Offenlegung geschützter Informationen (Paragraf 1), die Erlangung oder Offenlegung von Geschäftsgeheimnissen (Paragraf 3), die Unterstützung ausländischer Nachrichtendienste (Paragraf 4), die Durchführung von Sabotage (Paragraf 12) oder die Ausübung bestimmter verbotener Handlungen für eine ausländische Macht mit der Absicht, eine Störwirkung zu erzielen (Paragraf 13).

([127]) Siehe Anhang 2 Paragraf 2 Absatz 1, Paragraf 3 Absatz 1, Paragraf 4 Absatz 1 und Paragraf 10 Absatz 1 des National Security Act 2023.

([128]) Siehe Anhang 2 Paragraf 2 Absatz 4 Buchstabe b, Paragraf 3 Absatz 4 Buchstabe b und c, Paragraf 4 Absatz 4 Buchstabe b und c und Paragraf 10 Absatz 1 des National Security Act 2023.

([129]) Mittels Offenlegungsanordnungen gemäß dem Anhang 3 des National Security Act 2023 kann ein Beamter eine Person auffordern, Informationen bereitzustellen, Dokumente vorzulegen und/oder Fragen zu beantworten, die für eine Untersuchung zur Identifizierung von Vermögenswerten im Zusammenhang mit Aktivitäten ausländischer Mächte, einschließlich der Bewegung oder Nutzung dieser Vermögenswerte, relevant sind.

([130]) Mittels Kundeninformationsanordnungen gemäß dem Anhang 4 des National Security Act 2023 kann ein Beamter ein Finanzinstitut auffordern, Kundeninformationen zu einer bestimmten Person bereitzustellen.

([131]) Mittels Kontoüberwachungsanordnungen nach Anhang 5 kann von einem Finanzinstitut verlangt werden, einem Beamten für den in der Anordnung festgelegten Zeitraum, der 90 Tage nicht überschreiten darf, und in der darin festgelegten Weise die in der Anordnung genannten Informationen bereitzustellen.

([132]) Anhang 3 Paragraf 2 Absatz 1, Anhang 4 Paragraf 1, Anhang 5 Paragraf 1 des National Security Act 2023.

([133]) Der Investigatory Powers Act 2016 (siehe: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) ersetzte eine Reihe von Gesetzen über das Abfangen von Kommunikationsvorgängen, den Zugriff auf Geräte und die Beschaffung von Kommunikationsdaten, insbesondere Teil I des RIPA 2000, der zuvor den allgemeinen Rechtsrahmen für die Ausübung von Ermittlungsbefugnissen durch Strafverfolgungs- und nationale Sicherheitsbehörden bildete.

(84) Seit der Verabschiedung des Durchführungsbeschlusses (EU) 2021/1772 bildet das IPA 2016 zusammen mit dem Regulation of Investigatory Powers Act 2000 (RIPA) für England, Wales und Nordirland und dem Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) für Schottland weiterhin die Rechtsgrundlage und legt die geltenden Beschränkungen und Garantien für die Ausübung dieser Befugnisse fest, wie im Durchführungsbeschluss (EU) 2021/1772 beschrieben. Wichtig ist, dass nach dem Rechtsrahmen weiterhin vorgeschrieben ist, dass die Behörden für die Ausübung dieser Befugnisse eine Anordnung ([134]) benötigen, die von einer zuständigen Behörde ([135]) ausgestellt und von einem unabhängigen Justizbeauftragten (Judicial Commissioner) ([136]) genehmigt wird („Double-Lock"-Verfahren). Die Ausstellung einer solchen Anordnung unterliegt weiterhin einer Erforderlichkeits- und Verhältnismäßigkeitsprüfung ([137]).

(85) Gleichzeitig wurden seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 mit dem Investigatory Powers (Amendment) Act 2024, der im April 2024 die Königliche Zustimmung erhielt, bestimmte spezifische Elemente des IPA 2016 geändert ([138]). Soweit sich diese Änderungen und andere einschlägige Entwicklungen auf die Bedingungen, Beschränkungen und Garantien im Zusammenhang mit der Nutzung der oben genannten spezifischen Ermittlungsbefugnisse durch Behörden im Vereinigten Königreich zu Strafverfolgungszwecken beziehen, wie in den Erwägungsgründen 177 bis 215 des Durchführungsbeschlusses (EU) 2021/1772 bewertet, werden sie in den folgenden Absätzen analysiert. In Bezug auf Elemente des Rechtsrahmens des Vereinigten Königreichs, die nicht durch das oben genannte Gesetz geändert wurden oder von anderen einschlägigen Entwicklungen betroffen sind, ist die Analyse im Durchführungsbeschluss (EU) 2021/1772 weiterhin gültig.

(86) Was die gezielte Beschaffung und gezielte Speicherung von Kommunikationsdaten ([139]) betrifft, so bleiben die Bedingungen und Garantien für diese Befugnisse, wie sie im Durchführungsbeschluss (EU) 2021/1772 bewertet wurden, in Kraft. Mit dem Investigatory Powers (Amendment) Act 2024 wurden die bestehenden Garantien präzisiert, indem in Paragraf 11 des IPA 2016 (in dem die unrechtmäßige Erlangung von Kommunikationsdaten von einem Telekommunikationsbetreiber als Straftat eingestuft wird) eine Liste von Beispielen dafür eingeführt wurde, was in dieser Bestimmung als „gesetzliche Befugnis" zu verstehen ist ([140]). Darüber hinaus wurde im Investigatory Powers (Amendment) Act 2024 die Definition von Kommunikationsdaten in Paragraf 261 IPA 2016 weiter präzisiert, indem ausdrücklich festgelegt wurde, dass Teilnehmerdaten als Kommunikationsdaten gelten ([141]).

([134]) In Teil 2 Kapitel 2 des IPA 2016 ist eine begrenzte Anzahl von Fällen aufgeführt, in denen Abfangmaßnahmen ohne eine entsprechende Anordnung durchgeführt werden können. Zum Beispiel: das Abfangen mit Zustimmung des Absenders oder des Empfängers, das Abfangen zu Verwaltungs- oder Durchsetzungszwecken, das Abfangen in bestimmten Einrichtungen (Gefängnissen, psychiatrischen Kliniken und Gewahrsamseinrichtungen für Immigranten) sowie das Abfangen im Rahmen eines einschlägigen internationalen Abkommens.

([135]) In den meisten Fällen wird die Anordnung vom Secretary of State gemäß dem IPA 2016 ausgestellt; in Schottland hingegen sind Minister befugt, Anordnungen für gezieltes Abfangen, Amtshilfeanordnungen und Anordnungen für gezielten Gerätezugriff auszustellen, wenn sich die zu überwachenden Personen oder Räumlichkeiten und die zu überwachenden Geräte in Schottland befinden (siehe Paragrafen 22 und 103 IPA 2016). Im Falle eines gezielten Gerätezugriffs kann ein Leiter einer Strafverfolgungsbehörde (im Sinne von Anhang 6 Teile 1 und 2 des IPA 2016) die Anordnung unter den Bedingungen von Paragraf 106 IPA 2016 erlassen.

([136]) Judicial Commissioners unterstützen den Beauftragten für Ermittlungsbefugnisse (Investigatory Powers Commissioner — IPC), ein unabhängiges Gremium, das die Nutzung von Ermittlungsbefugnissen durch Nachrichtendienste beaufsichtigt.

([137]) Siehe insbesondere Paragrafen 19 und 23 des IPA 2016.

([138]) Abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) Der Begriff „Kommunikationsdaten" („communications data") bezieht sich auf das „Wer", „Wann", „Wo" und „Wie" eines Kommunikationsvorgangs, nicht aber auf den Inhalt, d. h., was gesagt oder geschrieben wurde. Kommunikationsdaten könnten den Zeitpunkt und die Dauer eines Kommunikationsvorgangs, die Telefonnummer oder E-Mail-Adresse des Urhebers und des Empfängers und mitunter auch den Standort der Geräte, von denen aus die Kommunikation erfolgte, umfassen (siehe Paragraf 261 Absatz 5 IPA 2016). Gemäß dem IPA 2016 darf der Secretary of State Telekommunikationsbetreiber auffordern, Kommunikationsdaten zu speichern, damit bestimmte Behörden, einschließlich Strafverfolgungsbehörden und Nachrichtendiensten, gezielt darauf zugreifen können. In Teil 4 des IPA 2016 ist die Speicherung von Kommunikationsdaten, in Teil 3 die gezielte Beschaffung von Kommunikationsdaten geregelt. Des Weiteren sind in den Teilen 3 und 4 des IPA 2016 spezifische Einschränkungen für die Nutzung dieser Befugnisse sowie spezifische Garantien vorgesehen.

([140]) Wenn beispielsweise die betreffende Person die Kommunikationsdaten in Ausübung einer gesetzlichen Befugnis der zuständigen Behörde erhält oder wenn die Kommunikationsdaten aufgrund einer gerichtlichen Anordnung oder einer anderen richterlichen Genehmigung erhoben werden. Paragraf 11 Absatz 3A IPA 2016, eingeführt durch Paragraf 12 Absatz 3 des Investigatory Powers (Amendment) Act 2024.

([141]) Paragraf 261 Absätze 5A und 5B, eingeführt durch Paragraf 13 Absatz 3 des Investigatory Powers (Amendment) Act 2024.

(87) Die Ausstellung von Anordnungen zur Speicherung von Kommunikationsdaten ([142]) unterliegt weiterhin Beschränkungen und Garantien, wie in den Erwägungsgründen 208 und 209 des Durchführungsbeschlusses (EU) 2021/1772 beschrieben, insbesondere Anforderungen an die Notwendigkeit und Verhältnismäßigkeit sowie die Genehmigung durch einen unabhängigen Judicial Commissioner. Zwar wurde mit dem Investigatory Powers (Amendment) Act 2024 die Möglichkeit eingeführt, solche Anordnungen zu verlängern, jedoch unterliegt jede Verlängerung denselben Bedingungen der Notwendigkeit und Verhältnismäßigkeit und der Genehmigung durch den Judicial Commissioner ([143]).

(88) In Bezug auf Kommunikationsdaten wurde mit dem Investigatory Powers (Amendment) Act 2024 auch die Definition eines Telekommunikationsbetreibers geändert, d. h. der möglichen Adressaten einer Vorratsspeicherungsanordnung. Diese 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 einen Telekommunikationsdienst anzubieten oder bereitzustellen“ ([144]). Wichtig ist, dass die geänderte Definition weiterhin stets eine enge Verbindung zum Markt des Vereinigten Königreichs erfordert. Mit der Änderung wird somit klargestellt, dass große Unternehmen mit komplexen Unternehmensstrukturen in ihrer Gesamtheit unter das IPA 2016 fallen, ohne dass der Anwendungsbereich der Begriffsbestimmung auf Anbieter von Telekommunikationsdiensten ausgeweitet wird, die sich nicht an Personen im Vereinigten Königreich richten. Dies wird auch durch die Erläuterungen zum Investigatory Powers (Amendment) Act 2024 bestätigt, in denen dargelegt wird, dass die Änderung nicht darauf abzielt, zusätzliche Unternehmen in den Anwendungsbereich der einschlägigen Befugnisse nach dem IPA 2016 ([145]) aufzunehmen, sondern dass sie im Wesentlichen eine Klarstellungsfunktion hat.

(89) Schließlich wurden mit dem Investigatory Powers (Amendment) Act 2024 einige gezielte Änderungen des Verfahrens für die Ausstellung von Haftbefehlen eingeführt, unter anderem in Bezug auf gezieltes Abfangen und gezielten Gerätezugriff, und zwar Befugnisse, die auch von bestimmten Strafverfolgungsbehörden im Vereinigten Königreich zur Verhütung oder Aufdeckung schwerer Straftaten genutzt werden können. Die Änderungen betreffen nur den besonderen Fall, dass diese Befugnisse genutzt werden, um Mitteilungen oder private Informationen über eine Person zu erhalten, die Mitglied einer einschlägigen Legislative ist ([146]). Während Anordnungen in Bezug auf gezieltes Abfangen und gezielte Geräteeingriffe in der Regel vom Secretary of State erlassen werden können und von einem Judicial Commissioner genehmigt werden (siehe Erwägungsgründe 186 bis 196 und 210 bis 215 des Durchführungsbeschlusses (EU) 2021/1772), ist nach den Paragrafen 26 und 111 des IPA zusätzlich die Genehmigung durch den Premierminister erforderlich, wenn die Anordnung ein Mitglied des Parlaments oder eine andere zuständige Legislative betrifft (das sogenannte Triple-lock- oder Dreifach-Sicherungsverfahren). Nach dem Investigatory Powers (Amendment) Act 2024 kann der Premierminister nun fünf Secretaries of State benennen, die ermächtigt sind, die Befugnis des Premierministers zur Genehmigung dieser Anordnungen auszuüben, sofern eine Genehmigung dringend erforderlich ist und der Premierminister aufgrund medizinischer Unfähigkeit oder fehlenden Zugangs zu sicheren Kommunikationsmitteln nicht in der Lage ist, diese zu genehmigen. Wichtig ist, dass die in den oben genannten Erwägungsgründen des Durchführungsbeschlusses (EU) 2021/1772 beschriebenen Beschränkungen und Garantien in Bezug auf die Ausstellung dieser Anordnungen bestehen bleiben.

3.2.2. *Weiterverwendung der erhobenen Daten*

(90) Für die Weitergabe von Daten durch eine Strafverfolgungsbehörde an eine andere Behörde zu anderen Zwecken als denen, für die sie ursprünglich erhoben wurden, (die sogenannte Weitergabe — „onward sharing“) gelten weiterhin die Bedingungen, die in den Erwägungsgründen 142 bis 156 des Durchsetzungsbeschlusses (EU) 2021/1772 analysiert wurden.

([142]) Mit dem Erlass einer solchen Speicherungsanordnung nach den Paragrafen 87 bis 89 des IPA 2016 soll sichergestellt werden, dass Telekommunikationsbetreiber relevante Kommunikationsdaten, die andernfalls gelöscht würden, sobald sie nicht mehr für geschäftliche Zwecke benötigt werden, für einen Zeitraum von maximal 12 Monaten speichern. Die gespeicherten Daten müssen so lange zur Verfügung stehen, wie es für den Fall erforderlich wäre, dass eine Behörde sie nachträglich im Rahmen einer in Teil 3 des IPA 2016 vorgesehenen Genehmigung für eine gezielte Beschaffung von Kommunikationsdaten beschaffen muss.

([143]) Paragraf 94A des IPA 2016, eingeführt durch Paragraf 20 Absatz 4 des Investigatory Powers (Amendment) Act 2024.

([144]) Paragraf 261 Absatz 10 Buchstabe c IPA 2016, eingeführt durch Paragraf 19 des Investigatory Powers (Amendment) Act 2024.

([145]) Erläuterungen zum Investigatory Powers (Amendment) Act 2024, Paragraf 359, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Siehe Paragrafen 26 und 111 IPA 2016.

(91) Was die besondere Situation der Weiterübermittlungen aus dem Vereinigten Königreich in die Vereinigten Staaten betrifft, so ist das im Oktober 2019 geschlossene Abkommen zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugang zu elektronischen Daten zur Bekämpfung von schwerer Kriminalität (im Folgenden das „Abkommen zwischen dem Vereinigten Königreich und den USA“) ([147]) in Kraft getreten und wird seit Oktober 2022 umgesetzt. Nach dem Abkommen zwischen dem Vereinigten Königreich und den USA könnten Daten, die aus der EU an Dienstleister im Vereinigten Königreich übermittelt werden, Gegenstand von Anordnungen zur Herausgabe von Beweismitteln sein, die von den zuständigen US-amerikanischen Strafverfolgungsbehörden erlassen wurden und im Vereinigten Königreich anwendbar sind.

(92) Wichtig ist, dass die Bedingungen und Garantien, unter denen solche Anordnungen erlassen und ausgeführt werden können, wie in Erwägungsgrund 154 des Durchführungsbeschlusses (EU) 2021/1772 bewertet, weiterhin gelten. Insbesondere genießen die im Rahmen des Abkommens erlangten Daten einen Schutz, der den besonderen Garantien des sogenannten Rahmenabkommens zwischen der EU und den USA ([148]) gleichwertig ist, die alle sinngemäß in das Abkommen zwischen dem Vereinigten Königreich und den USA aufgenommen wurden ([149]).

(93) Seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 hat das Vereinigte Königreich erklärt, dass es unter anderem im Rahmen der Umsetzung des Abkommens zwischen dem Vereinigten Königreich und den Vereinigten Staaten in Zusammenarbeit mit den relevanten Parteien klargestellt hat, wie die spezifischen Garantien des Rahmenabkommens, die für die Zusammenarbeit zwischen Strafverfolgungsbehörden konzipiert wurden, angepasst und auf die spezifischen Übermittlungen, die unter das Abkommen zwischen dem Vereinigten Königreich und den USA fallen, angewandt werden. Insbesondere hat das Vereinigte Königreich erläutert, dass die Bestimmungen des Rahmenabkommens, in denen eine Rolle für die zuständige Behörde vorgesehen ist (die es in einer Situation der direkten Zusammenarbeit zwischen einem Diensteanbieter des Vereinigten Königreichs und einer Strafverfolgungsbehörde in den USA nicht gibt), sinngemäß dahin ausgelegt werden, dass sie sich auf die benannte Behörde (im Sinne des Abkommens zwischen dem Vereinigten Königreich und den USA) ([150]) der betreffenden Vertragspartei beziehen.

(94) Beispielsweise hat das Vereinigte Königreich in Bezug auf die Meldung eines Datensicherheitsvorfalls gemäß Artikel 10 des Rahmenabkommens zwischen der EU und den USA, der eine Benachrichtigung der übermittelnden zuständigen Behörde erfordert, erklärt, dass diese Bestimmung entsprechend gilt, sodass die Meldung an die benannte Behörde der Partei zu richten ist, von der die Daten übermittelt wurden.

(95) In Bezug auf die Zustimmung der übermittelnden zuständigen Behörde vor jeder Weiterübermittlung personenbezogener Daten gemäß Artikel 7 des Rahmenabkommens hat das Vereinigte Königreich klargestellt, dass es diese Bestimmung entsprechend anwenden wird, sodass die benannte Behörde der Vertragspartei, von der die Daten übermittelt wurden, jeder Weiterübermittlung zustimmen muss.

(96) In Bezug auf die Verpflichtungen nach Artikel 8 des Rahmenabkommens zur Aufrechterhaltung der Qualität und der Vollständigkeit der Daten würde eine sinngemäße Auslegung der Bestimmung dazu führen, dass die benannte Behörde der Vertragspartei, die die Daten erhält, für die Kontaktaufnahme mit dem Anbieter, der die Daten übermittelt hat, verantwortlich ist, falls Probleme hinsichtlich der Datenqualität und -vollständigkeit auftreten.

([147]) Abkommen zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugang zu elektronischen Daten zur Bekämpfung von schwerer Kriminalität, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([148]) Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten (ABl. L 336 vom 10.12.2016, S. 3, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Artikel 9 Absatz 1 des Abkommens.

([150]) Nach Artikel 1 Absatz 8 des Abkommens zwischen dem Vereinigten Königreich und den USA bezeichnet der Ausdruck „benannte Behörde“ („designated authority“) die staatliche Stelle, die für das Vereinigte Königreich vom Secretary of State for the Home Department und für die Vereinigten Staaten vom Attorney General benannt wurde.

(97) Mit Blick auf den Rechtsbehelf hat das Vereinigte Königreich betont, dass bei Übermittlungen im Rahmen des Abkommens zwischen dem Vereinigten Königreich und den Vereinigten Staaten stets die benannten Behörden der Vertragsparteien beteiligt ist. Wenn die USA die Vertragspartei sind, die Daten von Diensteanbietern im Vereinigten Königreich erhält, handelt das US-Justizministerium als benannte Behörde. Daher wird nach der Auslegung des Vereinigten Königreichs bei jedem auf der Grundlage des Abkommens zwischen dem Vereinigten Königreich und den Vereinigten Staaten gestellten Ersuchen das Justizministerium als gemäß dem US Judicial Redress Act benannte Bundesbehörde beteiligt sein, sodass gemäß Artikel 19 des Rahmenabkommens ein Rechtsbehelf gegen das Justizministerium eingelegt werden kann. Darüber hinaus hat das Vereinigte Königreich gegenüber den Kommissionsdienststellen bestätigt, dass der Judicial Redress Act nicht der einzige Rechtsbehelfsmechanismus ist. Je nach den Umständen und dem Kontext des Einzelfalls sind nach anderen geltenden US-Rechtsvorschriften alternative Wege vorgesehen, über die Rechtsbehelfe eingelegt werden können.

3.2.3. *Aufsicht und Rechtsbehelfe*

(98) Je nach den Befugnissen, die die zuständigen Behörden bei der Verarbeitung personenbezogener Daten zu Strafverfolgungszwecken nutzen (sei es im Rahmen des DPA 2018 oder des IPA 2016), sorgen verschiedene Stellen weiterhin für die Aufsicht über die Ausübung dieser Befugnisse, wie in den Erwägungsgründen 158 bis 174 des Durchführungsbeschlusses (EU) 2021/1772 bewertet, und es stehen weiterhin Rechtsbehelfsmechanismen nach Teil 3 des DPA 2018, im Rahmen des IPA 2016 und im Rahmen des Menschenrechtsgesetzes von 1998 zur Verfügung, wie in den Erwägungsgründen 250 bis 269 des Durchführungsbeschlusses (EU) 2021/1772 analysiert.

(99) In Bezug auf die Aufsicht über Teil 3 des DPA 2018 werden die Funktionen und Befugnisse der Information Commission in den Erwägungsgründen 158 bis 160 und 162 des Durchführungsbeschlusses (EU) 2021/1772 vorbehaltlich der Änderungen analysiert, die mit dem in den Paragrafen 2.3.1 und 2.3.2 des vorliegenden Beschlusses beschriebenen Data (Use and Access) Act eingeführt wurden.

(100) Was die Umsetzung dieser Befugnisse betrifft, so hat der Information Commissioner seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 zahlreiche Beschwerden bearbeitet ([151]), mehrere Untersuchungen durchgeführt und Durchsetzungsmaßnahmen in Bezug auf die Datenverarbeitung durch Strafverfolgungsbehörden ergriffen. Zwischen 2021 und 2025 führte der Information Commissioner Untersuchungen durch und erteilte verschiedenen Polizeibehörden Verwarnungen wegen verschiedener Verstöße gegen ihre Datenschutzverpflichtungen, beispielsweise bei der Beantwortung von Anträgen auf Auskunft, bei der Einrichtung von Sicherheitsmaßnahmen für Videoüberwachungsdaten, beim Umgang mit sensiblen Strafregisterdaten, bei der Zusammenführung der Daten verschiedener Personen oder bei der Weitergabe personenbezogener Daten an Dritte ([152]). Der Information Commissioner veröffentlichte ferner Leitlinien, Stellungnahmen und Leitfäden, z. B. zum Recht auf Zugang oder zur Bearbeitung offensichtlich unbegründeter oder exzessiver Anträge gemäß Teil 3 des DPA 2018 ([153]).

(101) Was die Ausübung von Ermittlungsbefugnissen im Rahmen des IPA 2016 betrifft, so wird die unabhängige und gerichtliche Aufsicht weiterhin vom Investigatory Powers Commissioner (IPC) wahrgenommen, der von anderen Judicial Commissioners unterstützt wird, die gemeinsam als Judicial Commissioners bezeichnet werden ([154]). In diesem Bereich wurden mit dem Investigatory Powers (Amendments) Act 2024 nur begrenzte und gezielte Änderungen vorgenommen, die die Unabhängigkeit, die Aufgaben und die Befugnisse der Judicial Commissioners nicht beeinträchtigen, sondern darauf abzielen, das Funktionieren des bestehenden Aufsichtssystems in der Praxis zu stärken, insbesondere durch die Einführung stellvertretender IPC, denen der IPC bestimmte Befugnisse übertragen kann, wenn er nicht in der Lage oder nicht verfügbar ist, seine Aufgaben wahrzunehmen. Diese stellvertretenden IPC müssen Judicial Commissioners sein und werden vom IPC ernannt ([155]).

([151]) So gingen bei der Information Commission im Zeitraum 2023-2024 beispielsweise 1 890 Beschwerden auf der Grundlage der DSGVO und/oder des DPA 2018 über Organisationen innerhalb der Teilsektoren „Polizeibehörde“, „Polizeikräfte“ und „Polizeikommissare“ ein. Siehe auch den Jahresbericht und Jahresabschluss 2023/2024 des Information Commissioner, abrufbar unter folgendem Link: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Weitere Informationen finden Sie unter dem folgenden Link: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) Abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ und https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Siehe Erwägungsgrund 250 des Durchführungsbeschlusses (EU) 2021/1772.

([155]) Paragraf 227 IPA 2016, eingeführt durch Paragraf 7 des Investigatory Powers (Amendment) Act.

3.3. Einschlägige Entwicklungen in Bezug auf den Zugriff und die Verwendung durch Behörden des Vereinigten Königreichs für Zwecke der nationalen Sicherheit

(102) Was die im Zusammenhang mit der nationalen Sicherheit ausgeübten Ermittlungsbefugnisse anbelangt, so bildet der IPA 2016 weiterhin den rechtlichen Rahmen für die Ausübung dieser Befugnisse. Zusätzlich zu den in den Erwägungsgründen 77 bis 85 dieses Beschlusses beschriebenen Änderungen in Bezug auf gezielte Ermittlungsbefugnisse, auf die sich unter bestimmten Bedingungen auch bestimmte Strafverfolgungsbehörden berufen können, wurde mit dem Investigatory Powers (Amendment) Act 2024 auch eine der im IPA 2016 vorgesehenen Befugnisse geändert, die als Massenbefugnis ausgeübt werden kann.

(103) Konkret wurde mit dem Investigatory Powers (Amendment) Act 2024 in den neuen Teil 7A des IPA 2016 eine spezifische Regelung für die Speicherung und Prüfung einer bestimmten Untergruppe von personenbezogenen Massendatensätzen eingeführt ([156]), d. h. für Datensätze, bei denen die Personen, auf die sich die personenbezogenen Daten beziehen, keine oder nur eine geringe berechtigte Erwartung hinsichtlich der Wahrung ihrer Privatsphäre in Bezug auf die Daten haben könnten ([157]). Ob ein personenbezogener Massendatensatz Teil dieser spezifischen Untergruppe von Datensätzen ist, wird von der Leitung eines Nachrichtendienstes auf der Grundlage aller Umstände entschieden, insbesondere i) der Art der Daten, ii) dem Umfang, in dem die Daten von den betroffenen Personen veröffentlicht wurden, oder ob diese der Veröffentlichung der Daten zugestimmt haben, iii) wenn die Daten veröffentlicht wurden, inwieweit sie unter redaktioneller Kontrolle oder durch eine Person, die nach professionellen Standards handelt, veröffentlicht wurden, iv) wenn die Daten veröffentlicht wurden oder anderweitig öffentlich zugänglich sind, inwieweit die Daten allgemein bekannt sind, und v) inwieweit die Daten bereits öffentlich genutzt wurden ([158]).

(104) Wichtig ist, dass für die Speicherung und Prüfung von personenbezogenen Massendatensätzen, die nicht unter diese Kategorie fallen, d. h. solche, die sensibler sind und daher eine angemessene Erwartung hinsichtlich der Wahrung der Privatsphäre mit sich bringen, die in den Erwägungsgründen 239 und 240 des Durchführungsbeschlusses (EU) 2021/1772 bewertete Regelung beibehalten wird, insbesondere die Notwendigkeit einer Anordnung, die zunächst vom Secretary of State und dann vom Judicial Commissioner genehmigt werden muss, vorbehaltlich der Anforderungen an die Notwendigkeit und Verhältnismäßigkeit der Maßnahme gemäß Teil 7 des IPA 2016 ([159]).

(105) In Teil 7A des IPA 2016 sind zwei Arten von Genehmigungen vorgesehen: Einzelgenehmigung und Kategoriegenehmigung. Die Speicherung oder Speicherung und Prüfung aller gemäß Teil 7A gespeicherten personenbezogenen Massendatensätze muss im Rahmen einer dieser Genehmigungen genehmigt werden. Beide Genehmigungen erfordern grundsätzlich ([160]) eine Genehmigung durch die Leitung des Nachrichtendienstes (oder eine in deren Namen handelnde Person) und die Zustimmung durch einen unabhängigen Judicial Commissioner ([161]). Eine Einzelgenehmigung wird von der Leitung eines Nachrichtendienstes unter den in Paragraf 226B Absatz 4 IPA 2016 genannten Bedingungen und vorbehaltlich der vorherigen Genehmigung durch die Judicial Commissioners erteilt. Der Judicial Commissioner muss die Schlussfolgerungen der Person, welche die Genehmigung erteilt hat, dahin gehend überprüfen, ob Paragraf 226A, d. h. die Anforderung einer geringen oder nicht vorhandenen angemessenen Erwartung hinsichtlich der Wahrung der Privatsphäre, auf den in der Genehmigung beschriebenen personenbezogenen Massendatensatz zutrifft ([162]).

([156]) Nach Paragraf 200 IPA 2016 ausgestellte Anordnungen für personenbezogene Massendatensätze ermächtigen Nachrichtendienste, Datensätze zu speichern und zu prüfen, die personenbezogene Daten zu einer Reihe von Personen enthalten und die so beschaffen sind, 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, und die von einem Nachrichtendienst elektronisch gespeichert und zur Analyse im Rahmen der Ausübung seiner gesetzlichen Aufgaben aufbewahrt werden, siehe auch Paragraf 199 des IPA 2016.

([157]) Paragraf 226A Absatz 1 IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act 2024.

([158]) Paragraf 226A Absatz 3 IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act 2024.

([159]) Mit dem Investigatory Powers (Amendment) Act 2024 wurde Paragraf 213 IPA 2016 dahin gehend geändert, dass Anordnungen für personenbezogene Massendatensätze zwölf Monate nach ihrer Ausstellung unwirksam werden. Zuvor mussten solche Anordnungen alle sechs Monate verlängert werden. Siehe Paragraf 3 des Investigatory Powers (Amendment) Act 2024.

([160]) Eine Einzelgenehmigung kann ohne vorherige richterliche Genehmigung nur erteilt werden, wenn i) die Person, welche die Einzelgenehmigung erteilt, der Auffassung ist, dass der betreffende personenbezogene Massendatensatz unter eine bestehende Kategoriegenehmigung fällt, oder ii) in dringenden Fällen, siehe Paragraf 226B Absatz 6 IPA 2016. Im letzteren Fall muss die Entscheidung über die Erteilung einer dringenden Einzelgenehmigung innerhalb von drei Arbeitstagen nach dem Tag der Erteilung von einem Judicial Commissioner überprüft werden, siehe Paragraf 226BC IPA 2016.

([161]) Paragraf 226B Absatz 1 IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act.

([162]) Paragraf 226BB Absatz 1 Buchstabe a IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act 2024.

(106) Eine Kategoriegenehmigung berechtigt zur Speicherung oder zur Speicherung und Überprüfung einer in der Genehmigung beschriebenen Kategorie von personenbezogenen Massendatensätzen.

(107) Die Entscheidung über die Erteilung der Kategoriegenehmigung wird von der Leitung des Nachrichtendienstes getroffen, wenn sie der Auffassung ist, dass Paragraf 226A für jeden Datensatz innerhalb der Kategorie gilt, und wenn die Entscheidung über die Erteilung der Genehmigung von einem unabhängigen Judicial Commissioner genehmigt wird ([163]). Letzterer muss prüfen, ob Paragraf 226A, d. h. die Anforderung einer geringen oder nicht vorhandenen angemessenen Erwartung hinsichtlich der Wahrung der Privatsphäre, auf alle Datensätze zutrifft, die unter die in der Genehmigung beschriebene Kategorie von Datensätzen fallen ([164]).

(108) Wichtig ist, dass der Judicial Commissioner bei der Genehmigung einer Entscheidung über die Erteilung einer Einzel- oder Kategoriegenehmigung „die gleichen Grundsätze anwendet, die ein Gericht bei einem Antrag auf gerichtliche Überprüfung anwenden würde“ ([165]) und diese Angelegenheiten mit der gebotenen Sorgfalt prüft, um sicherzustellen, dass der Judicial Commissioner die ihm durch Paragraf 2 IPA 2016 auferlegten Pflichten (allgemeine Pflichten in Bezug auf den Schutz der Privatsphäre) ([166]) erfüllt. Darüber hinaus unterliegt die Erteilung von Genehmigungen einer strengen nachträglichen Kontrolle, insbesondere durch die jährliche Berichterstattung an den Secretary of State und den Ausschuss für Nachrichtendienste und Sicherheit (Intelligence and Security Committee) des Parlaments ([167]) sowie durch regelmäßige Inspektionen des Büros des IPC ([168]).

(109) Was die einschlägigen Entwicklungen im Bereich der Aufsicht betrifft, so hat das Amt des IPC Jahresberichte für die Jahre 2021, 2022 und 2023 veröffentlicht, in denen detaillierte Statistiken und Informationen über die Ausübung von Ermittlungsbefugnissen durch Nachrichtendienste und Strafverfolgungsbehörden im Vereinigten Königreich bereitgestellt werden ([169]). In den Berichten werden auch die Prüfungen und Ermittlungen des Amtes sowie deren Ergebnisse beschrieben, wodurch bestätigt wird, dass die IPC ihre sehr wichtige Aufsichtsfunktion im Rahmen der Ermittlungsbefugnisse des Vereinigten Königreichs weiterhin wahrnimmt. So prüfte sie im Jahr 2023 die Notwendigkeit und Verhältnismäßigkeit der Ausübung von Befugnissen zum massenhaften Abfangen (wie in den Erwägungsgründen 218 bis 225 des Durchführungsbeschlusses (EU) 2021/1772 bewertet) durch die Government Communications Headquarters (GCHQ) und kam zu dem Schluss, dass eine erhebliche Mehrheit der Aussagen mit einer soliden Begründung formuliert wurde, während in einigen Fällen die Verhältnismäßigkeit nicht gut zum Ausdruck gebracht wurde. Diese Ergebnisse wurden mit dem Compliance-Team der GCHQ erörtert, das sich verpflichtete, zusätzliche interne Schulungen zur Sensibilisierung in Auftrag zu geben, um dieses Problem anzugehen ([170]).

(110) Darüber hinaus veröffentlichte das Investigatory Powers Tribunal einen öffentlichen Bericht über seine Tätigkeiten und die Rechtsprechung für den Zeitraum 2021 bis 2023 ([171]). Aus dem Bericht geht hervor, dass sich die Zahl der beim Gericht eingegangenen Rechtssachen seit 2017 mehr als verdoppelt hat, wobei 2023 mehr als

([163]) Paragraf 226BA des IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act.

([164]) Paragraf 226BB Absatz 1 Buchstabe b IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act.

([165]) Paragraf 226BB Absatz 2 Buchstabe a IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act 2024.

([166]) Paragraf 226BB Absatz 2 Buchstabe b IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act 2024. Gemäß den allgemeinen Pflichten in Bezug auf den Schutz der Privatsphäre, die in Paragraf 2 des IPA 2016 festgelegt sind, muss eine Behörde folgende Aspekte berücksichtigen: a) ob das, was mit dem Durchsuchungsbefehl, der Genehmigung oder dem Bescheid erreicht werden soll, auch mit anderen, weniger eingreifenden Mitteln erreicht werden könnte, b) ob das Schutzniveau, das in Bezug auf die Beschaffung von Informationen aufgrund des Durchsuchungsbefehls, der Genehmigung oder des Bescheids anzuwenden ist, aufgrund der besonderen Sensibilität dieser Informationen höher ist, c) das öffentliche Interesse an der Integrität und Sicherheit von Telekommunikationssystemen und Postdiensten und d) alle anderen Aspekte des öffentlichen Interesses am Schutz der Privatsphäre.

([167]) Paragrafen 226DA und 226DB des IPA 2016, eingeführt durch Paragraf 2 des Investigatory Powers (Amendment) Act 2024.

([168]) Siehe Jahresbericht 2023 des Investigatory Powers Commissioner Office, abrufbar unter folgendem Link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, S. 3.

([169]) Die Jahresberichte sind unter folgendem Link abrufbar: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Siehe Paragrafen 6.39 bis 6.43 des Jahresberichts 2023, abrufbar unter folgendem Link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

([171]) Bericht des Investigatory Powers Tribunal 2021-2023, abrufbar unter folgendem Link: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

400 Rechtssachen eingegangen sind ([172]). Die meisten Beschwerden betrafen Strafverfolgungsbehörden, dicht gefolgt von Sicherheits- und Nachrichtendiensten ([173]). Wichtig ist, dass das Gericht in den Jahren 2022 und 2023 Urteile in Rechtssachen erlassen hat, die es vor 2021 erhalten hatte und in denen es festgestellt hat, dass britische Behörden (nämlich die Polizei von Schottland ([174]), die Polizei von Greater Manchester ([175]), die Polizei von Surrey ([176]) sowie der MI5 und der Innenminister ([177]) rechtswidrig gehandelt hatten. In Bezug auf Rechtsbehelfe ordnete das Investigatory Powers Tribunal unter anderem die Vernichtung von unrechtmäßig erlangtem Material und in einem Fall auch die Zahlung von 12 000 GBP als Entschädigung für die festgestellten Verstöße an. Der Jahresbericht bestätigt somit, dass das Investigatory Powers Tribunal seine wichtige Rolle bei der Gewährleistung der Aufsicht und des Rechtsschutzes im Bereich der Strafverfolgung und des Zugangs zu personenbezogenen Daten für die nationale Sicherheit wirksam erfüllt.

(111) Darüber hinaus werden in dem Bericht auch wichtige Entwicklungen hervorgehoben, wie z. B. ein Urteil des Europäischen Gerichtshofs für Menschenrechte, in dem der Gerichtshof entschieden hat, dass Einzelpersonen überall auf der Welt vor dem Investigatory Powers Tribunal Klage gegen die Anwendung des britischen Massenüberwachungsprogramms erheben können, wenn das fragliche Verhalten von einer öffentlichen Einrichtung des Vereinigten Königreichs begangen wurde und im Vereinigten Königreich stattgefunden hat ([178]).

4. **SCHLUSSFOLGERUNG**

(112) Die Kommission ist der Ansicht, dass die UK GDPR und der DPA 2018 in der durch den Data (Use and Access) Act geänderten Fassung weiterhin ein Schutzniveau für aus der Europäischen Union übermittelte personenbezogene Daten gewährleisten, das der Sache nach dem durch die Verordnung (EU) 2016/679 garantierten Schutzniveau gleichwertig ist.

(113) Darüber hinaus ist die Kommission der Auffassung, dass die Aufsichtsmechanismen und Rechtsbehelfe im Recht des Vereinigten Königreich es insgesamt ermöglichen, Verstöße zu erkennen und in der Praxis zu ahnden und der betroffenen Person Rechtsbehelfe anzubieten, um Auskunft über die sie betreffenden personenbezogenen Daten zu erhalten und schließlich die Berichtigung oder Löschung dieser Daten zu erwirken.

(114) Schließlich vertritt die Kommission auf der Grundlage der verfügbaren Informationen über die Rechtsordnung des Vereinigten Königreichs die Auffassung, dass jeder Eingriff britischer Behörden in die Grundrechte der Personen, deren personenbezogene Daten aus der Europäischen Union in das Vereinigte Königreich zu Zwecken des öffentlichen Interesses, insbesondere zu Zwecken der Strafverfolgung und der nationalen Sicherheit, übermittelt werden, weiterhin auf das zur Erreichung des betreffenden rechtmäßigen Ziels unbedingt erforderliche Maß beschränkt ist und dass ein wirksamer Rechtsschutz gegen derartige Eingriffe besteht.

(115) Daher sollte in Anbetracht der Feststellungen dieses Beschlusses beschlossen werden, dass das Vereinigte Königreich weiterhin ein angemessenes Schutzniveau im Sinne von Artikel 45 der Verordnung (EU) 2016/679 gemäß seiner Auslegung im Lichte der Charta der Grundrechte der Europäischen Union gewährleistet.

(116) Diese Schlussfolgerung beruht sowohl auf der einschlägigen innerstaatlichen Regelung, wie sie seit der Annahme des Durchführungsbeschlusses (EU) 2021/1772 weiterentwickelt wurde, als auch auf den internationalen Verpflichtungen des Vereinigten Königreichs, die sich insbesondere durch den Beitritt zur Europäischen Menschenrechtskonvention und die Anerkennung der Gerichtsbarkeit des Europäischen Gerichtshofs für Menschenrechte ergeben. Die kontinuierliche Einhaltung dieser internationalen Verpflichtungen ist daher ein besonders wichtiges Element der Bewertung, auf die sich dieser Beschluss stützt.

([172]) Bericht des Investigatory Powers Tribunal 2021-2023, S. 5.
([173]) Bericht des Investigatory Powers Tribunal 2021-2023, S. 12.
([174]) Wilson/Polizei Schottland [2022] UKIPTrib 5.
([175]) Pendlebury/Greater Manchester Police [2023] UKIPTrib 2.
([176]) Hill/Metropolitan Police Service & Independent Office for Police Conduct [2022] UKIPTrib 6.
([177]) Liberty & Privacy International/Security Service und Secretary of State for the Home Department [2023] UKIPTrib 1.
([178]) *Wieder und Guarnieri/Vereinigtes Königreich*, [2023] EGMR 668, siehe auch Investigatory Powers Tribunal Report 2021-2023, S. 6.

5. AUSWIRKUNGEN DIESES BESCHLUSSES UND MAßNAHMEN DER DATENSCHUTZBEHÖRDEN

(117) Die Mitgliedstaaten und ihre Organe müssen die notwendigen Maßnahmen treffen, um Rechtsakten der Unionsorgane nachzukommen, da für diese Rechtsakte eine Vermutung der Rechtmäßigkeit gilt, sodass sie Rechtswirkungen entfalten, solange sie nicht auslaufen, zurückgenommen, im Rahmen einer Nichtigkeitsklage für nichtig erklärt oder infolge eines Vorabentscheidungsersuchens oder einer Einrede der Rechtswidrigkeit für ungültig erklärt wurden.

(118) Daher ist ein nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlassener Angemessenheitsbeschluss der Kommission für alle Organe der Mitgliedstaaten, an die er gerichtet ist, einschließlich ihrer unabhängigen Aufsichtsbehörden, verbindlich. Insbesondere dürfen während der Geltungsdauer des Durchführungsbeschlusses (EU) 2021/1772 in der durch diesen Beschluss geänderten Fassung Übermittlungen von einem Verantwortlichen oder Auftragsverarbeiter in der Europäischen Union an Verantwortliche oder Auftragsverarbeiter im Vereinigten Königreich erfolgen, ohne dass eine weitere Genehmigung eingeholt werden muss.

(119) Es sei daran erinnert, dass nach Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 und wie vom Gerichtshof im Urteil in der Rechtssache Schrems ([179]) erläutert Folgendes gilt: Wenn eine nationale Datenschutzbehörde, auch auf eine Beschwerde hin, die Vereinbarkeit eines Angemessenheitsbeschlusses der Kommission mit den Grundrechten des Einzelnen auf Privatsphäre und Datenschutz infrage stellt, muss das nationale Recht Rechtsbehelfe vorsehen, die es der Datenschutzbehörde ermöglichen, diese Einwände vor einem nationalen Gericht geltend zu machen, das gegebenenfalls ein Vorabentscheidungsverfahren beim Gerichtshof einleiten muss ([180]).

6. ÜBERWACHUNG

(120) Gemäß Artikel 45 Absatz 4 der Verordnung (EU) 2016/679 überwacht die Kommission fortlaufend die einschlägigen Entwicklungen im Vereinigten Königreich, um festzustellen, ob dort weiterhin ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet ist. Eine solche Überwachung ist besonders wichtig, da das Vereinigte Königreich eine geänderte Datenschutzregelung anwenden und durchsetzen wird. Darüber hinaus verleiht der geänderte Datenschutzrahmen des Vereinigten Königreichs dem Secretary of State die Befugnis, diesen Rahmen durch Sekundärrecht weiter zu spezifizieren. In diesem Zusammenhang sollte solchen zusätzlichen Spezifikationen sowie der praktischen Anwendung der geänderten Vorschriften des Vereinigten Königreichs für die Übermittlung personenbezogener Daten in Drittländer besondere Aufmerksamkeit gewidmet werden; die Wirksamkeit der Ausübung individueller Rechte, einschließlich aller relevanten Entwicklungen in Recht und Praxis in Bezug auf die neu eingeführten Ausnahmen oder Beschränkungen dieser Rechte, die Funktionsweise des umstrukturierten ICO, insbesondere hinsichtlich der Bearbeitung von Beschwerden und der Anwendung korrigierender Befugnisse, sowie die Einhaltung der Beschränkungen und Schutzvorkehrungen in Bezug auf den staatlichen Zugang, insbesondere im Hinblick auf den neu eingeführten Teil 7A des IPA 2016. Unter anderem sollten Entwicklungen in der Rechtsprechung sowie die Aufsicht durch das ICO und andere unabhängige Stellen in die Überwachung der Kommission einfließen.

(121) Zur Erleichterung dieser Überwachung sollten die Behörden des Vereinigten Königreichs die Kommission unverzüglich über jede wesentliche Änderung der britischen Rechtsordnung informieren, die Auswirkungen auf den Rechtsrahmen hat, der Gegenstand des Durchführungsbeschlusses (EU) 2021/1772 in der durch diesen Beschluss geänderten Fassung ist, sowie über jede Entwicklung in der Praxis im Zusammenhang mit der Verarbeitung der in Durchführungsbeschluss (EU) 2021/1772 in der geänderten Fassung bewerteten personenbezogenen Daten, sowohl hinsichtlich der Verarbeitung personenbezogener Daten durch Verantwortliche und Auftragsverarbeiter nach der UK GDPR als auch in Bezug auf die Beschränkungen und Schutzvorkehrungen für den Zugriff auf personenbezogene Daten durch öffentliche Stellen. Dies sollte auch Entwicklungen in Bezug auf die in Erwägungsgrund 120 genannten Elemente einschließen.

(122) Damit die Kommission ihre Überwachungsfunktion wirksam ausüben kann, sollten die Mitgliedstaaten die Kommission über alle relevanten Maßnahmen der nationalen Datenschutzbehörden informieren, insbesondere über Anfragen oder Beschwerden von betroffenen EU-Bürgern in Bezug auf die Übermittlung personenbezogener Daten aus der Europäischen Union an zuständige Behörden im Vereinigten Königreich. Ferner sollte die Kommission über alle Hinweise informiert werden, dass die Maßnahmen der britischen Behörden, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder für die nationale Sicherheit zuständig sind, einschließlich etwaiger Aufsichtsstellen, nicht das erforderliche Schutzniveau gewährleisten.

([179]) *Schrems I*, Rn. 65.

([180]) *Schrems I*, Rn. 65. „Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen."

(123) Soweit verfügbare Informationen, insbesondere solche aus der Überwachung des Durchführungsbeschlusses (EU) 2021/1772 in der durch diesen Beschluss geänderten Fassung oder von Behörden des Vereinigten Königreichs oder der Mitgliedstaaten bereitgestellte Informationen, ergeben, dass das vom Vereinigten Königreich gewährte Schutzniveau möglicherweise nicht mehr angemessen ist, sollte die Kommission die zuständigen britischen Behörden unverzüglich darüber informieren und die Ergreifung geeigneter Maßnahmen innerhalb einer festgelegten Frist verlangen, die drei Monate nicht überschreiten darf. Sofern erforderlich, kann dieser Zeitraum je nachdem, worum es sich handelt und/oder welche Maßnahmen zu ergreifen sind, um eine bestimmte Frist verlängert werden. Ein solches Verfahren würde beispielsweise in Fällen eingeleitet, in denen Weiterübermittlungen — auch auf der Grundlage neuer, vom Secretary of State erlassener Angemessenheitsvorschriften oder vom Vereinigten Königreich geschlossener internationaler Übereinkünfte — nicht mehr im Rahmen der Garantien erfolgen würden, die die Kontinuität des Schutzes im Sinne des Artikel 44 der Verordnung (EU) 2016/679 gewährleisten.

(124) Falls die zuständigen Behörden des Vereinigten Königreichs nach Ablauf dieser Frist keine derartigen Maßnahmen ergriffen haben oder nicht auf andere Weise glaubhaft gemacht haben, dass dieser Beschluss weiterhin auf einem angemessenen Schutzniveau beruht, wird die Kommission das Verfahren gemäß Artikel 93 Absatz 2 der Verordnung (EU) 2016/679 einleiten, um diesen Beschluss teilweise oder vollständig auszusetzen oder aufzuheben.

(125) Alternativ wird die Kommission dieses Verfahren einleiten, um den Beschluss zu ändern, indem sie insbesondere Datenübermittlungen zusätzlichen Bedingungen unterwirft oder den Anwendungsbereich der Angemessenheitsfeststellung auf Datenübermittlungen beschränkt, für die auch weiterhin ein angemessenes Schutzniveau gewährleistet ist.

(126) In hinreichend begründeten Fällen äußerster Dringlichkeit wird die Kommission von der Möglichkeit Gebrauch machen, nach dem in Artikel 93 Absatz 3 der Verordnung (EU) 2016/679 genannten Verfahren sofort geltende Durchführungsrechtsakte zur Aussetzung, Aufhebung oder Änderung des Beschlusses zu erlassen.

7. ÜBERPRÜFUNG, GELTUNGSDAUER UND ERNEUERUNG DIESES BESCHLUSSES

(127) Zur Anwendung von Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 und unter Berücksichtigung der Tatsache, dass das vom Recht des Vereinigten Königreichs gewährte Schutzniveau Änderungen unterliegen kann, sollte die Kommission nach Annahme dieses Beschlusses regelmäßig überprüfen, ob die Feststellungen zur Angemessenheit des vom Vereinigten Königreich gewährten Schutzniveaus nach wie vor tatsächlich und rechtlich gerechtfertigt sind, unter Berücksichtigung der in Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 aufgeführten Elemente. Solche Evaluierungen sollten mindestens alle vier Jahre stattfinden und sich auf alle Aspekte der Funktionsweise dieses Beschlusses, einschließlich der Funktionsweise der einschlägigen Aufsichts- und Durchsetzungsmechanismen, erstrecken.

(128) Zur Durchführung der Überprüfung sollte die Kommission mit einschlägigen Vertretern der Behörden des Vereinigten Königreichs, einschließlich der Informationskommission, zusammentreffen. Die Teilnahme an diesem Treffen sollte Vertretern der Mitglieder des Europäischen Datenschutzausschusses offenstehen. Im Rahmen der Überprüfung sollte die Kommission die Behörden des Vereinigten Königreichs ersuchen, umfassende Informationen über alle Aspekte vorzulegen, die für die Feststellung der Angemessenheit von Belang sind. Die Kommission sollte auch Erläuterungen zu allen für diesen Beschluss maßgeblichen, ihr vorliegenden Informationen einholen, einschließlich Informationen vom Europäischen Datenschutzausschuss, einzelnen Datenschutzbehörden, zivilgesellschaftlichen Gruppen, öffentlichen Berichten oder Medienberichten oder jeder anderen verfügbaren Informationsquelle.

(129) Auf der Grundlage der Überprüfung sollte die Kommission einen öffentlichen Bericht erstellen, der dem Europäischen Parlament und dem Rat vorgelegt wird.

(130) Die Kommission muss auch berücksichtigen, dass sich der in diesem Beschluss und im Durchführungsbeschluss (EU) 2021/1772 bewertete Datenschutzrahmen weiterentwickeln kann.

(131) Daher ist es angemessen vorzusehen, dass dieser Beschluss für einen Zeitraum von sechs Jahren ab seinem Inkrafttreten gilt.

(132) Ergeben insbesondere Informationen aus der Überwachung dieses Beschlusses, dass die Feststellungen über die Angemessenheit des im Vereinigten Königreich gewährleisteten Schutzniveaus weiterhin sachlich und rechtlich gerechtfertigt sind, sollte die Kommission spätestens sechs Monate vor Ablauf der Geltungsdauer dieses Beschlusses das Verfahren zur Änderung dieses Beschlusses einleiten, indem sie seinen zeitlichen Anwendungsbereich grundsätzlich um einen weiteren Zeitraum von vier Jahren verlängert. Ein solcher Durchführungsrechtsakt zur Änderung dieses Beschlusses ist nach dem in Artikel 93 Absatz 2 der Verordnung (EU) 2016/679 genannten Verfahren zu erlassen.

8. **SCHLUSSBEMERKUNGEN**

(133) Der Europäische Datenschutzausschuss hat eine Stellungnahme ([181]) veröffentlicht, der bei der Ausarbeitung dieses Beschlusses Rechnung getragen wurde.

(134) Die in diesem Beschluss vorgesehene Maßnahme entspricht der Stellungnahme des gemäß Artikel 93 der Verordnung (EU) 2016/679 eingesetzten Ausschusses.

(135) Der Durchführungsbeschluss (EU) 2021/1772 sollte daher entsprechend geändert werden.

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Artikel 1 Absatz 2 des Durchführungsbeschlusses (EU) 2021/1772 wird aufgehoben.

Artikel 2

Artikel 4 des Durchführungsbeschlusses (EU) 2021/1772 erhält folgende Fassung:

„*Artikel 4*

Die Geltungsdauer dieses Beschlusses endet am 27. Dezember 2031, sofern sie nicht nach dem in Artikel 93 Absatz 2 der Verordnung (EU) 2016/679 genannten Verfahren verlängert wird.“

Artikel 3

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 19. Dezember 2025

Für die Kommission
Michael MCGRATH
Mitglied der Kommission

([181]) Stellungnahme 26/2025 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, abrufbar unter folgendem Link: https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.