Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2571

23.12.2025

DURCHFÜHRUNGSBESCHLUSS (EU) 2025/2571 DER KOMMISSION

vom 19. Dezember 2025

zur Änderung des Durchführungsbeschlusses (EU) 2021/1773 der Kommission gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich

(Bekannt gegeben unter Aktenzeichen C(2025) 8782)

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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 (Richtlinie zum Datenschutz bei der Strafverfolgung) ([1]), insbesondere auf Artikel 36 Absatz 3,

in Erwägung nachstehender Gründe:

1. EINLEITUNG

(1) Im Durchführungsbeschluss (EU) 2021/1773 der Kommission ([2]) wird der Schluss gezogen, dass das Vereinigte Königreich für die Zwecke des Artikels 36 der Richtlinie (EU) 2016/680 ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die im Rahmen des Anwendungsbereichs der genannten Richtlinie aus der Europäischen Union an das Vereinigte Königreich übermittelt werden.

(2) Bei der Annahme des Durchführungsbeschlusses (EU) 2021/1773 berücksichtigte die Kommission, dass das Vereinigte Königreich mit dem Ende des im Abkommen über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft ([3]) 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 ([4]) eine neue Datenschutzregelung erlassen, anwenden und durchsetzen könnte, 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) 2021/1773 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. Der Durchführungsbeschluss (EU) 2021/1773 sollte daher am 27. Juni 2025 auslaufen, sofern er nicht nach dem in Artikel 58 Absatz 2 der Richtlinie (EU) 2016/680 genannten Verfahren verlängert wird.

(4) Um über eine mögliche Verlängerung des Durchführungsbeschlusses (EU) 2021/1773 zu entscheiden, muss die Kommission prüfen, ob die Schlussfolgerung, dass das Vereinigte Königreich ein angemessenes Schutzniveau gewährleistet, angesichts der Entwicklungen seit dem Erlass des Durchführungsbeschlusses (EU) 2021/1773 in Bezug auf die in Artikel 36 Absatz 2 der Richtlinie (EU) 2016/680 aufgeführten Elemente weiterhin sachlich und rechtlich gerechtfertigt ist.

(5) Insbesondere hat die Regierung des Vereinigten Königreichs am 23. Oktober 2024 den Gesetzentwurf Data (Use and Access) Bill ([5]) in das Parlament des Vereinigten Königreichs eingebracht, mit dem Änderungen des Data Protection Act 2018 (DPA 2018) vorgeschlagen werden, der im Durchführungsbeschluss (EU) 2021/1773

([1]) ABl. L 119 vom 4.5.2016, S. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.
([2]) Durchführungsbeschluss (EU) 2021/1773 der Kommission vom 28. Juni 2021 gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (ABl. L 360 vom 11.10.2021, S. 69, ELI: http://data.europa.eu/eli/dec_impl/2021/1773/oj).
([3]) ABl C 384I vom 12.11.2019, S. 1.
([4]) ABl. L 149 vom 30.4.2021, S. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.
([5]) Abrufbar unter folgendem Link: https://bills.parliament.uk/bills/3825/news.

bewertet wird. Am 24. Juni 2025 erließ die Kommission den Durchführungsbeschluss (EU) 2025/1225 ([6]), mit dem die Geltungsdauer des Beschlusses (EU) 2021/1773 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.

(6) Seit der Annahme des Durchführungsbeschlusses (EU) 2021/1773 überwachte die Kommission fortlaufend die einschlägigen Entwicklungen im Vereinigten Königreich ([7]). Gemäß Erwägungsgrund 165 des Durchführungsbeschlusses (EU) 2021/1773 wurde besonderes Augenmerk auf die praktische Anwendung der Vorschriften des Vereinigten Königreichs für die Übermittlung personenbezogener Daten an Drittländer und die möglichen Auswirkungen auf das Schutzniveau für Daten, die gemäß dem Durchführungsbeschluss (EU) 2021/1773 übermittelt werden, sowie auf die Wirksamkeit der Ausübung individueller Rechte, einschließlich aller relevanten Entwicklungen in Recht und Praxis hinsichtlich der Ausnahmen oder Beschränkungen dieser Rechte, gelegt. 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 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 Richtlinie (EU) 2016/680 aus der Europäischen Union in das Vereinigte Königreich übermittelt werden.

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

2.1. Der Datenschutzrechtsrahmen des Vereinigten Königreichs

(8) Bei Erlass des Durchführungsbeschlusses (EU) 2021/1773 wurde der Rechtsrahmen für 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 im Vereinigten Königreich, in den einschlägigen Teilen des DPA 2018 ([8]), geändert durch die Verordnungen von 2019 über Datenschutz, Privatsphäre und elektronische Kommunikation (Änderungen usw.) (EU-Austritt) Data Protection, Privacy and Electronic Communications (Amendments usw.) (EU Exit) Regulations 2019 — (im Folgenden „DPPEC Regulations") ([9]) festgelegt, insbesondere in Teil 3 dieses Gesetzes.

(9) Dieses Gesetz, das die entsprechenden in der Europäischen Union geltenden Vorschriften genau wiedergab, bildet zwar weiterhin die Datenschutzvorschriften des Vereinigten Königreichs für die betreffenden Verarbeitungstätigkeiten, wurde seither jedoch in begrenztem Umfang geändert, worin sich der Umstand niederschlägt, dass das Vereinigte Königreich nicht mehr dem Recht der Europäischen Union unterliegt.

(10) Zunächst wurde im Gesetz über das beibehaltene EU-Recht (Aufhebung und Reform) von 2023 (REUL Act) ([10]) klargestellt, dass die allgemeinen Grundsätze des EU-Rechts nach Ende 2023 nicht mehr Teil des innerstaatlichen Rechts des Vereinigten Königreichs sind ([11]). Darüber hinaus sind die Gerichte des Vereinigten Königreichs nicht mehr verpflichtet, unverändertes „assimiliertes Recht", das zuvor als „beibehaltenes EU-Recht" bezeichnet wurde, im

([6]) Durchführungsbeschluss (EU) 2025/1225 der Kommission vom 24. Juni 2025 zur Änderung des Durchführungsbeschlusses (EU) 2021/1773 gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates über den angemessenen Schutz personenbezogener Daten durch das Vereinigte Königreich, (ABl. L, 2025/1225, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1225/oj).

([7]) Artikel 36 Absatz 4 der Richtlinie (EU) 2016/680.

([8]) 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 enthielt der DPA 2018 nationale Vorschriften, die, soweit dies gemäß der Verordnung (EU) 2016/679 zulässig war, die Anwendung der Vorschriften der Verordnung (EU) 2016/679 präzisierten und einschränkten, und setzte die Richtlinie (EU) 2016/680 um.

([9]) 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.

([10]) Retained EU Law (Revocation and Reform) Act 2023, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2023/28.

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

Einklang mit den allgemeinen Grundsätzen des EU-Rechts auszulegen, sondern dieses Recht ist vielmehr im Einklang mit dem innerstaatlichen Recht des Vereinigten Königreichs auszulegen ([12]). Wie auch in Erwägungsgrund 12 des Durchführungsbeschlusses (EU) 2021/1773 erwähnt, muss jedoch das unveränderte assimilierte Recht von den zuständigen Gerichten des Vereinigten Königreichs weiterhin im Einklang mit der einschlägigen Rechtsprechung des Gerichtshofs der Europäischen Union ausgelegt werden, die vor dem Ende des Übergangszeitraums ([13]) ergangen ist. 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 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.

(11) Zweitens wurde seit der Annahme des Durchführungsbeschlusses (EU) 2021/1773 die Datenschutzgesetzgebung des Vereinigten Königreichs durch die Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023 ([14]) geändert. In diesen Regulations werden Verweise auf Grundrechte oder Grundfreiheiten im DPA 2018 (die zuvor so definiert wurden, dass sie die Grundrechte und Grundfreiheiten der EU abdecken ([15])) 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 ([16]). 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 ([17]).

(12) Schließlich wurde 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 Modalitäten für die Ausübung der Rechte betroffener Personen, die Bedingungen für eine automatisierte Entscheidungsfindung und der Anwendungsbereich bestimmter Anforderungen an die Rechenschaftspflicht. 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.

(13) Mit diesem Beschluss werden legislative, regulatorische und sonstige Entwicklungen bewertet, die für die Schlussfolgerung zum Schutzniveau des Vereinigten Königreichs gemäß dem Durchführungsbeschluss (EU) 2021/1773 maßgeblich sind. Die Bewertung im Durchführungsbeschluss (EU) 2021/1773 gilt weiterhin für diejenigen Aspekte des Datenschutzrahmens des Vereinigten Königreichs, die seit der Annahme des Durchführungsbeschlusses (EU) 2021/1773 nicht geändert oder von anderen Entwicklungen beeinflusst wurden.

([12]) Paragraf 5 Absatz A2 des European Union (Withdrawal) Act 2018 in der durch das REUL-Gesetz geänderten Fassung.
([13]) Paragraf 6 Absätze 3 und 7 des European Union (Withdrawal) Act 2018 in der durch den REUL Act geänderten Fassung.
([14]) Abrufbar unter folgendem Link: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.
([15]) 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.
([16]) Paragraf 2 Absatz 3 der Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023.
([17]) Artikel 6, 8, 10 und 13 der EMRK (siehe auch Anhang 1 des Human Rights Act 1998), verfügbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/1998/42/contents).

(14) 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 ([18]). Der Gerichtshof der Europäischen Union hat klargestellt, dass es dazu keines identischen Schutzniveaus bedarf ([19]). Insbesondere können sich die Mittel, auf die das betreffende Drittland für den Schutz personenbezogener Daten zurückgreift, von denen unterscheiden, die in der Europäischen Union herangezogen werden, sofern sie sich in der Praxis als wirksam erweisen, um ein angemessenes Schutzniveau zu gewährleisten ([20]). Daher erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den Vorschriften der Union. Vielmehr besteht die Prüfung darin, ob das ausländische System insgesamt aufgrund des Wesensgehalts der Rechte auf Datenschutz sowie ihrer wirksamen Anwendung, Überwachung und Durchsetzung das erforderliche Maß an Schutz gewährleistet ([21]).

2.1.1. *Begriffsbestimmungen*

(15) Grundlegende Datenschutzkonzepte, die die Terminologie der Richtlinie (EU) 2016/680 wiedergeben, gelten in der Datenschutzregelung des Vereinigten Königreichs weiterhin. Diese Konzepte wurden in den Erwägungsgründen 26 und 27 des Durchführungsbeschlusses (EU) 2021/1773 bewertet.

(16) Durch die Präzisierung der Definition und der Bedingungen für die Einholung der Einwilligung wird jedoch im Data (Access and Use) Act der Rechtsrahmen für die Verwendung der Einwilligung als Rechtsgrundlage für die Verarbeitung personenbezogener Daten bestätigt ([22]). Die aktualisierten Bestimmungen übernehmen die Formulierungen der britischen DSGVO (UK GDPR) und erhöhen somit die Kohärenz innerhalb der Datenschutzregime des Vereinigten Königreichs. Diese Angleichung erleichtert den zuständigen Behörden eine klarere Auslegung, wenn sie sich auf die Einwilligung als rechtmäßige Grundlage für die Verarbeitung stützen.

(17) Zunächst führt Paragraf 69 des Data (Use and Access) Act einen neuen Unterabsatz 33(1A) in die DPA 2018 ein, der „Einwilligung" als freiwillig erteilte, spezifische, informierte und eindeutige Willensbekundung der betroffenen Person definiert. Diese Angabe muss in Form einer Erklärung oder einer eindeutigen bestätigenden Handlung erfolgen und zum Ausdruck bringen, dass die betreffende Person mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist.

(18) Zweitens fügt derselbe Paragraf den Paragrafen 40A in den DPA 2018 ein, in dem die Bedingungen festgelegt sind, die erfüllt sein müssen, wenn auf die Einwilligung zurückgegriffen wird. Der Verantwortliche muss nachweisen können, dass die betroffene Person eine gültige Einwilligung gegeben hat. Wird die Einwilligung schriftlich als Teil eines umfassenderen Dokuments eingeholt, muss sie in einer Weise dargestellt werden, die sie klar von anderen Sachverhalten unterscheidet, und zwar in einer zugänglichen, verständlichen und einfachen Sprache. Eine Bestimmung des Dokuments, das diesen Normen nicht entspricht, ist nicht bindend ([23]).

(19) Auch Verantwortliche oder Auftragsverarbeiter müssen die betroffene Person vor Einholung der Einwilligung über ihr Recht, die Einwilligung zu widerrufen, informieren. Das Widerrufsverfahren muss genauso einfach sein wie das Verfahren zur Erteilung der Zustimmung. Dadurch wird sichergestellt, dass die betroffene Person die tatsächliche Kontrolle über die Verwendung ihrer personenbezogenen Daten behält ([24]).

(20) Schließlich wird im Data (Use and Access) Act klargestellt, dass bei der Bewertung, ob eine Einwilligung „freiwillig" ist, geprüft werden muss, ob die Erbringung eines Dienstes davon abhängig gemacht wurde, dass die betroffene Person der Verarbeitung personenbezogener Daten zustimmt, die für die Erbringung dieses Dienstes nicht erforderlich sind. Ist dies der Fall, kann dies die Gültigkeit der Einwilligung beeinträchtigen ([25]).

([18]) Erwägungsgrund 67 der Richtlinie (EU) 2016/680.
([19]) Rechtssache C-362/14, Schrems (im Folgenden „Schrems I"), ECLI:EU:C:2015:650, Rn. 73.
([20]) Schrems I, Rn. 74.
([21]) 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, Abschnitt 3.1., S. 6-7, abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52017DC0007.
([22]) Paragrafen 33 und 40A DPA 2018, eingeführt durch Paragraf 69 Absätze 1, 2 und 4 des Data (Use and Access) Act.
([23]) Paragraf 40A Absätze 2 und 3 des DPA 2018, eingeführt durch Paragraf 69 Absatz 4 des Data (Use and Access) Act.
([24]) Paragraf 40A Absätze 5 und 6 des DPA 2018, eingeführt durch Paragraf 69 Absatz 4 des Data (Use and Access) Act.
([25]) Paragraf 40A Absatz 7 des DPA 2018, eingeführt durch Paragraf 69 Absatz 4 des Data (Use and Access) Act.

(21) Wichtig ist, dass gemäß dem überarbeiteten Teil 3 des DPA 2018 die Einwilligung weiterhin keine Rechtsgrundlage darstellt, die für Verarbeitungsvorgänge im Rahmen des Geltungsbereichs des vorliegenden Beschlusses relevant ist, wie in Erwägungsgrund 35 des Durchführungsbeschlusses (EU) 2021/1773 erläutert. Darüber hinaus ist, wie in Erwägungsgrund 36 des Durchführungsbeschlusses (EU) 2021/1773 festgestellt, eine Verarbeitung im Bereich der Strafverfolgung weiterhin nicht allein auf Grundlage einer Einwilligung zulässig, da eine zuständige Behörde grundsätzlich zur Verarbeitung der Daten befugt sein muss. Konkret bedeutet dies — in Anlehnung an die Richtlinie (EU) 2016/680 ([26]) —, dass die Einwilligung als zusätzliche Voraussetzung dient, um bestimmte begrenzte und spezifische Verarbeitungsvorgänge zu ermöglichen, die ansonsten nicht durchgeführt werden könnten, wie etwa die Erhebung und Verarbeitung einer DNA-Probe einer nicht verdächtigen Person.

2.2. **Garantien, Rechte und Pflichten**

2.2.1. *Verarbeitung sensibler personenbezogener Daten*

(22) Wie in den Erwägungsgründen 38 bis 42 des Durchführungsbeschlusses (EU) 2021/1773 bewertet, bietet der Datenschutzrahmen des Vereinigten Königreichs weiterhin spezifische Garantien für besondere Datenkategorien.

(23) Sowohl die Begriffsbestimmungen besonderer Kategorien personenbezogener Daten als auch die spezifischen Vorschriften für die Verarbeitung dieser Datenkategorien in Teil 3 des DPA 2018 behalten ihre Gültigkeit. Gleichzeitig überträgt der Data (Use and Access) Act dem Secretary of State neue Regulierungsbefugnisse, um soweit erforderlich neue besondere Kategorien von Daten hinzuzufügen und die Bedingungen für ihre Nutzung anzupassen ([27]). Wichtig ist dabei, dass es dem Secretary of State durch diese Befugnis nicht gestattet ist, bestehende besondere Kategorien von Daten zu streichen oder abzuändern oder die Bedingungen für die Verarbeitung dieser Kategorien zu ändern ([28]).

(24) Daher berühren diese Änderungen nicht das Schutzniveau für besondere Kategorien personenbezogener Daten, das im Durchführungsbeschluss (EU) 2021/1773 als der Sache nach gleichwertig mit dem Schutzniveau innerhalb der EU angesehen wird.

2.2.2. *Rechte des Einzelnen*

(25) Gemäß dem Rahmen des Vereinigten Königreichs genießen die betroffenen Personen weiterhin dieselben Rechte des Einzelnen wie nach der Richtlinie (EU) 2016/680, die gegen den Verantwortlichen oder 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 57 bis 65 des Durchführungsbeschlusses (EU) 2021/1773 bewertet.

(26) Im Data (Use and Access) Act werden bestimmte Modalitäten festgelegt, unter denen diese Rechte ausgeübt werden können.

(27) Erstens haben die Verantwortlichen nach der derzeitigen Regelung das Recht, einen Antrag abzulehnen oder eine angemessene Gebühr zu erheben, wenn ein Antrag offensichtlich unbegründet oder exzessiv ist ([29]). In diesem Zusammenhang überträgt der Data (Use and Access) Act dem Secretary of State eine neue Regelungsbefugnis, die es dem Secretary of State ermöglicht, Verordnungen zu erlassen, mit denen die Verantwortlichen verpflichtet werden, Leitlinien zu den von ihnen unter solchen Umständen erhobenen Gebühren zu erstellen und zu veröffentlichen. Darüber hinaus stellt der Data (Use and Access) Act klar, dass Datenverantwortliche, wenn sie eine Anfrage aus den genannten Gründen ablehnen, weiterhin verpflichtet sind, die betroffene Person über die Gründe der Ablehnung und über das Recht der betroffenen Person, Beschwerde bei der Information Commissioner einzulegen, zu informieren. Diese Mitteilung muss unverzüglich erfolgen ([30]).

(28) Zweitens sind im Data (Use and Access) Act die Fristen festgelegt, innerhalb deren die Verantwortlichen die Anträge der betroffenen Person beantworten müssen. Konkret werden die erforderlichen Antwortfristen an die in der UK GDPR festgelegten Fristen angeglichen. Mit den überarbeiteten Bestimmungen ist außerdem eine Verlängerung der Antwortfrist um bis zu zwei weitere Monate vorgesehen, wenn das Ersuchen komplex ist oder wenn mehrere

([26]) Siehe Erwägungsgründe 35 und 37 der Richtlinie (EU) 2016/680.

([27]) Paragraf 74 des Data (Use and Access) Act. Solche Regelungen unterliegen dem positiven Abstimmungsverfahren, was bedeutet, dass sie der aktiven Zustimmung des Parlaments des Vereinigten Königreichs bedürfen.

([28]) Siehe den neuen Paragrafen 42A des DPA 2018, eingeführt durch Paragraf 74 des Data (Use and Access) Act, sowie die Erläuterungen zum Data (Use and Access) Bill, Rn. 577, abrufbar unter folgendem Link: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

([29]) Paragraf 53 Absatz 1 DPA 2018. Siehe auch Erwägungsgrund 64 des Durchführungsbeschlusses (EU) 2021/1773.

([30]) Paragraf 53 Absatz 4A, 6 und 7 des DPA 2018, eingeführt durch Paragraf 75 des Data (Use and Access) Act.

Ersuchen eingehen. In solchen Fällen muss der Verantwortliche die betroffene Person über die Verlängerung und die Gründe dafür unterrichten ([31]). Mit dem Data (Use and Access) Act wurde auch ein Mechanismus eingeführt, der es Verantwortlichen ermöglicht, die Frist für die Beantwortung eines Ersuchens auszusetzen, wenn von der betroffenen Person weitere Informationen benötigt werden, um die angeforderten Daten zu identifizieren ([32]).

(29) Drittens ändert der Data (Use and Access) Act den Paragrafen 45 des DPA 2018 — ausschließlich in Bezug auf das Auskunftsrecht über Informationen und personenbezogene Daten —, um die Klarstellung aufzunehmen, die in der bestehenden nationalen Rechtsprechung, gestützt auf den Grundsatz der Verhältnismäßigkeit nach EU-Recht, entwickelt wurde, dass Verantwortliche nur angemessene und verhältnismäßige Nachforschungen nach den angeforderten Informationen und personenbezogenen Daten durchführen müssen ([33]). Von der neuen Bestimmung wird erwartet, dass sie im Einklang mit der bestehenden Rechtsprechung ausgelegt wird, die vorsieht, dass „[…] bei der Verhältnismäßigkeitsprüfung das Endziel der Suche abzuwägen ist, nämlich der potenzielle Nutzen, den die Bereitstellung der Informationen für die betroffene Person bringen könnte, gegenüber 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*“ ([34]).

(30) Während die Modalitäten für die Beantwortung von Anträgen der betroffenen Personen 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 ([35]).

(31) Mit dem Data (Use and Access) Act wurde zudem ein neuer Paragraf 45A in den DPA 2018 eingefügt, der eine ausdrückliche Ausnahme von der Verpflichtung schafft, einer betroffenen Person Auskunft oder Informationen zu erteilen, wenn die Informationen durch das Anwaltsgeheimnis geschützt sind ([36]). Diese Ausnahme gilt speziell für die Pflichten nach den Paragrafen 44 Absatz 2 und 45 Absatz 1 des DPA 2018, die Verantwortliche verpflichten, betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten zu informieren und ihnen Zugang zu diesen Daten zu gewähren ([37]). Es wird klargestellt, dass Verantwortliche nicht verpflichtet sind, Informationen offenzulegen, wenn dies gegen das Berufsgeheimnis verstoßen würde. Eine ähnliche Ausnahme besteht auch in der UK GDPR ([38]).

(32) Hinsichtlich der Garantien müssen Verantwortliche, wenn sie sich auf diese Ausnahme berufen, die betroffene Person schriftlich und ohne unangemessene Verzögerung darüber informieren, dass die Ausnahme angewendet wurde, die Gründe dafür erläutern und sie über ihr Recht unterrichten, eine Überprüfung durch die Informationskommission zu beantragen oder Rechtsmittel einzulegen ([39]). Um die Rechenschaftspflicht zu gewährleisten, sind Verantwortliche nach Paragraf 45A Absatz 4 des DPA 2018 verpflichtet, Aufzeichnungen über den Grund für ihre Entscheidung, die Ausnahme anzuwenden, zu führen und diese der Information Commission auf Anfrage zur Verfügung zu stellen ([40]).

([31]) Paragraf 54 Absatz 3A und Paragraf 54 Absatz b3 des DPA 2018, eingeführt durch Paragraf 76 Absatz 6 des Data (Use and Access) Act.

([32]) Paragraf 54 Absätze 3C und 3D des DPA 2018, eingeführt durch Paragraf 76 Absätze 5 und 6 des Data (Use and Access) Act.

([33]) Paragraf 45 Absatz 2A des DPA 2018, eingeführt durch Paragraf 78 des Data (Use and Access) Act.

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

([35]) 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/.

([36]) Paragraf 45A, eingeführt durch Paragraf 79 des Data (Use and Access) Act. Im Vereinigten Königreich ist die Vertraulichkeit der anwaltlichen Korrespondenz ein zentrales Recht, das bestimmte vertrauliche Kommunikationen zwischen einem Mandanten und seinem Rechtsberater davor schützt, ohne Zustimmung des Mandanten offengelegt zu werden. Es umfasst zwei Hauptkategorien: das Rechtsberatungsprivileg („legal advice privilege“), das den Austausch zum Zwecke der Einholung oder Erbringung von Rechtsberatung schützt, und das Prozessprivileg („litigation privilege“), das für Kommunikationen gilt, die in Vorbereitung oder während eines Gerichtsverfahrens erfolgen.

([37]) Die nach Teil 3 zuständigen Behörden stützten sich zuvor auf andere verfügbare Ausnahmen nach Paragraf 44 Absatz 4 (Recht auf Unterrichtung) und Paragraf 45 Absatz 4 (Zugangsrecht) des DPA 2018.

([38]) Anhang 2, Absatz 19 des DPA 2018.

([39]) Paragraf 45A Absatz 2 des DPA 2018, eingeführt durch Paragraf 79 des Data (Use and Access) Act. Eine Ausnahme von dieser Mitteilungspflicht gilt, wenn die Übermittlung einer solchen Mitteilung selbst den privilegierten oder vertraulichen Charakter der Informationen beeinträchtigen würde. In solchen Fällen muss der Verantwortliche weder nachweisen, dass die Ausnahme angewendet wurde, noch weitere Erläuterungen geben.

([40]) Paragraf 45A des DPA 2018, eingeführt durch Paragraf 79 des Data (Use and Access) Act.

(33) Schließlich wurden mit dem Data (Use and Access) Act 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 ([41]). 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.

(34) 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 ([42]). 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 ([43]). Dies wird auch in den Leitlinien der ICO zur Anwendung von Ausnahmen im Bereich der nationalen Sicherheit bestätigt ([44]).

2.2.3. *Beschränkungen für Weiterübermittlungen*

(35) Das Schutzniveau für personenbezogene Daten, die aus der Europäischen Union an Strafverfolgungsbehörden im Vereinigten Königreich übermittelt werden, darf nicht durch die Weiterübermittlung dieser Daten an Empfänger in einem Drittland beeinträchtigt werden. Wie in den Erwägungsgründen 74 bis 87 des Durchführungsbeschlusses (EU) 2021/1773 bewertet, ähnelt die Regelung für die internationale Übermittlung personenbezogener Daten aus dem Vereinigten Königreich nach wie vor sehr stark den Regelungen in Kapitel V Richtlinie (EU) 2016/680.

(36) Mit dem Data (Use and Access) Act wurde Teil 3 Kapitel 5 des DPA 2018 über die Übermittlung personenbezogener Daten an zuständige Behörden in Drittländern geändert, doch wird die folgende Kernanforderung beibehalten: a) Die Übermittlung ist für einen Zweck der Strafverfolgung erforderlich, b) die Übermittlung muss auf der Grundlage i) von Regelungen zur Genehmigung der Übermittlung (in Ersetzung der bisherigen Angemessenheitsvorschriften), ii) geeigneter Garantien oder iii) besonderer Umstände erfolgen und c) Empfänger der Datenübermittlung muss i) eine relevante Behörde (d. h. die einer zuständigen Behörde entsprechende Stelle) des Drittlands, (ii) eine relevante internationale Organisation, (iii) ein Auftragsverarbeiter, der im Auftrag einer zuständigen Behörde tätig ist, oder (iv) eine andere Person als eine zuständige Behörde, jedoch nur, wenn die Übermittlung für die Erfüllung eines der Zwecke der Strafverfolgung unbedingt erforderlich ist ([45]). Diese allgemeinen Grundsätze für Datenübermittlungen werden in Paragraf 73 DPA 2018 übernommen, 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 von Teil 3 des DPA 2018 erfolgt ([46]).

(37) Bezüglich der Verordnungen zur Genehmigung einer Übermittlung legt Paragraf 74AA Absatz 2 der DPA 2018 fest, dass der Secretary of State solche Verordnungen nur erlassen darf, wenn er der Auffassung ist, dass der Datenschutztest erfüllt ist. Dies bedeutet, dass die Möglichkeit des Secretary of State gemäß Paragraf 74AA Absatz 3 der DPA 2018, bei der Erstellung solcher Verordnungen die Zweckmäßigkeit der Erleichterung von Datenflüssen zu berücksichtigen, stets der Bedingung unterliegt, dass der Datenschutztest erfüllt wird. die Bedingung geknüpft ist, dass die Datenschutzprüfung erfüllt ist. Der neue Paragraf 74AB ([47]) des DPA 2018 formuliert den rechtlichen Standard für die zu erfüllende Datenschutzprüfung und verlangt, dass der Schutzstandard für betroffene Personen in Empfängerländern oder in internationalen Organisationen nicht wesentlich niedriger ist als der Standard, der für betroffene Personen gemäß den einschlägigen Datenschutzgesetzen des Vereinigten Königreichs vorgesehen ist.

([41]) 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.

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

([43]) 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.

([44]) 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/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([45]) Paragraf 73 DPA 2018 in der durch Anhang 8 Paragraf 3 Absätze 4 und 5 des Data (Use and Access) Act geänderten Fassung.

([46]) Paragraf 73 DPA 2018 in der durch Anhang 8 Paragraf 3 Absatz 3 des Data (Use and Access) Act geänderten Fassung.

([47]) Wie in der durch Anhang 8 Paragraf 4 Absatz 2 des Data (Use and Access) Act eingeführt.

Paragraf 74AB Absatz 2 DPA 2018 enthält ferner eine nicht erschöpfende Liste von Elementen, die bei der Beurteilung, ob diese Prüfung erfüllt ist, zu berücksichtigen sind, wie die Achtung der Rechtsstaatlichkeit und der Menschenrechte, das Bestehen und die Befugnisse einer Datenschutzbehörde, die Regelungen für gerichtliche oder außergerichtliche Rechtsbehelfe, die Vorschriften über die Übermittlung personenbezogener Daten aus dem Land oder von der Organisation an andere Länder oder 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 gemäß dem früheren Paragrafen 74A des DPA 2018 umformuliert wird, werden die Kernelemente dieser Liste in der neuen Bestimmung beibehalten und bleiben somit nahe an den Vorgaben von Artikel 36 der Richtlinie (EU) 2016/680. Darüber hinaus haben die Behörden des Vereinigten Königreichs bestätigt, dass der Secretary of State auch Elemente berücksichtigen wird, die nicht in Paragraf 74AB Absatz 2 aufgeführt sind, wie etwa die Gesetze und Praktiken in einem Drittland hinsichtlich des behördlichen Zugriffs auf personenbezogene Daten zu Zwecken wie der nationalen Sicherheit oder der Strafverfolgung, soweit sie den allgemeinen Schutzstandard beeinflussen. Darüber hinaus sind die Behörden des Vereinigten Königreichs der Auffassung, dass die einschlägige Rechtsprechung des Drittlands ein wesentlicher Bestandteil der Prüfung der in Paragraf 74AB Absatz 2 des DPA 2018 nicht abschließend aufgeführten Aspekte sein wird.

(38) Verordnungen zur Genehmigung einer Übermittlung unterliegen weiterhin den „allgemeinen" Verfahrensvorschriften nach Paragraf 182 des DPA 2018, wie in Erwägungsgrund 77 des Durchführungsbeschlusses (EU) 2021/1773 dargelegt. Im Rahmen dieses Verfahrens muss der Secretary of State den Information Commissioner konsultieren, wenn er beabsichtigt, britische Angemessenheitsverordnungen zu erlassen ([48]). 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 ([49]).

(39) In Bezug auf geeignete Garantien ist in Paragraf 75 des DPA 2018 in der durch Anhang 8 Absatz 6 des Data (Use and Access) Act geänderten Fassung festgelegt, dass solche Übermittlungen nur erfolgen dürfen, wenn: a) ein geeignetes Rechtsinstrument den vorgesehenen Empfänger der Daten bindet, das die in dem neu eingefügten Absatz 4 festgelegten Bedingungen erfüllt, insbesondere dahin gehend, dass jede zuständige Behörde des Vereinigten Königreichs, die Vertragspartei dieses Instruments ist, nach vernünftigem Ermessen und unter Wahrung der Verhältnismäßigkeit der Auffassung ist, dass der Datenschutztest erfüllt ist, oder b) der Verantwortliche nach vernünftigem Ermessen und unter Wahrung der Verhältnismäßigkeit der Auffassung ist, dass der Datenschutztest in Bezug auf die Übermittlung oder die betreffende Art der Übermittlung erfüllt ist. Der neu eingefügte Paragraf 75 Absatz 5 des DPA 2018 stellt klar, dass der Datenschutztest 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. Dies ähnelt den in Artikel 37 der Richtlinie (EU) 2016/680 festgelegten Maßnahmen. Infolgedessen gelten in der EU und im Vereinigten Königreich dieselben rechtlichen Standards für die Genehmigung einer Übermittlung vorbehaltlich geeigneter Garantien. Nach dem neu eingefügten Paragrafen 75 Absatz 6 DPA 2018 ist unter Berücksichtigung aller Umstände oder wahrscheinlichen Umstände der Übermittlung oder der Art der Übermittlung, einschließlich der Art und des Umfangs der übermittelten personenbezogenen Daten, zu bestimmen, was angemessen und verhältnismäßig ist.

(40) In Bezug auf Übermittlungen aufgrund besonderer Umstände gemäß Paragraf 76 des DPA 2018 werden mehrere technische Änderungen vorgenommen, die die Bestimmung an Änderungen anderer Regelungen anpassen, ohne das Schutzniveau für personenbezogene Daten im Vereinigten Königreich zu beeinträchtigen ([50]).

(41) Was die Umsetzung der internationalen Übermittlungsregeln des Vereinigten Königreichs betrifft, so gab es seit der Annahme des Durchführungsbeschlusses (EU) 2021/1773 mehrere Entwicklungen.

(42) Erstens führte das Vereinigte Königreich nach Abschluss einer Vereinbarung zwischen dem Innenministerium und dem ICO im Jahr 2022, in der ihre jeweiligen Aufgaben bei der Beurteilung der Angemessenheit der Strafverfolgung festgelegt wurden ([51]), Bewertungen der Datenschutzrahmen in den Amtsbezirken (Bailiwicks) Jersey und Guernsey

([48]) 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.

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

([50]) Absatz 7 von Anhang 8 des Data (Use and Access) Act.

([51]) Abrufbar unter folgendem Link: https://ico.org.uk/media2/about-the-ico/mou/4025752/ico-ho-mou.pdf.

sowie auf der Isle of Man durch. Infolgedessen erließ das Vereinigte Königreich im Juli 2023 Angemessenheitsvorschriften für Guernsey ([52]), im November 2023 für Jersey ([53]) und im Januar 2025 für die Isle of Man ([54]). Diese Verordnungen bestätigen, dass jede Rechtsordnung ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die gemäß Teil 3 des DPA 2018 übermittelt werden. Obwohl diese Verordnungen ursprünglich nach dem früheren Rechtsrahmen erlassen wurden, bleibt die ihnen zugrunde liegende Bewertung auch im aktualisierten Rahmen gültig. Infolgedessen erleichtern die Verordnungen weiterhin die internationale Zusammenarbeit im Bereich der Strafverfolgung.

(43) Die Kommission bewertete außerdem die Datenschutzrahmen für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Strafverfolgung sowie die Vorschriften über den Zugang öffentlicher Stellen zu personenbezogenen Daten für Zwecke der nationalen Sicherheit in den Vogteien Jersey und Guernsey sowie auf der Isle of Man, als sie die Funktionsweise der Angemessenheitsbeschlüsse prüfte, die auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG gemäß Artikel 97 der Verordnung (EU) 2016/679 erlassen wurden. Gestützt unter anderem auf diese Bewertung kam die Kommission zu dem Schluss, dass alle drei Jurisdiktionen weiterhin ein angemessenes Schutzniveau für aus der EU übermittelte personenbezogene Daten gewährleisten ([55]).

(44) Zweitens haben das Vereinigte Königreich und die Vereinigten Staaten im Jahr 2022 das britisch-US-amerikanische Datenschutzabkommen ([56]) geschlossen, das die Bestimmungen des EU-US-Rahmenabkommens ([57]) mutatis mutandis anwendet und einen gleichwertigen Schutz im Zusammenhang mit dem Datenaustausch zwischen dem Vereinigten Königreich und den Vereinigten Staaten zu Strafverfolgungszwecken gewährleistet.

(45) Drittens hat das ICO in den Jahren 2023 und 2025 seine Leitlinien zu internationalen Übermittlungen nach Teil 3 Kapitel 5 des DPA 2018 aktualisiert ([58]). In der Aktualisierung von 2023 wurde die Bedeutung der Anforderung „unbedingt erforderlich" für Datenübermittlungen an andere Empfänger als die zuständigen Strafverfolgungsbehörden präzisiert, wodurch den Verantwortlichen mehr Sicherheit bei der Bewertung der Rechtmäßigkeit solcher Übermittlungen verschafft wird. Im Jahr 2025 wurde die Liste der geeigneten Länder und Gebiete nach den Angemessenheitsverordnungen des Vereinigten Königreichs für die Isle of Man aktualisiert.

2.2.4. *Automatisierte Entscheidungsfindung*

(46) Unter Beibehaltung mehrerer Elemente der Vorschriften für die automatisierte Entscheidungsfindung, die in den Erwägungsgründen 72 und 73 des Durchführungsbeschlusses (EU) 2021/1773 bewertet wurden, wurden mit dem Data (Use and Access) Act einige Aspekte dieser Vorschriften geändert.

(47) Erstens enthält der neu eingefügte Paragraf 50B des DPA 2018 ein allgemeines Verbot wichtiger Entscheidungen, die ganz oder teilweise auf der Verarbeitung besonderer Kategorien personenbezogener Daten beruhen. Es sind darin jedoch zwei Ausnahmen von diesem Verbot vorgesehen: die betroffene Person hat ausdrücklich in diese Verarbeitung eingewilligt; oder die Entscheidung ist gesetzlich vorgeschrieben oder zulässig ([59]).

(48) In Bezug auf die zweite Situation schreibt der neu eingefügte Paragraf 50C des DPA 2018 vor, dass Verantwortliche für jede wichtige Entscheidung, die ganz oder teilweise auf personenbezogenen Daten beruht und ausschließlich automatisiert erfolgt, geeignete Garantien implementieren müssen. Diese Garantien müssen umfassen, dass die

([52]) Abrufbar unter folgendem Link: https://www.legislation.gov.uk/uksi/2023/1221/contents/made.
([53]) Abrufbar unter folgendem Link: https://www.legislation.gov.uk/uksi/2023/744/made.
([54]) Abrufbar unter folgendem Link: https://www.legislation.gov.uk/uksi/2025/89/contents/made.
([55]) Bericht der Kommission an das Europäische Parlament und den Rat über die erste Überprüfung der Wirkungsweise der Angemessenheitsfeststellungen gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG vom 15. Januar 2024, abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0007; sowie die Länderberichte über die Funktionsweise der gemäß der Richtlinie 95/46/EG erlassenen Angemessenheitsbeschlüsse, die das Dokument Bericht der Kommission an das Europäische Parlament und den Rat über die erste Überprüfung der Funktionsweise der gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Angemessenheitsbeschlüsse begleiten, abrufbar unter folgendem Link: https://commission.europa.eu/document/download/f8229eb2-1a36-4cf5-a099-1cd001664bff_en?filename=JUST_template_comingsoon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf.
([56]) Abrufbar unter folgendem Link: https://www.gov.uk/government/publications/ukusa-exchange-of-notes-on-the-protection-of-personal-information-relating-to-prevention-investigation-detection-and-prosecution-of-criminal-offe.
([57]) 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), abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:22016A1210(01)&from=DE.
([58]) Abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/international-transfers/.
([59]) Paragraf 50B des DPA 2018, eingeführt durch Paragraf 80 Absatz 3 des Data (Use and Access) Act.

betroffene Person über den Entscheidungsprozess informiert wird, dass sie die Entscheidung anfechten oder Stellungnahmen abgeben kann und dass sie das Eingreifen einer Person in den Entscheidungsprozess beantragen kann ([60]). Paragraf 50C Absatz 4 des DPA 2018 sieht zwar eine Ausnahme von der Anwendung dieser Garantien vor, wenn eine solche Ausnahme erforderlich ist, um behördliche oder gerichtliche Ermittlungen, Verfahren oder Maßnahmen nicht zu behindern, die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen nicht zu beeinträchtigen, die öffentliche Sicherheit oder die nationale Sicherheit zu schützen oder die Rechte und Freiheiten anderer zu wahren. Die Anwendung dieser Garantien wird jedoch nur vorübergehend ausgesetzt, da der Verantwortliche verpflichtet ist, die Entscheidung so bald wie nach vernünftigem Ermessen möglich zu überprüfen und eine sinnvolle menschliche Beteiligung an der Überprüfung sicherzustellen ([61]).

(49) Darüber hinaus wird in dem neuen Paragraf 50A DPA 2018 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. Paragraf 50A des DPA 2018 stellt außerdem klar, dass eine „wichtige Entscheidung" eine Entscheidung ist, die nachteilige rechtliche Auswirkungen oder vergleichbar bedeutende nachteilige Auswirkungen für eine betroffene Person zur Folge hat ([62]). Diese Beschränkung auf Entscheidungen, die sich nachteilig auf die betroffene Person auswirken, spiegelt wider, dass es im Gegensatz zur Verarbeitung nach der UK GDPR unwahrscheinlich ist, dass die zuständigen Behörden Entscheidungen treffen, die von den betroffenen Personen als positiv angesehen werden.

(50) Schließlich gewährt der neu eingefügte Paragraf 50D des DPA 2018 dem Secretary of State die Befugnis, sekundäres Recht zu erlassen, um zu bestimmen, was eine sinnvolle menschliche Beteiligung darstellt und was nicht, welche Entscheidungen als solche mit vergleichbar erheblichen nachteiligen Auswirkungen auf betroffene Personen gelten und welche 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 ([63]). Wichtig ist, dass der Secretary of State vor dem Erlass von Verordnungen gemäß Paragraf 50D des DPA 2018 den ICO konsultieren muss ([64]) und dass die Verordnungen dem positiven Abstimmungsverfahren unterliegen ([65]), was bedeutet, dass sie von beiden Kammern des britischen Parlaments genehmigt werden müssen, bevor sie in Kraft treten können.

(51) Mit dem Data (Use and Access) Act wurde zwar der Rahmen für die automatisierte Entscheidungsfindung geändert, es ist jedoch darauf hinzuweisen, dass automatisierte Entscheidungsfindung nach dem Rechtsrahmen des Vereinigten Königreichs weiterhin dem zentralen Schutzmechanismus unterliegt, der das Recht auf menschliches Eingreifen in allen Fällen automatisierter Entscheidungen, das heißt auf der Grundlage der Verarbeitung sensibler und nicht sensibler personenbezogener Daten, vorsieht ([66]).

2.2.5. *Rechenschaftspflicht*

(52) Der Rechtsrahmen des Vereinigten Königreichs wahrt weiterhin den in der Richtlinie (EU) 2016/680 verankerten Grundsatz der Rechenschaftspflicht, wonach die Behörden geeignete technische und organisatorische Maßnahmen ergreifen müssen, um die Einhaltung der Datenschutzverpflichtungen sicherzustellen und nachzuweisen, wie in den Erwägungsgründen 88 bis 92 des Durchführungsbeschlusses (EU) 2021/1773 bewertet.

(53) Eine der verschiedenen im DPA 2018 vorgesehenen Maßnahmen, um die Rechenschaftspflicht sicherzustellen und es den Verantwortlichen und Auftragsverarbeitern zu ermöglichen, die Einhaltung nachzuweisen, besteht darin, dass die zuständigen Behörden Protokolle über ihre Verarbeitungstätigkeiten, einschließlich der Erhebung, Änderung, Abfrage, Offenlegung, Kombination und Löschung personenbezogener Daten, führen müssen ([67]). Mit dem Data (Use and Access) Act werden die spezifischen Pflichten der Verantwortlichen gemäß dieser Bestimmung geändert, indem in Paragraf 62 des DPA 2018 die Verpflichtung der Verantwortlichen gestrichen wird, bei der Abfrage oder Offenlegung personenbezogener Daten eine Begründung zu dokumentieren ([68]). Wichtig ist, dass die Verpflichtung der Verantwortlichen, die Verarbeitungstätigkeiten als solche zu protokollieren, weiterhin besteht, sodass der zentrale Mechanismus zur Gewährleistung der Rechenschaftspflicht erhalten bleibt.

([60]) Paragraf 50C des DPA 2018, eingeführt durch Paragraf 80 Absatz 3 des Data (Use and Access) Act.
([61]) Paragraf 50C Absatz 3 und 4 des DPA 2018, eingeführt durch Paragraf 80 Absatz 3 des Data (Use and Access) Act.
([62]) Paragraf 50A des DPA 2018, eingeführt durch Paragraf 80 Absatz 3 des Data (Use and Access) Act.
([63]) Paragraf 50D des DPA 2018, eingeführt durch Paragraf 80 Absatz 3 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 Verordnungen dürfen die in Paragraf 50C festgelegten Anforderungen nicht ändern.
([64]) Paragraf 182 Absatz 2 DPA 2018.
([65]) Paragraf 50D Absatz 5 DPA 2018.
([66]) Paragraf 50C Absatz 2 Buchstabe c DPA 2018.
([67]) Paragraf 62 DPA 2018. Siehe Erwägungsgrund 90 des Durchführungsbeschlusses (EU) 2021/1773.
([68]) Paragraf 82 des Data (Use and Access) Act.

2.3. **Aufsicht und Durchsetzung**

2.3.1. *Unabhängige Aufsicht*

(54) Im Vereinigten Königreich wird die Überwachung und Durchsetzung der Einhaltung des Datenschutzrahmens weiterhin von einer unabhängigen Datenschutzaufsichtsbehörde durchgeführt, wie in den Erwägungsgründen 93 bis 99 des Durchführungsbeschlusses (EU) 2021/1773 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.

(55) 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 ([69]). Das Gesetz enthält auch Bestimmungen dafür, dass der Information Commissioner die Rolle des Vorsitzenden der Information Commission übernimmt, der eines der nicht geschäftsführenden Mitglieder ist ([70]). 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 ([71]) 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 ([72]).

(56) 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 95 bis 98 des Durchführungsbeschlusses (EU) 2021/1773 ([73]) 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 ([74]). Die anderen nicht geschäftsführenden Mitglieder werden vom Secretary of State nach Konsultation der vorsitzenden Person ernannt. Bewerber können nur dann zur Ernennung empfohlen oder ernannt werden, wenn sie auf der Grundlage ihrer Verdienste im Rahmen eines fairen und offenen Auswahlverfahrens ausgewählt werden und wenn der Secretary of State davon überzeugt ist, dass sie sich nicht in einem Interessenkonflikt befinden ([75]). Die geschäftsführenden Mitglieder sind Bedienstete der Information Commission, die zu von den nicht geschäftsführenden Mitgliedern festgelegten Bedingungen beschäftigt werden ([76]). Die anderen nicht geschäftsführenden Mitglieder werden vom Secretary of State nach Konsultation der vorsitzenden Person ernannt. Die Ernennung von Mitgliedern der Geschäftsführung unterliegt ebenfalls einer Auswahl nach Leistung auf der Grundlage eines fairen und offenen Auswahlverfahrens ([77]).

(57) Der Vorsitzende kann von Seiner Majestät nur auf eine Beschlussfassung beider Kammern des Parlaments hin seines Amtes enthoben werden und nur dann, wenn der Secretary of State der betreffenden Kammer einen Bericht vorgelegt hat, in dem er darlegt, dass sich der Vorsitzende seiner Überzeugung nach eines schweren Fehlverhaltens schuldig gemacht hat, in einem Interessenkonflikt steht, besonderen Informationspflichten in Bezug auf potenzielle Interessenkonflikte nicht nachgekommen ist oder nicht in der Lage, nicht geeignet oder nicht willens ist, die Funktionen des Vorsitzenden auszuüben ([78]). 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 ([79]).

([69]) Absatz 3(1) von Anhang 12A zum DPA 2018.
([70]) Paragrafen 117, 118, 119 und 120 in Verbindung mit Anhang 14 des Data (Use and Access) Act.
([71]) Absätze 13 und 14 von Anhang 12A zum DPA 2018.
([72]) Absatz 16 von Anhang 12A zum DPA 2018.
([73]) Artikel 52 der UK-GDPR sowie Anhang 12A des DPA 2018, eingeführt durch Paragraf 117 des Data (Use and Access) Act.
([74]) Absatz 5(1) von Anhang 12A zum DPA 2018.
([75]) Anhang 12A Paragrafen 3 Absatz 2, 5 und 6 des DPA 2018.
([76]) Absatz 11 von Anhang 12A zum DPA 2018.
([77]) Absatz 5(2) von Anhang 12A zum DPA 2018.
([78]) Anhang 12A Paragraf 7 Absatz 6 und 7 des DPA 2018.
([79]) Anhang 12A Paragraf 9, Absatz 6, 7, 8 und 9 des DPA 2018.

(58) Der Data (Use and Access) Act ändert nichts an den Kernaufgaben der Information Commission, die weiterhin die in Anhang 13 des DPA 2018 festgelegten Funktionen ausübt. Dazu gehören die Überwachung und Durchsetzung der Einhaltung von Teil 3 des DPA 2018, die Beratung des Parlaments und der Regierung, die Sensibilisierung der Öffentlichkeit, die Unterstützung von Verantwortlichen und Auftragsverarbeitern bei der Erfüllung ihrer Verpflichtungen sowie die Unterrichtung von Einzelpersonen über ihre Rechte ([80]). Der Data (Use and Access) Act stellt klar, dass die Information Commission bei der Wahrnehmung der Aufgabe, ein angemessenes Schutzniveau für personenbezogene Daten sicherzustellen, die Interessen der betroffenen Personen, der Verantwortlichen und anderer berücksichtigen, das allgemeine öffentliche Interesse einbeziehen sowie das öffentliche Vertrauen in die Verarbeitung personenbezogener Daten stärken muss ([81]).

(59) Darüber hinaus ist im Data (Use and Access) Act festgelegt, dass die Information Commission, soweit dies unter den gegebenen Umständen relevant ist, 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 bei der Wahrnehmung ihrer Aufgaben im Rahmen der Datenschutzvorschriften berücksichtigt ([82]). Im EU-Datenschutzrecht wird ebenfalls anerkannt, dass der Schutz personenbezogener Daten mit mehreren anderen Grundrechten und Zielen wie Sicherheit und Justiz in Einklang zu bringen ist ([83]).

2.3.2. *Durchsetzung, einschließlich Sanktionen, und Rechtsbehelfe*

(60) Die Befugnisse und Aufgaben der Information Commission entsprechen weiterhin denen der Datenschutzaufsichtsbehörden der Mitgliedstaaten gemäß den einschlägigen Artikeln der Richtlinie (EU) 2016/680 ([84]), wie in den Erwägungsgründen 100 bis 109 des Durchführungsbeschlusses (EU) 2021/1773 bewertet.

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

(62) Durch Paragraf 97 des Data (Use and Access) Act wurde Paragraf 142 des DPA 2018 geändert, um der Information Commission ausdrücklich zu gestatten, nicht nur Informationen, sondern auch bestimmte Dokumente anzufordern, um ihre Fähigkeit zur Untersuchung und Überprüfung der Einhaltung der Vorschriften zu verbessern.

(63) Mit Paragraf 98 des Data (Use and Access) Act wurden die Befugnisse der Information Commission gemäß Paragraf 146 des DPA 2018 erweitert, indem die Information Commission ermächtigt wurde, von einem Verantwortlichen oder Auftragsverarbeiter die Erstellung eines unabhängigen Berichts zu einer bestimmten Angelegenheit zu verlangen. Der Bericht muss von einer „zugelassenen Person" erstellt werden; die Information Commission hat die endgültige Befugnis, die vorgeschlagene Person zu bestätigen oder eine Person zu bestellen, wenn kein geeigneter Vorschlag unterbreitet wird oder der Verantwortliche nicht tätig wird ([85]). In der Prüfungsmitteilung können das Format, der Inhalt und die Frist für den Bericht festgelegt werden ([86]). Alle damit verbundenen Kosten, einschließlich der Gebühren der zugelassenen Person, sind vom Verantwortlichen oder vom Auftragsverarbeiter zu tragen ([87]).

(64) Paragraf 100 des Data (Use and Access) Act führt Befragungsmitteilungen als neues Durchsetzungsinstrument nach Paragraf 148A des DPA 2018 ein. Die Information Commission kann eine Person unter Wahrung von Schutzvorkehrungen wie dem Schutz vor Selbstbelastung und dem Schutz des Anwaltsgeheimnisses zur Teilnahme an Befragungen verpflichten ([88]).

(65) Paragraf 101 des Data (Use and Access) Act ändert Anhang 16 des DPA 2018, um der Information Commission mehr Flexibilität bei der Ausstellung von Sanktionsmitteilungen zu ermöglichen. Während die derzeitige Sechsmonatsfrist für die Ausstellung eines endgültigen Sanktionsbescheids nach einer Absichtsanzeige weiterhin die allgemeine Regel bleibt, darf die Information Commission eine Sanktionsmitteilung auch nach Ablauf dieser Frist erlassen, wenn es nach vernünftigem Ermessen nicht möglich ist, die Frist einzuhalten. In solchen Fällen muss der Bescheid so bald wie möglich erfolgen. Beschließt die Information Commission, keinen Bußgeldbescheid zu erlassen, so muss sie die betroffene Person innerhalb von sechs Monaten, oder sobald dies nach vernünftigem Ermessen möglich ist, schriftlich davon in Kenntnis setzen. Der Paragraf führt zudem eine neue Verpflichtung für die Information Commission ein, Leitlinien zu den Umständen zu veröffentlichen, unter denen für die Ausstellung eines Sanktionsbescheids mehr als sechs Monate benötigt werden können.

([80]) Anhang 13 des DPA 2018.
([81]) Paragraf 91 des Data (Use and Access) Act, mit dem Paragraf 120A des DPA 2018 eingeführt wird.
([82]) Paragraf 91 des Data (Use and Access) Act, mit dem Paragraf 120B des DPA 2018 eingeführt wird.
([83]) Siehe Erwägungsgrund 2 der Richtlinie (EU) 2016/680.
([84]) Anhang 13 Paragraf 2 des DPA 2018.
([85]) Paragraf 98 des Data (Use and Access) Act, mit dem Paragraf 146A des DPA 2018 eingeführt wird.
([86]) Paragraf 98 des Data (Use and Access) Act, mit dem Paragraf 146(3A) des DPA 2018 eingeführt wird.
([87]) Paragraf 98 des Data (Use and Access) Act, mit dem Paragraf 146(11A) des DPA 2018 eingeführt wird.
([88]) Paragraf 98 des Data (Use and Access) Act, mit dem Paragraf 146(8B) des DPA 2018 eingeführt wird.

(66) Paragraf 102 des Data (Use and Access) Act führt neue Berichtspflichten für die Information Commission ein. Er ändert Paragraf 139 und fügt einen neuen Paragraf 161A in das DPA 2018 ein, der die Information Commission verpflichtet, einen Jahresbericht über ihr aufsichtsrechtliches Handeln zu veröffentlichen. In diesem Bericht muss dargelegt werden, wie die Ermittlungs- und Durchsetzungsbefugnisse nach der UK GDPR und den Teilen 3 und 4 des DPA 2018 ausgeübt wurden. Außerdem muss darin die Anzahl der Bußgeldbescheide offengelegt werden, die nach Ablauf des Sechsmonatszeitraums nach einer Absichtserklärung erlassen wurden, und die Verzögerung begründet werden. Darüber hinaus muss in dem Bericht erläutert werden, wie die Information Commission ihre eigenen Leitlinien befolgt hat, wenn sie Regulierungsentscheidungen trifft.

(67) Paragraf 103 des Data (Use and Access) Act stärkt das Beschwerdeverfahren für betroffene Personen. Er fügt die neuen Paragrafen 164A und 164B in das DPA 2018 ein. In Paragraf 164A ist vorgesehen, dass betroffene Personen das Recht haben, direkt bei den Verantwortlichen Beschwerde einzulegen, wenn sie der Ansicht sind, dass ihre Rechte nach der UK GDPR oder Teil 3 des DPA 2018 verletzt wurden. Die Verantwortlichen müssen dieses Verfahren ermöglichen, Beschwerden innerhalb von 30 Tagen zur Kenntnis nehmen und unverzüglich antworten. Außerdem müssen sie die Antragsteller über die Fortschritte und Ergebnisse auf dem Laufenden halten. Nach Paragraf 164B ist der Secretary of State befugt, Vorschriften zu erlassen, mit denen die Verantwortlichen verpflichtet werden, die Zahl der eingegangenen Beschwerden zu melden.

(68) Paragraf 104 des Data (Use and Access) Act fügt einen neuen Paragrafen 180A in das DPA 2018 ein, um die Befugnisse der Gerichte in Verfahren über Auskunftsersuchen betroffener Personen klarzustellen. Nach dieser Bestimmung können die Gerichte von den Verantwortlichen verlangen, die strittigen Informationen dem Gericht zur Prüfung vorzulegen, wenn sie darüber entscheiden, ob eine betroffene Person Anspruch auf diese Informationen hat. Die Informationen dürfen jedoch nicht an die betroffene Person weitergegeben werden, es sei denn, das Gericht entscheidet, dass sie ein Auskunftsrecht hat. Dieser Paragraf stellt klar, dass die Gerichte strittiges Material prüfen können, ohne es vorzeitig an die klagende Partei offenzulegen, und stellt damit eine zuvor im Data Protection Act 1998 bestehende Schutzvorkehrung wieder her.

(69) Im Hinblick auf die Umsetzung dieser Befugnisse hat der Information Commissioner seit dem Erlass des Durchführungsbeschlusses (EU) 2021/1773 zahlreiche Beschwerden bearbeitet ([89]) sowie 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 ([90]). Der Information Commissioner veröffentlichte und aktualisierte außerdem Leitlinien, Stellungnahmen und Leitfäden, etwa zum Recht auf Auskunft oder zum Umgang mit offensichtlich unbegründeten oder übermäßigen Anträgen nach Teil 3 des DPA 2018 ([91]) oder auch seinen Leitfaden zur Datenverarbeitung durch Strafverfolgungsbehörden ([92]).

3. SCHLUSSFOLGERUNG

(70) Die Kommission ist der Ansicht, dass Teil 3 des DPA 2018 für zu Strafverfolgungszwecken von zuständigen Behörden in der Europäischen Union an zuständige Behörden im Vereinigten Königreich übermittelte personenbezogene Daten weiterhin ein Schutzniveau bietet, das der Sache nach dem durch die Richtlinie (EU) 2016/680 garantierten Schutzniveau gleichwertig ist.

([89]) 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.

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

([91]) 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/.

([92]) Abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/.

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

(72) Daher sollte beschlossen werden, dass das Vereinigte Königreich weiterhin ein angemessenes Schutzniveau im Sinne des Artikels 36 Absatz 2 der Richtlinie (EU) 2016/680 gemäß seiner Auslegung im Lichte der Charta der Grundrechte der Europäischen Union gewährleistet.

4. AUSWIRKUNGEN DIESES BESCHLUSSES UND MAßNAHMEN DER DATENSCHUTZBEHÖRDEN

(73) 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.

(74) Daher ist ein nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 erlassener Angemessenheitsbeschluss der Kommission für alle Organe der Mitgliedstaaten, an die er gerichtet ist, einschließlich ihrer unabhängigen Aufsichtsbehörden, verbindlich. Insbesondere können während der Geltungsdauer des Durchführungsbeschlusses (EU) 2021/1773 in der durch diesen Beschluss geänderten Fassung Übermittlungen von einem Verantwortlichen oder Auftragsverarbeiter in der Union an Verantwortliche oder Auftragsverarbeiter im Vereinigten Königreich erfolgen, ohne dass eine weitere Genehmigung eingeholt werden muss.

(75) Gleichzeitig sei daran erinnert, dass gemäß Artikel 47 Absatz 5 der Richtlinie (EU) 2016/680 und wie vom Gerichtshof im Urteil *Schrems I* erläutert 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 in Frage stellt, muss das nationale Recht Rechtsbehelfe vorsehen, die es der Datenschutzbehörde ermöglichen, diese Rügen vor einem nationalen Gericht geltend zu machen, das gegebenenfalls ein Vorabentscheidungsverfahren beim Gerichtshof einleiten muss ([93]).

5. ÜBERWACHUNG

(76) Gemäß Artikel 36 Absatz 4 der Richtlinie (EU) 2016/680 überwacht die Kommission fortlaufend die einschlägigen Entwicklungen im Vereinigten Königreich, um festzustellen, ob dort weiterhin ein der Sache nach 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; ferner der Wirksamkeit der Ausübung individueller Rechte, einschließlich aller relevanten Entwicklungen in Recht und Praxis in Bezug auf die neu eingeführten Ausnahmen oder Beschränkungen dieser Rechte, und der Funktionsweise des umstrukturierten ICO, auch in Bezug auf die Bearbeitung von Beschwerden und die Anwendung von Abhilfebefugnissen. Unter anderem sollten Entwicklungen in der Rechtsprechung sowie die Aufsicht durch das ICO und andere unabhängige Stellen in die Überwachung der Kommission einfließen.

(77) Zur Vereinfachung dieser Überwachung sollten die Behörden des Vereinigten Königreichs die Kommission unverzüglich und regelmäßig über jede wesentliche Änderung der Rechtsordnung des Vereinigten Königreichs unterrichten, die sich auf den Rechtsrahmen auswirkt, der Gegenstand des Durchführungsbeschlusses (EU) 2021/1773 in der durch den vorliegenden Beschluss geänderten Fassung ist, sowie über jede Entwicklung der im Durchführungsbeschluss (EU) 2021/1773 (in der durch den vorliegenden Beschluss geänderten Fassung) bewerteten Verfahrensweisen im Zusammenhang mit der Verarbeitung personenbezogener Daten, insbesondere im Hinblick auf die in Erwägungsgrund 39 genannten Elemente.

(78) 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 jeden Hinweis darauf informiert werden, dass die Maßnahmen der Behörden des Vereinigten Königreichs, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständig sind, einschließlich der Aufsichtsbehörden, nicht das erforderliche Schutzniveau gewährleisten.

([93]) Schrems I, Rn. 65.

(79) Lassen verfügbare Informationen — insbesondere Informationen, die sich aus der Überwachung dieses Beschlusses ergeben oder vom Vereinigten Königreich oder den Mitgliedstaaten bereitgestellt werden — darauf schließen, dass das vom Vereinigten Königreich gewährleistete Schutzniveau möglicherweise nicht mehr angemessen ist, sollte die Kommission die zuständigen Behörden des Vereinigten Königreichs unverzüglich davon in Kenntnis setzen und sie auffordern, innerhalb einer bestimmten Frist, die drei Monate nicht überschreiten darf, geeignete Maßnahmen zu ergreifen. Sofern erforderlich, kann dieser Zeitraum je nachdem, worum es sich handelt und/oder welche Maßnahmen zu ergreifen sind, um eine bestimmte Frist verlängert werden.

(80) 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 58 Absatz 2 der Richtlinie (EU) 2016/680 einleiten, um diesen Beschluss teilweise oder vollständig auszusetzen oder aufzuheben.

(81) Alternativ wird die Kommission dieses Verfahren einleiten, um den Durchführungsbeschluss (EU) 2021/1773 in der durch diesen Beschluss geänderten Fassung anzupassen, indem sie insbesondere Datenübermittlungen zusätzlichen Bedingungen unterwirft oder den Anwendungsbereich der Angemessenheitsfeststellung auf jene Datenübermittlungen beschränkt, für die weiterhin ein angemessenes Schutzniveau gewährleistet ist.

(82) In hinreichend begründeten Fällen äußerster Dringlichkeit wird die Kommission von der Möglichkeit Gebrauch machen, nach dem in Artikel 58 Absatz 3 der Richtlinie (EU) 2016/680 genannten Verfahren sofort geltende Durchführungsrechtsakte zur Aussetzung, Aufhebung oder Änderung des Beschlusses zu erlassen.

6. ÜBERPRÜFUNG, GELTUNGSDAUER UND ERNEUERUNG DIESES BESCHLUSSES

(83) In Anwendung von Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 und angesichts der Tatsache, dass sich das durch den Rechtsrahmen des Vereinigten Königreichs gewährte Schutzniveau ändern könnte, sollte die Kommission nach der Annahme dieses Beschlusses regelmäßig prüfen, ob die Feststellungen über die Angemessenheit des durch das Vereinigte Königreich gewährleisteten Schutzniveaus noch sachlich und rechtlich gerechtfertigt sind. 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.

(84) 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.

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

(86) Die Kommission muss auch berücksichtigen, dass sich der in diesem Beschluss und im Durchführungsbeschluss (EU) 2021/1773 bewertete Datenschutzrahmen weiterentwickeln kann.

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

(88) 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 58 Absatz 2 der Verordnung (EU) 2016/680 genannten Verfahren zu erlassen.

7. SCHLUSSBEMERKUNGEN

(89) Der Europäische Datenschutzausschuss hat eine Stellungnahme ([94]) veröffentlicht, der bei der Ausarbeitung dieses Beschlusses Rechnung getragen wurde.

(90) Die in diesem Beschluss vorgesehene Maßnahme entspricht der Stellungnahme des nach Artikel 58 der Richtlinie (EU) 2016/680 eingesetzten Ausschusses.

(91) Nach Artikel 6a des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts sind die Bestimmungen der Richtlinie (EU) 2016/680, und somit dieses Durchführungsbeschlusses, die sich auf die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten beziehen, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, für Irland nicht bindend, wenn Irland nicht durch die Vorschriften gebunden ist, die Formen der justiziellen Zusammenarbeit in Strafsachen oder der polizeilichen Zusammenarbeit regeln, in deren Rahmen die auf der Grundlage des Artikels 16 AEUV festgelegten Vorschriften eingehalten werden müssen. Dennoch ist die Richtlinie (EU) 2016/680 aufgrund des Durchführungsbeschlusses (EU) 2020/1745 des Rates ([95]) ab dem 1. Januar 2021 vorläufig in Kraft zu setzen und auf Irland anzuwenden. Irland ist daher durch diesen Beschluss zu denselben Bedingungen gebunden, die auch für die Anwendung der Richtlinie (EU) 2016/680 in Irland gelten, entsprechend dem Durchführungsbeschluss (EU) 2020/1745 im Hinblick auf den Teil des Schengen-Besitzstands, an dem es sich beteiligt.

(92) Nach den Artikeln 2 und 2a des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks ist Dänemark durch die Bestimmungen der Richtlinie (EU) 2016/680, und somit dieses Durchführungsbeschlusses, die sich auf die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten beziehen, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, weder gebunden noch zu ihrer Anwendung verpflichtet. Da die Richtlinie (EU) 2016/680 jedoch den Schengen-Besitzstand ergänzt, teilte Dänemark gemäß Artikel 4 des genannten Protokolls am 26. Oktober 2016 seinen Beschluss mit, die Richtlinie (EU) 2016/680 umzusetzen. Dänemark ist daher völkerrechtlich zur Umsetzung des vorliegenden Beschlusses verpflichtet.

(93) Für Island und Norwegen stellt dieser Beschluss eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar ([96]).

(94) Für die Schweiz stellt dieser Beschluss eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar ([97]).

(95) Für Liechtenstein stellt dieser Beschluss eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar ([98]).

(96) Der Durchführungsbeschluss (EU) 2021/1773 sollte daher entsprechend geändert werden —

([94]) Stellungnahme 27/2025 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission zur Änderung der Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, abrufbar unter folgendem Link: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_en.

([95]) Durchführungsbeschluss (EU) 2020/1745 des Rates vom 18. November 2020 zur Inkraftsetzung der Bestimmungen des Schengen-Besitzstands über Datenschutz und zur vorläufigen Inkraftsetzung von einigen Bestimmungen des Schengen-Besitzstands in Irland (ABl. L 393 vom 23.11.2020, S. 3, ELI: http://data.europa.eu/eli/dec_impl/2020/1745/oj).

([96]) Übereinkommen zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands – Schlußakte (ABl. L 176 vom 10.7.1999, S. 36, ELI: http://data.europa.eu/eli/agree_internation/1999/439(1)/oj).

([97]) ABl. L 53 vom 27.2.2008, S. 52.

([98]) ABl. L 160 vom 18.6.2011, S. 21.

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Artikel 4 des Durchführungsbeschlusses (EU) 2021/1773 erhält folgende Fassung:

„*Artikel 4*

Dieser Beschluss tritt am 27. Dezember 2031 außer Kraft, sofern er nicht gemäß dem in Artikel 58 Absatz 2 der Richtlinie (EU) 2016/680 genannten Verfahren verlängert wird."

Artikel 2

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 19. Dezember 2025

Für die Kommission
Michael MCGRATH
Mitglied der Kommission