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

(Bekannt gegeben unter Aktenzeichen C(2021) 4801)

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 ([1]) des Rates, insbesondere auf Artikel 36 Absatz 3,

in Erwägung nachstehender Gründe:

1. EINFÜHRUNG

(1) Die Richtlinie (EU) 2016/680 enthält die Vorschriften für die Übermittlung personenbezogener Daten durch zuständige Behörden in der Union an Drittländer und internationale Organisationen, soweit die betreffenden Übermittlungen in ihren Anwendungsbereich fallen. Die Vorschriften für internationale Übermittlungen personenbezogener Daten durch die zuständigen Behörden sind in Kapitel V der Richtlinie (EU) 2016/680, insbesondere in den Artikeln 35 bis 40, festgelegt. Der Fluss personenbezogener Daten in Drittländer und aus Drittländern ist für die wirksame Zusammenarbeit bei der Strafverfolgung wesentlich, wobei jedoch sichergestellt sein muss, dass das unionsweit gewährleistete Schutzniveau für personenbezogene Daten bei solchen Übermittlungen nicht beeinträchtigt wird ([2]).

(2) Nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau bieten. Unter dieser Voraussetzung können personenbezogene Daten nach Artikel 35 Absatz 1 und Erwägungsgrund 66 der Richtlinie (EU) 2016/680 ohne weitere Genehmigung an ein Drittland übermittelt werden (es sei denn, dass ein anderer Mitgliedstaat, von dem die Daten stammen, die Übermittlung zu genehmigen hat).

(3) Wie in Artikel 36 Absatz 2 der Richtlinie (EU) 2016/680 festgelegt, muss die Annahme eines Angemessenheitsbeschlusses auf einer umfassenden Analyse der Rechtsordnung des Drittlands beruhen. Die Kommission muss im Rahmen ihrer Prüfung feststellen, ob das betreffende Drittland ein Schutzniveau garantiert, das dem innerhalb der Europäischen Union gewährleisteten Schutzniveau „der Sache nach gleichwertig" ist (Erwägungsgrund 67 der Richtlinie (EU) 2016/680). Die Frage, ob ein Schutzniveau „der Sache nach gleichwertig" ist, wird anhand des Maßstabs beurteilt, der in den EU-Rechtsvorschriften, insbesondere in der Richtlinie (EU) 2016/680, festgelegt und durch die Rechtsprechung des Gerichtshofs der Europäischen Union ([3]) entwickelt wurde. Die vom Europäischen Datenschutzausschuss herausgegebene Referenzgrundlage für Angemessenheit ist in diesem Zusammenhang ebenfalls von Bedeutung ([4]).

(4) Der Gerichtshof der Europäischen Union hat klargestellt, dass es dazu keines identischen Schutzniveaus bedarf ([5]). 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. ([6]) Daher erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den Vorschriften der Union. Die Frage ist vielmehr, ob das ausländische System insgesamt aufgrund des Wesensgehalts der Rechte auf Privatsphäre sowie ihrer wirksamen Anwendung, Überwachung und Durchsetzung das erforderliche Maß an Schutz ([7]) bietet.

([1]) ABl. L 119 vom 4.5.2016, S. 89.
([2]) Siehe Erwägungsgrund 64 der Richtlinie (EU) 2016/680.
([3]) Siehe zuletzt Rechtssache C-311/18, Maximilian Schrems/Data Protection Commissioner („Schrems II"), ECLI:EU:C:2020:559.
([4]) Siehe die Empfehlungen 01/2021 zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung, angenommen im Februar 2021, abrufbar unter folgendem Link: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_de
([5]) Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner (im Folgenden „Schrems"), ECLI:EU:C:2015:650, Rn. 73.
([6]) Schrems, Rn. 74.
([7]) 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/PDF/?uri=CELEX:52017DC0007&from=EN

(5) Die Kommission hat das einschlägige Recht und die einschlägige Praxis im Vereinigten Königreich sorgfältig analysiert. Auf der Grundlage ihrer nachstehenden Feststellungen kommt die Kommission zu dem Schluss, dass das Vereinigte Königreich ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die von zuständigen Behörden in der Union, die in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, an zuständige Behörden im Vereinigten Königreich, die in den Anwendungsbereich von Teil 3 des Gesetzes über den Datenschutz von 2018 (Data Protection Act 2018 — im Folgenden „DPA 2018“) ([8]) fallen, übermittelt werden.

(6) Dieser Beschluss hat zur Folge, dass solche Übermittlungen für einen Zeitraum von vier Jahren, vorbehaltlich einer etwaigen Verlängerung und unbeschadet der in Artikel 35 der Richtlinie (EU) 2016/680 festgelegten Bedingungen, ohne weitere Genehmigung vorgenommen werden dürfen.

2. VORSCHRIFTEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN DURCH ZUSTÄNDIGE BEHÖRDEN FÜR ZWECKE DER STRAFVERFOLGUNG

2.1. Der konstitutionelle Rahmen

(7) Das Vereinigte Königreich ist eine parlamentarische Demokratie. Das Land verfügt über ein souveränes Parlament, das allen anderen staatlichen Einrichtungen übergeordnet ist, eine aus dem Parlament hervorgehende und ihm gegenüber rechenschaftspflichtige Exekutive sowie eine unabhängige Justiz. Die Exekutive bezieht ihre Hoheitsgewalt daraus, dass sie das Vertrauen der gewählten Mitglieder des Unterhauses genießt; sie ist gegenüber beiden Kammern des Parlaments (dem Unterhaus und dem Oberhaus) rechenschaftspflichtig, die für die Kontrolle der Regierung und die Erörterung sowie Verabschiedung von Gesetzesinitiativen verantwortlich sind. Das britische Parlament hat dem schottischen Parlament, dem walisischen Parlament (Senedd Cymru) und der parlamentarischen Versammlung für Nordirland die Verantwortung für die Gesetzgebung in bestimmten inneren Angelegenheiten in Schottland, Wales und Nordirland übertragen. Während Datenschutzfragen dem britischen Parlament vorbehalten sind — d. h. in diesem Bereich gelten landesweit einheitliche Rechtsvorschriften —, wurden andere für diesen Beschluss relevante Politikbereiche den Parlamenten der einzelnen Landesteile übertragen. So wurde beispielsweise die Zuständigkeit für die Strafrechtssysteme Schottlands und Nordirlands, einschließlich polizeilicher Aufgaben (d. h. der von Polizeikräften ausgeführten Tätigkeiten), an das schottische Parlament bzw. die parlamentarische Versammlung für Nordirland ([9]) übertragen.

(8) Das Vereinigte Königreich besitzt keine kodifizierte Verfassung im Sinne eines konkreten Verfassungsdokuments; vielmehr haben sich die Verfassungsgrundsätze im Laufe der Zeit auf der Grundlage der Rechtsprechung und insbesondere des Gewohnheitsrechts fortentwickelt. Der Verfassungsrang bestimmter Dokumente, wie der Magna Carta, der Bill of Rights von 1689 und des Gesetzes über die Menschenrechte (Human Rights Act) von 1998, ist anerkannt. Maßgeblich für die Entwicklung der Grundrechte des Einzelnen als Teil der Verfassung waren das Gewohnheitsrecht („Common Law“), die genannten Dokumente sowie internationale Verträge, insbesondere die Europäische Menschenrechtskonvention (im Folgenden „EMRK“), die das Vereinigte Königreich im Jahr 1951 ratifiziert hat. Im Jahr 1987 hat das Vereinigte Königreich außerdem das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (im Folgenden „Übereinkommen Nr. 108“) ratifiziert ([10]).

(9) 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 EMRK, in den Artikeln 1 bis 3 ihres Ersten Protokolls und in Artikel 1 ihres Dreizehnten Protokolls in Verbindung mit den Artikeln 16 bis 18 EMRK festgelegt sind. Dazu zählen das Recht auf Achtung des Privat- und Familienlebens, was das Recht auf Datenschutz einschließt, und das Recht auf ein faires Verfahren ([11]). Insbesondere darf eine Behörde gemäß Artikel 8 EMRK in die Ausübung des Rechts auf Privatsphäre nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

([8]) Data Protection Act 2018, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/12/contents

([9]) Explanatory Framework for Adequacy Discussions, Section F: Law enforcement, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

([10]) Die Grundsätze des Übereinkommens Nr. 108 wurden ursprünglich durch das Gesetz über den Datenschutz von 1984 (Data Protection Act 1984) in das Recht des Vereinigten Königreichs umgesetzt; dieses wurde später durch das Gesetz über den Datenschutz von 1998 (Data Protection Act 1998) und dann wiederum durch das Gesetz über den Datenschutz von 2018 (Data Protection Act 2018) ersetzt, das in Verbindung mit der britischen Datenschutz-Grundverordnung (United Kingdom General Data Protection Regulation) ausgelegt wird. Des Weiteren hat das Vereinigte Königreich im Jahr 2018 das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (im Folgenden „Übereinkommen Nr. 108+“) unterzeichnet und arbeitet derzeit an der Ratifizierung dieses Übereinkommens.

([11]) Artikel 6 und 8 EMRK (siehe auch Anhang 1 des Human Rights Act 1998).

(10) Nach dem Human Rights Act 1998 muss jede Handlung von Behörden mit einem in der EMRK garantierten Recht vereinbar sein ([12]). Darüber hinaus sind primärrechtliche und nachrangige Bestimmungen so auszulegen und umzusetzen, dass sie mit diesen Rechten vereinbar sind ([13]). Soweit eine Privatperson der Ansicht ist, dass ihre Rechte, einschließlich ihrer Rechte auf Privatsphäre und Datenschutz, durch eine Behörde verletzt wurden, kann sie auf der Grundlage des Human Rights Act 1998 die Gerichte des Vereinigten Königreichs anrufen, und kann letztlich, nach Ausschöpfung aller nationalen Rechtsbehelfe, den Europäischen Gerichtshof für Menschenrechte wegen Verletzung ihrer nach der EMRK garantierten Rechte anrufen.

2.2. **Der Rechtsrahmen des Vereinigten Königreichs für Datenschutz**

(11) Das Vereinigte Königreich ist zum 31. Januar 2020 aus der Europäischen Union ausgetreten. Auf der Grundlage des Abkommens über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft ([14]) fand das Unionsrecht im Vereinigten Königreich während des Übergangszeitraums bis zum 31. Dezember 2020 weiterhin Anwendung. Vor dem Austritt und während des Übergangszeitraums bestand im Vereinigten Königreich der Rechtsrahmen für den Schutz personenbezogener Daten, der 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 regelte, aus den einschlägigen Teilen des Data Protection Act 2018, mit dem die Richtlinie (EU) 2016/680 in nationales Recht umgesetzt wurde.

(12) Zur Vorbereitung auf den Austritt aus der EU erließ die Regierung des Vereinigten Königreichs das Gesetz von 2018 über den Austritt aus der Europäischen Union (European Union (Withdrawal) Act 2018 — im Folgenden „EUWA“) ([15]), durch das unmittelbar geltende Rechtsvorschriften der Union in das Recht des Vereinigten Königreichs übernommen wurden und das besagte, dass aus Unionsrecht abgeleitete innerstaatliche Rechtsvorschriften („EU-derived domestic legislation“) auch nach Ende des Übergangszeitraums wirksam bleiben. Teil 3 des DPA 2018 ([16]) zur Umsetzung der Richtlinie (EU) 2016/680 stellt eine solche aus Unionsrecht abgeleitete innerstaatliche Rechtsvorschrift im Sinne des EUWA dar. Gemäß EUWA muss eine unverändert aus Unionsrecht abgeleitete innerstaatliche Rechtsvorschrift von den Gerichten des Vereinigten Königreichs gemäß der einschlägigen Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof“) und den allgemeinen Grundsätzen des Unionsrechts ausgelegt werden, so wie sie unmittelbar vor dem Ende des Übergangszeitraums galten (bezeichnet als „beibehaltene EU-Rechtsprechung“ („retained EU case law“) bzw. als „beibehaltene allgemeine Grundsätze des EU-Rechts“ („retained general principles of EU law“)) ([17]).

(13) Gemäß EUWA sind die Minister des Vereinigten Königreichs befugt, im Wege von Verordnungen abgeleitete Rechtsvorschriften einzuführen, um aufgrund des Austritts des Vereinigten Königreichs aus der Union notwendige Änderungen am beibehaltenen EU-Recht vorzunehmen. Diese Befugnis wurde durch Erlass der 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“) ([18]) ausgeübt. Mit diesen Verordnungen werden die Datenschutzgesetze des Vereinigten Königreichs, einschließlich des DPA 2018, geändert, um sie an den nationalen Kontext anzupassen ([19]).

([12]) Paragraf 6 des Human Rights Act 1998.

([13]) Paragraf 3 des Human Rights Act 1998.

([14]) Abkommen über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft (2019/C 384 I/01, XT/21054/2019/INIT, ABl. C 384I vom 12.11.2019, S. 1) (im Folgenden „Austrittsabkommen“), abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

([15]) Gesetz von 2018 über den Austritt (European Union (Withdrawal) Act 2018), abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) Data Protection Act 2018, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/12/contents

([17]) Paragraf 6 EUWA 2018.

([18]) Data Protection, Privacy and Electronic Communications (Amendments usw.) (EU Exit) Regulations 2019, abrufbar unter folgendem Link: https://www.legislation.gov.uk/uksi/2019/419/contents/made, geändert durch die DPPEC-Verordnungen 2020, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) Durch die im Zuge des EU-Austritts erlassenen Verordnungen wurde Teil 3 des DPA 2018 in verschiedenen Punkten geändert. Vielfach handelt es sich dabei um technische Änderungen, etwa die Streichung von Verweisen auf den „Mitgliedstaat“ oder auf die „Richtlinie zum Datenschutz bei der Strafverfolgung“ (siehe z. B. Paragraf 48 Absatz 8 oder Paragraf 73 Absatz 5 Buchstabe a DPA 2018 im Zusammenhang mit „domestic law“), sodass Teil 3 nach Ende des Übergangszeitraums als innerstaatliche Rechtsvorschrift wirksam ist. An einigen Stellen waren andere Arten von Änderungen erforderlich, zum Beispiel bei der Frage, wer („who“) Angemessenheitsbeschlüsse („adequacy decisions“) für die Zwecke der britischen Datenschutzvorschriften erlässt (siehe Paragraf 74A DPA 2018), d. h. der Secretary of State anstelle der Europäischen Kommission.

(14) Folglich werden im Vereinigten Königreich die Rechtsnormen über die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafverfolgung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, nach dem Übergangszeitraum gemäß dem Austrittsabkommen weiterhin in den einschlägigen Teilen des DPA 2018 (jedoch in der durch die DPPEC Regulations geänderten Fassung) und insbesondere in Teil 3 dieses Gesetzes geregelt. Die britische Datenschutz-Grundverordnung (United Kingdom General Data Protection Regulation — im Folgenden „UK GDPR“) findet auf diese Art der Verarbeitung keine Anwendung.

(15) Teil 3 des DPA 2018 enthält die Vorschriften über die Verarbeitung personenbezogener Daten für Zwecke der Strafverfolgung, einschließlich der Datenschutzgrundsätze, der Rechtsgrundlagen für die Verarbeitung (Rechtmäßigkeit), der Rechte der betroffenen Personen, der Verpflichtungen der zuständigen Behörden als Verantwortliche und Einschränkungen der Weiterübermittlung. Gleichzeitig sind die geltenden Vorschriften für Aufsicht, Durchsetzung und Rechtsbehelfe, die im Bereich der Strafverfolgung zur Anwendung kommen, in den Teilen 5 und 6 des DPA 2018 festgelegt.

(16) Um der wichtigen Rolle der Polizeikräfte im Bereich der Strafverfolgung Rechnung zu tragen, sollten auch die Vorschriften zur Regelung der Polizeiarbeit berücksichtigt werden. Da die Polizeiarbeit dezentralisiert gehandhabt wird, ist sie in a) England und Wales, b) Schottland und c) Nordirland durch unterschiedliche, aber inhaltlich oftmals ähnliche Gesetze geregelt ([20]). Darüber hinaus liefern verschiedene Arten von Leitliniendokumenten zusätzliche Klarstellungen zum Einsatz polizeilicher Befugnisse. Es gibt drei wesentliche Formen von Leitlinien für die Polizeiarbeit: 1. In Gesetzesform erlassene Anweisungen, zum Beispiel der Ethik-Kodex (Code of Ethics) ([21]) und der Verhaltenskodex für die Verwaltung polizeilicher Informationen (Code of Practice on the Management of Police Information — im Folgenden „MoPI Code of Practice“) ([22]), eingeführt gemäß dem Polizeigesetz (Police Act) von 1996 ([23]), oder die gemäß dem Gesetz über polizeiliche und strafrechtliche Beweismittel (Police and Criminal Evidence Act) ([24]) eingeführten Kodizes (im Folgenden „PACE-Codes“) ([25]); 2. die vom College of Policing erstellten Leitlinien über zugelassene dienstliche Vorgehensweisen bei der Verwaltung polizeilicher Informationen (Authorised Professional Practice on the Management of Police Information — im Folgenden „APP Guidance on the Management of Police Information“ oder „APP Guidance“) ([26]), sowie 3. operative Leitlinien (herausgegeben von der Polizei selbst). Der National Police Chiefs Council (eine für alle Polizeikräfte im Vereinigten Königreich zuständige Koordinierungsstelle) gibt operative Leitlinien heraus, die von allen Polizeikräften gebilligt wurden und somit landesweit gelten ([27]). Diese Leitlinien sollen für dienststellenübergreifend einheitliche Vorgehensweisen bei der Informationsverwaltung sorgen ([28]).

(17) Der MoPI Code of Practice wurde 2005 vom Secretary of State in Anwendung seiner Befugnisse nach Paragraf 39A des Police Act 1996 herausgegeben ([29]). Jeder nach dem Police Act herausgegebene Verhaltenskodex muss vom Secretary of State genehmigt werden; außerdem muss die National Crime Agency dazu konsultiert werden, bevor er dem Parlament vorgelegt wird. Nach Paragraf 39A Absatz 7 des Police Act hat die Polizei nach dem Gesetz erlassene Kodizes gebührend zu berücksichtigen, sodass von ihr erwartet wird, sich an die darin enthaltenen Vorgaben zu

([20]) Ausführlichere Erläuterungen zu den Polizeikräften und ihren Befugnissen im Vereinigten Königreich siehe Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement (siehe Fußnote 9).

([21]) The Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales, abrufbar unter folgendem Link: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Police Service Northern Ireland Code of Ethics, abrufbar unter folgendem Link: https://www.nipolicingboard.org.uk/psni-code-ethics; Code of Ethics for policing in Scotland, abrufbar unter folgendem Link: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([22]) Code of Practice on the Management of Police Information, abrufbar unter folgendem Link: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([23]) Police Act 1996, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/1996/16/contents

([24]) Police and Criminal Evidence Act 1984, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/1984/60/contents

([25]) Verhaltenskodizes nach dem Police and Criminal Evidence Act 1984 (PACE), abrufbar unter folgendem Link: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

([26]) Authorised Professional Practice on the Management of Police Information, abrufbar unter folgendem Link: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) Data Protection Manual for Police Data Protection Professionals, abrufbar unter folgendem Link: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) So gilt zum Beispiel der MoPI Code of Practice (siehe Fußnote 22) für die Speicherung operativer polizeilicher Informationen (siehe Erwägungsgrund 47 dieses Beschlusses).

([29]) Wie die britischen Behörden erläuterten, wurde während der Gespräche über das Thema Angemessenheit vom College of Policing gerade ein Verhaltenskodex für die Informations- und Dokumentenverwaltung (Information and Records Management Code of Practice) erarbeitet, der den MoPI Code of Practice ersetzen soll. Der Entwurf des Kodex wurde am 25. Januar 2021 zur öffentlichen Konsultation veröffentlicht und ist unter folgendem Link abrufbar: https://www.college.police.uk/article/information-records-management-consultation

halten ([30]). Darüber hinaus müssen Leitlinien ohne Gesetzescharakter (wie etwa die APP Guidance on the Management of Police Information) immer mit dem MoPI Code of Practice vereinbar sein, der solchen Leitlinien übergeordnet ist ([31]). Auch wenn Polizeibeamte in bestimmten operativen Situationen gezwungen sein können, von diesem Leitfaden abzuweichen, sind sie in jedem Fall verpflichtet, die Vorschriften von Teil 3 des DPA 2018 einzuhalten ([32]).

(18) Weitere Leitlinien zu den Datenschutzvorschriften des Vereinigten Königreichs für die Verarbeitung von Daten im Bereich der Strafverfolgung werden vom Büro des Information Commissioner (Information Commissioner's Office — im Folgenden „ICO") ([33]) bereitgestellt (nähere Informationen zum ICO finden sich in den Erwägungsgründen 93 bis 109). Obwohl die Leitlinien nicht rechtsverbindlich sind, wären die Gerichte in einem Verfahren verpflichtet, einen etwaigen Verstoß gegen die Leitlinien zu berücksichtigen, da sie auslegungsrelevant sind und zeigen, wie der Information Commissioner die Datenschutzvorschriften in der Praxis ausgelegt und durchsetzt ([34]).

(19) Schließlich müssen die britischen Strafverfolgungsbehörden gemäß den Erwägungsgründen 8 bis 10 sicherstellen, dass die Bestimmungen der EMRK und des Übereinkommens Nr. 108 eingehalten werden.

(20) Somit ist der Rechtsrahmen für die Verarbeitung von Daten durch die britischen Strafverfolgungsbehörden seiner Struktur und seinen wesentlichen Bestandteilen nach dem in der EU geltenden Rechtsrahmen sehr ähnlich. Dazu gehört auch, dass dieser Rahmen nicht nur auf Verpflichtungen beruht, die im innerstaatlichen Recht festgelegt sind und durch EU-Recht geprägt wurden, sondern auch auf völkerrechtlichen Verpflichtungen, die das Vereinigte Königreich insbesondere durch seinen Beitritt zur EMRK und zum Übereinkommen Nr. 108 sowie durch die Anerkennung der Gerichtsbarkeit des Europäischen Gerichtshofs für Menschenrechte eingegangen ist. Diese sich aus rechtsverbindlichen internationalen Instrumenten ergebenden Verpflichtungen, die insbesondere den Schutz personenbezogener Daten betreffen, sind daher ein besonders wichtiges Element des Rechtsrahmens, der in diesem Beschluss bewertet wird.

2.3. **Sachlicher und räumlicher Anwendungsbereich**

(21) Der sachliche Anwendungsbereich von Teil 3 des DPA 2018 entspricht dem Anwendungsbereich der Richtlinie (EU) 2016/680 im Sinne ihres Artikels 2 Absatz 2. Teil 3 gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten durch eine zuständige Behörde sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten durch eine zuständige Behörde, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(22) Zudem fällt ein Verantwortlicher nur dann in den Anwendungsbereich dieses Teils 3, wenn es sich dabei um eine zuständige Behörde („competent authority") handelt und die Verarbeitung für Zwecke der Strafverfolgung („law enforcement purposes") erfolgt. Daher sind die Datenschutzvorschriften, die in diesem Beschluss bewertet werden, auf alle Strafverfolgungsaufgaben dieser zuständigen Behörden anwendbar.

(23) Als „zuständige Behörde" im Sinne der Begriffsbestimmung in Paragraf 30 DPA 2018 gelten die in Anhang 7 des DPA 2018 aufgeführten Personen sowie jede andere Person, soweit sie gesetzlich festgelegte Aufgaben für die Zwecke der Strafverfolgung ausübt. Die in Anhang 7 aufgeführten zuständigen Behörden umfassen nicht nur Polizeikräfte, sondern auch alle ministeriellen Regierungsbehörden im Vereinigten Königreich und andere Behörden mit Ermittlungsaufgaben (dazu gehören z. B. der Commissioner for Her Majesty's Revenue and Customs, die Welsh Revenue Authority, die Competition and Markets Authority und Her Majesty's Land Register), Staatsanwaltschaften,

---

([30]) In der Rechtssache R/Commission of Police of the Metropolis [2014], EWCA Civ 585, wurde der Rechtsstatus des MoPI Code of Practice bestätigt, und Lord Justice Laws erklärte, dass der Metropolitan Police Commissioner nach Paragraf 39A des Police Act 1996 verpflichtet ist, dem MoPI Code of Practice und der APP Guidance on Management of Police Information Rechnung zu tragen.

([31]) Die zuständige Aufsichtsbehörde Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) kontrolliert, ob die Polizei die Vorgaben des MoPI Code of Practice einhält.

([32]) Siehe diesbezüglich die Stellungnahme des College of Policing zur Einhaltung der APP Guidance in Bezug auf alle Aspekte der Polizeiarbeit, in der erklärt wird: „Die APP Guidance wurde vom Berufsverband der Polizei (dem College of Policing) als offizielle Quelle für die Ausübung des Polizeidienstes genehmigt. Es wird erwartet, dass Polizeibeamte und -personal der APP Guidance bei der Wahrnehmung ihrer Aufgaben Rechnung tragen. Unter bestimmten Umständen kann es jedoch in hinreichend begründeten Fällen gerechtfertigt sein, dass eine Dienststelle von der APP Guidance abweicht. Die Verantwortung für etwaige Risiken, die auf der lokalen oder nationalen Ebene durch Handlungen außerhalb der landesweit vereinbarten Leitlinien entstehen, trägt die Dienststelle; kommt es in der Folge zu einem Vorfall oder einer Untersuchung (zum Beispiel durch das Independent Office of Police Conduct), so haftet die Dienststelle für alle damit verbundenen Risiken." Die Stellungnahme ist abrufbar unter folgendem Link: https://www.app.college.police.uk/faq-page/

([33]) Guide to Law Enforcement Processing, abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

([34]) Siehe Rechtssache Bridges/Chief Constable of South Wales Police, [2019] EWHC 2341 (Admin), in der der High Court zwar darauf hinwies, dass die Leitlinien keinen Gesetzescharakter haben, jedoch feststellte: „Bei Prüfung der Frage, ob ein Verantwortlicher der Verpflichtung nach Paragraf 64 [d. h. der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung bei einer mit hohem Risiko behafteten Verarbeitung] nachgekommen ist, hat das Gericht die Leitlinien des Information Commissioner zu Datenschutz-Folgenabschätzungen zu berücksichtigen".

sonstige Strafjustizbehörden und andere mit Strafverfolgungsaufgaben betraute Träger oder Organisationen ([35]). Teil 3 des DPA 2018 gilt zudem für Gerichte und Tribunale im Rahmen der Ausübung ihrer richterlichen Funktionen, mit Ausnahme des Teils, der die Rechte der betroffenen Person und die Aufsichtsfunktion des ICO betrifft ([36]). Die in Anhang 7 enthaltene Liste der zuständigen Behörden ist nicht endgültig und kann vom Secretary of State im Wege von Verordnungen unter Berücksichtigung von Änderungen der behördlichen Organisationsstruktur aktualisiert werden ([37]).

(24) Die betreffende Verarbeitung muss also einem Zweck der Strafverfolgung („law enforcement purpose") dienen, der definiert wird als Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit ([38]). Die Verarbeitung durch eine zuständige Behörde wird nicht durch Teil 3 des DPA 2018 geregelt, wenn sie nicht für Zwecke der Strafverfolgung erfolgt. Dies ist zum Beispiel der Fall, wenn die Competition and Markets Authority nicht strafbare Sachverhalte untersucht (z. B. Unternehmenszusammenschlüsse). In diesem Fall kommt die UK GDPR in Verbindung mit Teil 2 des DPA 2018 zur Anwendung, weil die zuständigen Behörden personenbezogene Daten zu anderen Zwecken als zu Strafverfolgungszwecken verarbeiten. Um zu bestimmen, welche Datenschutzregelung (Teil 3 oder Teil 2 des DPA 2018) auf eine bestimmte Verarbeitung personenbezogener anwendbar ist, muss die zuständige Behörde, d. h. der Verantwortliche, prüfen, ob es sich beim Hauptzweck („primary purpose") der fraglichen Verarbeitung um einen der Strafverfolgungszwecke gemäß DPA 2018 handelt.

(25) In Bezug auf den räumlichen Anwendungsbereich von Teil 3 des DPA 2018 sieht Paragraf 207 Absatz 2 vor, dass der DPA für die Verarbeitung personenbezogener Daten im Zusammenhang mit den Tätigkeiten von Personen mit einer Niederlassung auf dem gesamten Gebiet des Vereinigten Königreichs gilt. Dazu gehören Behörden im Hoheitsgebiet von England, Wales, Schottland und Nordirland, die in den sachlichen Anwendungsbereich von Teil 3 des DPA 2018 fallen ([39]).

2.3.1. *Bestimmung der Begriffe „personenbezogene Daten" und „Verarbeitung"*

(26) Die Bestimmung der Schlüsselbegriffe „personenbezogene Daten" („personal data") und „Verarbeitung" („processing") findet sich in Paragraf 3 DPA 2018 und gilt im gesamten DPA. Die Begriffsbestimmungen sind eng an die entsprechenden Bestimmungen des Artikels 3 der Richtlinie (EU) 2016/680 angelehnt. Nach dem DPA 2018 gelten alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen, als personenbezogene Daten ([40]). Nach Paragraf 3 Absatz 3 DPA 2018 wird eine natürliche Person als identifizierbar angesehen, wenn sie direkt oder indirekt, unter anderem mittels Zuordnung zu einer Kennung wie einem Namen oder einer Kennnummer, oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann. Das Konzept der „Verarbeitung" wird definiert als ein im Zusammenhang mit Daten oder einer Datenreihe ausgeführter Vorgang oder eine solche Vorgangsreihe, wie a) das Erheben, das Erfassen, die Organisation, das Ordnen oder das Speichern, b) das Anpassen oder Verändern, c) das Auslesen, das Abfragen oder die Verwendung, d) die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, e) den Abgleich oder die Verknüpfung, oder f) die Einschränkung, das Löschen oder die Vernichtung. Des Weiteren wird im Gesetz der Ausdruck „Verarbeitung sensibler Daten" („sensitive processing") definiert als „a) die Verarbeitung personenbezogener Daten, aus denen die Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, b) die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, c) die Verarbeitung von Gesundheitsdaten, d) die Verarbeitung von Daten zur Sexualität oder der sexuellen Orientierung" ([41]). Diesbezüglich sind die Ausdrücke „biometrische Daten" („biometric data") ([42]), „Gesundheitsdaten" („data concerning health") ([43]) und „genetische Daten" („genetic data") ([44]) in Paragraf 205 DPA 2018 definiert.

([35]) Dazu gehören nach Anhang 7 des DPA 2018 die Directors of Public Prosecutors, der Director of Public Prosecutors for Northern Ireland und die Information Commission.

([36]) Paragraf 43 Absatz 3 DPA 2018.

([37]) Paragraf 30 Absatz 3 DPA 2018. Die Nachrichtendienste (Secret Intelligence Service, Security Service und die Government Communications Headquarters) gelten nicht als zuständige Behörden (siehe Paragraf 30 Absatz 2 DPA 2018), und Teil 3 des DPA 2018 findet auf deren Tätigkeiten keine Anwendung. Ihre Tätigkeiten fallen in den Anwendungsbereich von Teil 4 des DPA 2018.

([38]) Paragraf 31 DPA 2018.

([39]) Das bedeutet, dass der DPA 2018 und somit dieser Beschluss nicht auf die der britischen Krone unterstehenden Gebiete und die übrigen überseeischen Gebiete des Vereinigten Königreichs, zum Beispiel die Falklandinseln oder Gibraltar, anwendbar sind.

([40]) Personenbezogene Daten von Verstorbenen fallen nicht in den Anwendungsbereich des DPA 2018.

([41]) Paragraf 35 Absatz 8 DPA 2018.

([42]) Der Ausdruck „biometrische Daten" („biometric data") bezeichnet mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer Person, die die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

([43]) Der Begriff „Gesundheitsdaten" („data concerning health") bezeichnet personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

([44]) Der Ausdruck „genetische Daten" („genetic data") bezeichnet personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

(27) In Paragraf 32 DPA 2018 werden die Ausdrücke „Verantwortlicher" („controller") und „Auftragsverarbeiter" („processor") im Zusammenhang mit der Verarbeitung personenbezogener Daten für Zwecke der Strafverfolgung in enger Anlehnung an die entsprechenden Begriffsbestimmungen in der Richtlinie (EU) 2016/680 definiert. Der Ausdruck „Verantwortlicher" („controller") bezeichnet die zuständige Behörde, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Ist diese Verarbeitung gesetzlich vorgegeben, so ist der Verantwortliche die zuständige Behörde, der diese Verpflichtung durch das betreffende Gesetz auferlegt wird. Der Ausdruck „Auftragsverarbeiter" („processor") bezeichnet jede Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (soweit es sich dabei nicht um Beschäftigte des Verantwortlichen handelt).

2.4. **Garantien, Rechte und Pflichten**

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

(28) Nach Paragraf 35 DPA 2018 hat die Verarbeitung personenbezogener Daten — ähnlich wie in Artikel 4 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/680 festgelegt — auf rechtmäßige Weise und nach dem Grundsatz von Treu und Glauben zu erfolgen. Gemäß Paragraf 35 Absatz 2 DPA 2018 ist die Verarbeitung personenbezogener Daten für einen der Strafverfolgungszwecke nur dann rechtmäßig, wenn sie auf gesetzlicher Grundlage beruht und entweder die betroffene Person ihre Einwilligung für die Verarbeitung zu dem betreffenden Zweck erteilt hat oder die Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde für den betreffenden Zweck wahrgenommenen wird.

2.4.1.1. Verarbeitung auf Grundlage des Rechts

(29) Ähnlich wie in Artikel 8 der Richtlinie (EU) 2016/680 muss eine Verarbeitung nach Teil 3 des DPA 2018 zur Gewährleistung ihrer Rechtmäßigkeit auf „Grundlage des Rechts" erfolgen. Die Verarbeitung gilt als rechtmäßig („lawful"), wenn sie kraft Gesetzes, Common Law oder königlicher Vorrechte gestattet ist ([45]).

(30) Die Befugnisse zuständiger Behörden sind im Allgemeinen gesetzlich geregelt, das heißt, ihre Aufgaben und Befugnisse sind in vom Parlament verabschiedeten Rechtsvorschriften eindeutig festgelegt ([46]). In bestimmten Fällen können die Polizei und andere in Anhang 7 des DPA 2018 aufgeführte zuständige Behörden Daten auch auf Grundlage des Common Law verarbeiten ([47]). Das britische Common Law hat sich im Wege der Rechtsprechung entwickelt. Das Common Law ist im Zusammenhang mit Befugnissen der Polizei relevant, die ihre grundlegende Pflicht, die Öffentlichkeit durch die Aufdeckung und Verhütung von Straftaten zu schützen, aus dieser Rechtsquelle ableitet ([48]). Die polizeilichen Befugnisse zur Erfüllung dieser Pflicht sind jedoch sowohl im Common Law als auch

([45]) Erläuterungen zum DPA 2018, Nummer 181, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Die Befugnisse der National Crime Agency beispielsweise beruhen auf dem Straf- und Gerichtsgesetz (Crime and Courts Act) von 2013, das unter folgendem Link abrufbar ist: https://www.legislation.gov.uk/ukpga/2013/22/contents. Die Befugnisse der Food Standards Agency sind im Gesetz über Lebensmittelstandards (Food Standards Act) von 1999 festgelegt, das unter folgendem Link abrufbar ist: https://www.legislation.gov.uk/ukpga/1999/28/contents. Weitere Beispiele sind das Gesetz über die Strafverfolgung (Prosecution of Offenders Act) von 1985, mit dem der Crown Prosecution Services geschaffen wurde (siehe https://www.legislation.gov.uk/ukpga/1985/23/contents)), das Gesetz über die Steuer- und Zollbehörden (Commissioners for Revenue and Customs Act) von 2005, mit dem die Steuer- und Zollbehörde Her Majesty's Revenue and Customs eingerichtet wurde (siehe https://www.legislation.gov.uk/ukpga/2005/11/contents), das Strafverfahrensgesetz für Schottland (Criminal Procedure (Scotland) Act) von 1995, mit dem die Scottish Criminal Cases Review Commission geschaffen wurde (siehe https://www.legislation.gov.uk/ukpga/1995/46/contents)), das Justizgesetz für Nordirland (Justice (Northern Ireland) Act) von 2002, mit dem der Public Prosecution Service in Northern Ireland eingerichtet wurde (siehe https://www.legislation.gov.uk/ukpga/2002/26/contents), und das Strafjustizgesetz (Criminal Justice Act) von 1987, durch das das Serious Fraud Office geschaffen und mit Befugnissen ausgestattet wurde (siehe https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Den Angaben der britischen Behörden zufolge beruhen beispielsweise innerhalb des in Schottland für die Strafverfolgung zuständigen Crown Office and Procurator Fiscal Service die Befugnisse des Lord Advocate (die vorgesetzte Stelle des Strafverfolgungssystems in Schottland), Todesfälle zu untersuchen und Straftaten zu verfolgen, auf dem Common Law, während einige seiner Aufgaben gesetzlich geregelt sind. Darüber hinaus leiten die Krone und damit auch verschiedene Dienststellen und Ministerien ihre Befugnisse aus einer Kombination aus Gesetzen, Bestimmungen des Common Law und königlichen Vorrechten ab (königliche Vorrechte bzw. „royal prerogatives" sind der Krone nach dem Common Law verliehene Befugnisse, die jedoch von den Ministern ausgeübt werden).

([48]) Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, S. 8 (siehe Fußnote 9).

in Gesetzen ([49]) verankert. Gesetzliche Befugnisse der Polizei haben Vorrang vor etwaigen nach dem Common Law gewährten Befugnissen ([50]).

(31) Die aus dem Common Law abgeleiteten Befugnisse und Pflichten eines Polizeibeamten erstrecken sich nach Auffassung der Gerichte auf „alle Schritte, die ihm zur Aufrechterhaltung des Friedens, zur Verhinderung von Straftaten oder zum Schutz von Eigentum vor Schäden durch strafbare Handlungen notwendig erscheinen“ ([51]). Im Common Law verankerte Befugnisse gelten nicht uneingeschränkt. Sie unterliegen einer Reihe von Einschränkungen, die unter anderem durch die Gerichte ([52]) und durch Rechtsvorschriften — insbesondere durch den Human Rights Act 1998 und den Equality Act 2010 ([53]) — festgelegt wurden. Dazu gehört auch, dass zuständige Behörden bei der Verarbeitung von Daten gemäß Teil 3 des DPA 2018 ihre im Common Law verankerten Befugnisse stets im Einklang mit den Vorschriften des DPA 2018 ausüben. ([54]) Darüber hinaus ist bei der Entscheidung zur Durchführung jedweder Form der Datenverarbeitung grundsätzlich den Anforderungen der anwendbaren Leitlinien Rechnung zu tragen, wie etwa dem MoPI Code of Practice und den für die einzelnen Länder des Vereinigten Königreichs geltenden spezifischen Leitlinien ([55]). Durch verschiedene, von der Regierung und den Polizeidienststellen herausgegebene Leitliniendokumente soll sichergestellt werden, dass Polizeibeamte ihre Befugnisse innerhalb der durch das Common Law oder das einschlägige Gesetz vorgegebenen Grenzen ausüben ([56]).

(32) Eine weitere Komponente des „Rechts“ sind die königlichen Vorrechte („royal prerogatives“), d. h. bestimmte Befugnisse der Krone, die von der Exekutive ausgeübt werden können und nicht gesetzlich festgelegt sind, sondern sich aus der Souveränität des Monarchen ergeben ([57]). Es gibt nur sehr wenige Beispiele königlicher Vorrechte, die im Zusammenhang mit der Strafverfolgung relevant sind. Dazu gehört beispielsweise der Rechtsrahmen für die gegenseitige Amtshilfe, der die Weitergabe von Daten durch einen Secretary of State an Drittländer für Zwecke der

([49]) Die wichtigsten Rechtsvorschriften zur Regelung der wesentlichen polizeilichen Befugnisse (Festnahme, Durchsuchung, Genehmigung der fortdauernden Internierung, Abnahme von Fingerabdrücken, Probenahme im Rahmen körperlicher Untersuchungen, Anordnung von Abfangmaßnahmen, Zugang zu Kommunikationsdaten) sind: i) für England und Wales: das Gesetz über polizeiliche und strafrechtliche Beweismittel (Police and Criminal Evidence Act) von 1984 (im Folgenden „PACE 1984“), abrufbar unter https://www.legislation.gov.uk/ukpga/1984/60/contents (in der durch das Gesetz zum Schutz der Freiheiten (Protection of Freedoms Act — PoFA) von 2012 geänderten Fassung), abrufbar unter https://www.legislation.gov.uk/ukpga/2012/9/contents) und das Gesetz über Ermittlungsbefugnisse (Investigatory Powers Act — IPA) von 2016, abrufbar unter https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) für Schottland: das Strafjustizgesetz Schottlands (Criminal Justice (Scotland) Act) von 2016, abrufbar unter https://www.legislation.gov.uk/asp/2016/1/contents, und das Strafverfahrensgesetz Schottlands (Criminal Procedure (Scotland) Act) von 1995, abrufbar unter https://www.legislation.gov.uk/ukpga/1995/46/contents, iii) für Nordirland: die Verordnung Nordirlands über polizeiliche und strafrechtliche Beweismittel (Police and Criminal Evidence (Northern Ireland) Order) von 1989, abrufbar unter https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Den Erläuterungen der britischen Behörden zufolge ist der Vorrang des Gesetzesrechts im Vereinigten Königreich seit Langem anerkannt und geht bis auf das Urteil in der Rechtssache *Entick/Carrington*, [1765] EWHC KB J98, zurück, in dem anerkannt wurde, dass der Ausübung von Befugnissen durch die Exekutive Grenzen gesetzt sind, und der Grundsatz aufgestellt wurde, dass die aus dem Common Law abgeleiteten Befugnisse sowie die Vorrechte des Monarchen und der Regierung dem in Gesetzen konkretisierten Recht untergeordnet sind.

([51]) Siehe Rechtssache Rice/Connolly, [1966] 2 QB 414.

([52]) Siehe Rechtssache R(Catt)/Association of Chief police Officers, [2015] AC 1065, in der Lord Sumption im Zusammenhang mit der Befugnis der Polizei zur Einholung und Speicherung von Informationen über eine Person (die eine Straftat begangen hatte) feststellte, dass die Polizei nach dem Common Law Informationen für polizeiliche Zwecke, d. h. im weiteren Sinne zur Aufrechterhaltung der öffentlichen Ordnung und zur Verhütung und Aufdeckung von Straftaten, einholen und speichern darf. Dies umfasst nicht die Befugnis zur Anwendung von Eingriffsmaßnahmen zur Informationsbeschaffung, wie etwa das Betreten von Privateigentum oder als Übergriff einzustufende Handlungen (ausgenommen Festnahmen im Rahmen der nach Common Law verliehenen Befugnisse). Nach Auffassung des Gerichts waren die nach Common Law verliehenen Befugnisse in diesem Fall mehr als ausreichend, um die Einholung und Speicherung der in diesem Rechtsmittelverfahren betroffenen Art von öffentlichen Informationen zu genehmigen.

([53]) Equality Act 2010, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2010/15/contents

([54]) Ein Fall, in dem die nach Common Law verliehenen polizeilichen Befugnisse im Rahmen des DPA 1998 beurteilt wurden, ist das Urteil des High Court in der Rechtssache Bridges/The Chief Constable of South Wales Police (siehe Fußnote 33). Siehe auch die Rechtssachen Vidal-Hall/Google Inc, [2015] EWCA Civ 311, und Richard/BBC, [2018] EWHC 1837 (Ch).

([55]) Siehe zum Beispiel die Leitlinien des Police Service of Northern Ireland über Dienstanweisungen zur Dokumentenverwaltung, abrufbar unter folgendem Link: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf

([56]) Das Unterhaus hat ein Informationspapier herausgegeben, in dem die wichtigsten im Common Law verankerten und gesetzlichen Befugnisse der Polizei in England und Wales dargelegt sind (siehe https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Dem Informationspapier zufolge ergeben sich die Befugnisse zur Aufrechterhaltung des königlichen Friedens („Crown's peace“) und zur Gewaltanwendung („use of force“) aus dem Common Law, die Kontroll- und Durchsuchungsbefugnisse („stop and search powers“) hingegen aus dem Gesetz. Die schottische Regierung informiert zudem auf ihrer Website über die polizeilichen Befugnisse der Festnahme, Kontrolle und Durchsuchung (siehe https://www.gov.scot/policies/police/police-powers/).

([57]) Nach Auskunft der britischen Behörden umfassen die von der Regierung ausgeübten Vorrechte unter anderem die Verhandlung und Ratifizierung von Verträgen, die Ausübung der Diplomatie und der Einsatz der Streitkräfte innerhalb des Vereinigten Königreichs zwecks Unterstützung der Polizei bei der Wahrung des Friedens.

Strafverfolgung ermöglicht, wobei die Befugnis zu dieser Form der Datenweitergabe nicht immer gesetzlich geregelt ist ([58]). Da die königlichen Vorrechte an die Grundsätze des Common Law ([59]) gebunden und dem Gesetz untergeordnet sind, unterliegen sie den im Human Rights Act 1998 und im DPA 2018 vorgesehenen Grenzen ([60]).

(33) Um dem Grundsatz der Rechtmäßigkeit zu entsprechen, verlangt die britische Regelung analog zu Artikel 8 der Richtlinie (EU) 2016/680, dass die zuständigen Behörden bei der Verarbeitung auf Grundlage des Rechts sicherstellen, dass diese Verarbeitung auch für die Erfüllung der Aufgabe erforderlich („necessary") ist, die für den Zweck der Strafverfolgung wahrgenommen wird. In einer Konkretisierung dieses Aspekts hat das ICO klargestellt: „Es muss sich um ein zielgerichtetes und verhältnismäßiges Mittel zur Erfüllung des Zwecks handeln. Die rechtmäßige Grundlage gilt nicht, wenn der Zweck nach vernünftigem Ermessen auch durch weniger stark eingreifende Mittel erzielt werden kann. Das Argument, die Verarbeitung sei erforderlich, weil man sich intern für bestimmte Betriebsabläufe entschieden habe, ist unzureichend. Ausschlaggebend ist die Frage, ob die Verarbeitung für den angegebenen Zweck erforderlich ist" ([61]).

2.4.1.2. Verarbeitung auf der Grundlage der Einwilligung der betroffenen Person

(34) Wie in Erwägungsgrund 28 erwähnt, sieht Paragraf 35 Absatz 2 DPA 2018 vor, dass eine Verarbeitung personenbezogener Daten auf der Grundlage der Einwilligung („consent") der betroffenen Person zulässig ist.

(35) Allerdings ist die Einwilligung als Rechtsgrundlage für die in den Anwendungsbereich dieses Beschlusses fallenden Verarbeitungsvorgänge offenbar nicht relevant. Die unter diesen Beschluss fallenden Verarbeitungsvorgänge werden immer Daten betreffen, die nach der Richtlinie (EU) 2016/680 von einer zuständigen Behörde eines Mitgliedstaats an eine zuständige Behörde im Vereinigten Königreich übermittelt worden sind. Daher werden sie typischerweise nicht die Form der direkten Interaktion (Erhebung) zwischen einer Behörde und betroffenen Personen umfassen, die auf der Grundlage der Einwilligung nach Paragraf 35 Absatz 2 Buchstabe a DPA 2018 erfolgen kann.

(36) Auch wenn der Rückgriff auf die Einwilligung für die im Rahmen dieses Beschlusses vorgenommene Bewertung als nicht relevant betrachtet wird, sei der Vollständigkeit halber darauf hingewiesen, dass die Verarbeitung im Rahmen der Strafverfolgung nie allein auf der Einwilligung beruht, da eine zuständige Behörde unabhängig davon grundsätzlich zur Verarbeitung der Daten befugt sein muss ([62]). Konkret, und in Anlehnung an Richtlinie (EU) 2016/680 ([63]), bedeutet dies, dass die Einwilligung als zusätzliche Bedingung vorliegen muss, um bestimmte begrenzte und spezifische Verarbeitungsvorgänge zu ermöglichen, die andernfalls nicht durchgeführt werden könnten, wie etwa die Erhebung und Verarbeitung der DNA-Probe einer nicht verdächtigen Person. In diesem Fall würde die Verarbeitung nicht erfolgen, wenn die Einwilligung nicht erteilt wird oder wenn sie widerrufen wird ([64]).

([58]) Siehe diesbezüglich die in den Erwägungsgründen 74-87 vorgenommene Bewertung der britischen Regelung der Weiterübermittlung von Daten.

([59]) Siehe Rechtssache Bancoult/Secretary of State for Foreign and Commonwealth Affairs, [2008] UKHL 61, in der das Gericht entschied, dass das Vorrecht zum Erlass von Rechtsverordnungen („Orders in Council") auch den allgemeinen Klagegründen unterliegt.

([60]) Siehe Rechtssache Attorney-General/De Keyser's Royal Hotel Ltd, [1920] AC 508, in der das Gericht entschied, dass Vorrechte nicht anwendbar sind, wenn sie durch gesetzliche Befugnisse ersetzt werden; in der Rechtssache Laker Airways Ltd/Department of Trade, [1977] QB 643, stellte das Gericht fest, dass Vorrechte nicht zur Aufhebung von Gesetzesrecht herangezogen werden können; in der Rechtssache R/Secretary of State for the Home Department, ex p. Fire Brigades Union, [1995] UKHL 3, entschied das Gericht, dass Vorrechte nicht herangezogen werden können, wenn sie mit erlassenen Rechtsvorschriften in Konflikt stehen, und zwar selbst dann nicht, wenn die erlassenen Rechtsvorschriften noch nicht in Kraft sind; in der Rechtssache R (Miller)/Secretary of State for Exiting the European Union, [2017] UKSC 5, bestätigte das Gericht, dass Vorrechte durch Gesetzesrecht angepasst und abgeschafft werden können. Einen allgemeinen Überblick über die Beziehung zwischen den königlichen Vorrechten und gesetzlichen bzw. im Common Law verankerten Befugnissen vermittelt das Informationspapier des Unterhauses, abrufbar unter folgendem Link: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf

([61]) Guide to Law Enforcement Processing, „What is the first principle about?", abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2

([62]) Dies folgt aus dem Wortlaut der einschlägigen Bestimmung des DPA 2018, wonach die Verarbeitung personenbezogener Daten für einen der Strafverfolgungszwecke nur dann rechtmäßig ist, wenn und insoweit sie auf Grundlage des Rechts erfolgt („it is based on law") und entweder a) die betroffene Person ihre Einwilligung für die Verarbeitung zu dem betreffenden Zweck erteilt hat oder b) die Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde für den betreffenden Zweck wahrgenommen wird.

([63]) Siehe Erwägungsgründe 35 bis 37 der Verordnung (EU) 2016/680.

([64]) Nach Angaben der britischen Behörden wäre die Einwilligung als Grundlage für die Verarbeitung beispielsweise angemessen, wenn die Polizei im Zusammenhang mit einer vermissten Person eine DNA-Probe nimmt, um sie mit einer gegebenenfalls aufgefundenen Leiche abzugleichen. Unter solchen Umständen wäre es für die Polizei unangemessen, die betroffene Person zur Abgabe einer Probe zu zwingen; stattdessen würde sie die Person um ihre Einwilligung bitten, die freiwillig erteilt wird und jederzeit widerrufen werden kann. Wird die Einwilligung widerrufen, so dürften die Daten nicht länger verarbeitet werden, sofern nicht eine neue Rechtsgrundlage für die Fortsetzung der Verarbeitung der Probe festgestellt wird (wenn z. B. die betroffene Person unter Verdacht gerät). Ein weiteres Beispiel wäre der Fall, dass eine Polizeidienststelle eine Straftat untersucht, bei der sich die Weiterleitung des Opfers (eines Raubüberfalls, einer Sexualstraftat, von häuslicher Gewalt, als Angehörige/r eines Mordopfers oder Opfers einer anderen Straftat) an eine Opferhilfestelle empfiehlt (d. h. an eine unabhängige gemeinnützige Hilfsorganisation zur Unterstützung der Opfer von Straftaten und traumatischen Ereignissen). Unter solchen Umständen gibt die Polizei nur persönliche Informationen wie den Namen und die Kontaktdaten an die Opferhilfestelle weiter, sofern das Opfer eingewilligt hat.

(37) Wird die Einwilligung des Betroffenen verlangt, so muss diese unmissverständlich und durch eine eindeutige bestätigende Handlung erteilt worden sein ([65]). Die Polizeidienststellen müssen über eine Datenschutzerklärung verfügen, die unter anderem die notwendigen Angaben im Zusammenhang mit der wirksamen Nutzung der Einwilligung umfasst. Darüber hinaus veröffentlichen einige Polizeidienststellen zusätzliche Angaben darüber, wie sie den Datenschutzvorschriften nachkommen und wie und in welchen Fällen sie die Einwilligung als Rechtsgrundlage nutzen würden ([66]).

2.4.1.3. Verarbeitung sensibler Daten

(38) Wenn besondere Kategorien („special categories") von Daten verarbeitet werden, sollten besondere Garantien vorhanden sein. Diesbezüglich sieht Teil 3 des DPA 2018 in Anlehnung an Artikel 10 der Richtlinie (EU) 2016/680 für die Verarbeitung sensibler Daten („sensitive processing") strengere Garantien vor ([67]).

(39) Nach Paragraf 35 Absatz 3 DPA 1998 dürfen die zuständigen Behörden sensible Daten nur in zwei Fällen zu Strafverfolgungszwecken verarbeiten, nämlich 1. wenn die betroffene Person in die Verarbeitung für den Strafverfolgungszweck eingewilligt hat und der Verantwortliche zum Zeitpunkt der Durchführung der Verarbeitung über eine angemessene Dokumentation verfügt ([68]); oder 2. wenn die Verarbeitung für den Zweck der Strafverfolgung unbedingt erforderlich ist, die Verarbeitung mindestens eine der Voraussetzungen nach Anhang 8 des DPA 2018 erfüllt und der Verantwortliche zum Zeitpunkt der Durchführung der Verarbeitung über eine angemessene Dokumentation verfügt ([69]).

(40) In Bezug auf den ersten Fall wird, wie in Erwägungsgrund 38 dargelegt, die Einwilligung für die Art der Übermittlung, die Gegenstand dieses Beschlusses ist, als nicht relevant betrachtet ([70]).

(41) Beruht die Verarbeitung sensibler Daten nicht auf der Einwilligung, kann sie unter einer der in Anhang 8 des DPA 2018 genannten Bedingungen erfolgen. Diese Bedingungen beziehen sich auf die Notwendigkeit der Verarbeitung zu gesetzlichen Zwecken, zu Zwecken der Rechtspflege, zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person, zum Schutz von Kindern und gefährdeten Personen, im Zusammenhang mit Rechtsansprüchen, im Rahmen gerichtlicher Handlungen, zur Verhinderung von Betrug, Archivierung, und in

([65]) Es gibt keine eigenständige Definition des Begriffs „Einwilligung" („consent") für Zwecke der Verarbeitung personenbezogener Daten gemäß Teil 3 des DPA 2018. In seinen Leitlinien zum Begriff „consent" nach Teil 3 des DPA 2018 stellt das ICO klar, dass er dieselbe Bedeutung hat wie in der Datenschutz-Grundverordnung und an diese angeglichen werden sollte, insbesondere im Hinblick darauf, dass „die Einwilligung freiwillig, für den konkreten Fall und in informierter Weise bekundet wird und dass die betroffene Person eine echte Wahl hat, in die Verarbeitung der Daten einzuwilligen" (Guide to Law Enforcement Processing, „What is the first principle about?" (siehe Fußnote 64) und Guide to Data Protection zum Thema Einwilligung, abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Siehe zum Beispiel die Informationen auf der Website der Polizei von Lincolnshire (unter https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) oder auf der Website der Polizei von West Yorkshire (siehe https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Paragraf 35 Absatz 8 DPA 2018.

([68]) Paragraf 35 Absatz 4 DPA 2018.

([69]) Paragraf 35 Absatz 5 DPA 2018.

([70]) Der Vollständigkeit halber sei darauf hingewiesen, dass, wenn die Verarbeitung auf Grundlage der Einwilligung erfolgt, diese Einwilligung freiwillig, für den konkreten Fall und in informierter Weise bekundet werden muss und dass die betroffene Person ausdrücklich die Wahl haben muss, ob sie in die Verarbeitung der betreffenden Daten einwilligt. Außerdem muss der Verantwortliche bei einer Verarbeitung auf Grundlage der Einwilligung der betroffenen Person über eine angemessene Dokumentation („appropriate policy document" — im Folgenden „APD") verfügen. In Paragraf 42 DPA 2018 ist dargelegt, welche Kriterien das APD zu erfüllen hat. Danach muss in dem Dokument zumindest erläutert werden, mit welchen Verfahren der Verantwortliche die Einhaltung der Datenschutzgrundsätze sicherstellt und wie der Verantwortliche bei der Speicherung und Löschung personenbezogener Daten verfährt. Nach Paragraf 42 DPA 2018 bedeutet dies, dass der Verantwortliche ein Dokument vorlegen muss, in dem a) erläutert wird, mit welchen Verfahren der Verantwortliche die Einhaltung der Datenschutzgrundsätze gewährleistet, und b) erläutert wird, wie der Verantwortliche bei der Speicherung und Löschung personenbezogener Daten verfährt, die auf Grundlage der Einwilligung der betroffenen Person verarbeitet werden, oder angegeben wird, wie lange die betroffenen personenbezogenen Daten voraussichtlich gespeichert werden. Zu den Dokumentationserfordernissen gehört insbesondere, dass der Verantwortliche bei der Aufzeichnung seiner Verarbeitungstätigkeiten stets die unter den Buchstaben a und b genannten Elemente einbeziehen sollte. Das ICO hat eine Vorlage für die Dokumentation herausgegeben (Guide to Law Enforcement Processing, „Conditions for sensitive processing", abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) und kann Durchsetzungsmaßnahmen ergreifen, wenn die Verantwortlichen diesen Anforderungen nicht nachkommen. Die Dokumentation wird bei der Prüfung möglicher Verstöße gegen den DPA 2018 auch durch das Gericht in Augenschein genommen. So haben die Gerichte in der Rechtssache R (Bridges)/Chief Constable of South Wales Police das APD des Verantwortlichen überprüft und festgestellt, dass es zwar geeignet war, aber ausführlicher hätte sein können. Daraufhin hat die Polizei von South Wales das APD überprüft und mit den neuen Leitlinien des ICO in Einklang gebracht (siehe Fußnote 33). Des Weiteren sollte das APD nach Paragraf 42 Absatz 3 DPA 2018 regelmäßig vom Verantwortlichen überprüft werden. Schließlich ist der Verantwortliche als weitere Garantie nach Paragraf 42 Absatz 4 DPA 2018 verpflichtet, ein erweitertes Verzeichnis seiner Verarbeitungstätigkeiten zu führen, das verglichen mit der in Paragraf 61 DPA 2018 vorgesehenen allgemeinen Pflicht des Verantwortlichen zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten zusätzliche Elemente umfasst.

Fällen, in denen die betroffene Person die personenbezogenen Daten offenkundig öffentlich gemacht hat. Abgesehen von dem Fall, in dem die Daten offenkundig öffentlich gemacht wurden, unterliegen alle in Anhang 8 genannten Bedingungen einer strengen Notwendigkeitsprüfung („strict necessity"). Dazu hat das ICO Folgendes klargestellt: „Der Ausdruck ‚unbedingt notwendig' bedeutet in diesem Zusammenhang, dass sich die Verarbeitung auf eine dringende gesellschaftliche Notwendigkeit beziehen muss und nach vernünftigem Ermessen nicht durch weniger starke Eingriffe erzielt werden kann" ([71]). Darüber hinaus unterliegen einige der Bedingungen zusätzlichen Einschränkungen. So muss beispielsweise beim Rückgriff auf die Bedingung der Notwendigkeit zu gesetzlichen Zwecken („statutory purposes" — Anhang 8 Nummer 1) und zum Schutz von Kindern und gefährdeten Personen („safeguarding condition" — Anhang 8 Nummer 4) zusätzlich das Kriterium des erheblichen öffentlichen Interesses erfüllt sein. Darüber hinaus muss die betroffene Person im Zusammenhang mit den Bedingungen betreffend den Schutz des Kindes (Anhang 8 Nummer 4) auch einer bestimmten Altersgruppe angehören und als gefährdet gelten. Ferner kann der Verantwortliche die Bedingung nach Anhang 8 Nummer 4 nur heranziehen, wenn bestimmte Umstände gegeben sind ([72]). Die Bedingungen der Notwendigkeit für richterliche Handlungen („judicial acts" — Anhang 8 Nummer 7) und zur Verhinderung von Betrug („preventing fraud" — Anhang 8 Nummer 8) unterliegen ebenfalls Einschränkungen. Beide gelten nur für bestimmte Verantwortliche. Die Notwendigkeit für richterliche Handlungen können nur die Gerichte oder andere Justizbehörden geltend machen, und auf das Kriterium der Betrugsbekämpfung können sich nur Verantwortliche stützen, bei denen es sich um Betrugsbekämpfungsstellen handelt.

(42) Schließlich muss im Falle der Verarbeitung auf Grundlage einer der in Anhang 8 aufgeführten Bedingungen, beziehungsweise gemäß Paragraf 42 DPA 2018, eine angemessene Dokumentation („appropriate policy document") vorliegen, in der erläutert wird, mit welchen Verfahren der Verantwortliche die Einhaltung der Datenschutzgrundsätze sicherstellt und wie er bei der Speicherung und Löschung personenbezogener Daten verfährt, und es gilt die Pflicht zum Führen eines erweiterten Verzeichnisses.

2.4.2. *Zweckbindung*

(43) Personenbezogene Daten sollten für einen bestimmten Zweck verarbeitet und anschließend nur verwendet werden, soweit dies mit dem Zweck der Verarbeitung nicht unvereinbar ist. Dieser Datenschutzgrundsatz wird durch Paragraf 36 DPA 2018 garantiert. Diese Bestimmung verlangt ähnlich wie Artikel 4 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680, dass a) personenbezogene Daten in jedem Fall für festgelegte, eindeutige und rechtmäßige Strafverfolgungszwecke erhoben werden und dass b) die so erhobenen Daten nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden.

(44) Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden kann zu Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken erfolgen ([73]). Diesbezüglich wird im DPA 2018 außerdem klargestellt, dass die Archivierung (oder die Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken) nicht zulässig ist, wenn sie im Hinblick auf Entscheidungen erfolgt, die gegenüber einer bestimmten betroffenen Person ergangen sind, oder wenn die Verarbeitung voraussichtlich mit erheblichem Schaden oder Leid für diese Person verbunden wäre ([74]).

2.4.3. *Richtigkeit und Datenminimierung*

(45) Die Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Ferner müssen sie dem Verarbeitungszweck entsprechen und maßgeblich sein und dürfen für die Zwecke, zu denen sie verarbeitet werden, nicht übermäßig sein. Diese Grundsätze werden analog zu Artikel 4 Absatz 1 Buchstaben c, d und e der Richtlinie (EU) 2016/680 in den Paragrafen 37 und 38 DPA 2018 garantiert. Dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf den Zweck der Strafverfolgung, für den sie verarbeitet werden ([75]),

([71]) Guide to Law Enforcement Processing, „Conditions for sensitive processing" (siehe Fußnote 70).

([72]) Die Verarbeitung erfolgt ohne die Einwilligung der betroffenen Person, wenn a) die Einwilligung für die Verarbeitung von der betroffenen Person nicht erteilt werden kann, b) vom Verantwortlichen nach vernünftigem Ermessen nicht verlangt werden kann, die Einwilligung der betroffenen Person für die Verarbeitung einzuholen, c) die Verarbeitung ohne die Einwilligung der betroffenen Person erfolgen muss, weil die Einholung der Einwilligung der betroffenen Person die Schutzgewährung nach Unterabsatz 1 Buchstabe a beeinträchtigen würde.

([73]) Siehe Paragraf 41 Absatz 1 DPA 2018.

([74]) Siehe Paragraf 41 Absatz 2 DPA 2018.

([75]) In den UK Explanatory Framework for Adequacy Discussions heißt es: „Dadurch wird sowohl den Rechten der betroffenen Personen als auch den operativen Erfordernissen der Strafverfolgungsbehörden Rechnung getragen. Der vorstehende Punkt wurde im Rahmen der Ausarbeitung des Datenschutzgesetzes sorgfältig geprüft, da Daten unter Umständen aus spezifischen und begrenzten operativen Gründen nicht berichtigt werden können. Dies ist insbesondere dann der Fall, wenn die fraglichen unrichtigen personenbezogenen Daten zu Beweiszwecken in ihrer ursprünglichen Form erhalten bleiben müssen." (Siehe UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, S. 21, siehe Fußnote 9).

unrichtig ([76]) sind, unverzüglich ([77]) gelöscht oder berichtigt werden, und damit personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht für einen der Strafverfolgungszwecke übermittelt oder bereitgestellt werden ([78]).

(46) Darüber hinaus sieht die Datenschutzregelung des Vereinigten Königreichs ähnlich wie Artikel 7 der Richtlinie (EU) 2016/680 vor, dass bei personenbezogenen Daten so weit wie möglich zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten unterschieden wird ([79]). Gegebenenfalls muss so weit wie möglich klar zwischen den personenbezogenen Daten unterschieden werden, die sich auf verschiedene Kategorien betroffener Personen beziehen, wie Verdächtige, verurteilte Straftäter, Opfer von Straftaten und Zeugen ([80]).

2.4.4. *Speicherbegrenzung*

(47) Gemäß Artikel 5 der Richtlinie (EU) 2016/680 sollten Daten grundsätzlich nicht länger gespeichert werden, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Gemäß Paragraf 39 DPA 2018 und analog zu Artikel 5 der EU-Richtlinie dürfen personenbezogene Daten, die zu einem der Strafverfolgungszwecke verarbeitet werden, nicht länger gespeichert werden, als es für den Zweck, zu dem sie verarbeitet werden, erforderlich ist. Die Rechtsordnung des Vereinigten Königreichs verlangt, dass für die regelmäßige Überprüfung der Notwendigkeit einer weiteren Speicherung personenbezogener Daten zu einem der Strafverfolgungszwecke angemessene Fristen vorgesehen werden. Weitere Vorschriften über Verfahrensweisen bei der Speicherung personenbezogener Daten und die anwendbaren Fristen wurden in den einschlägigen Rechtsvorschriften und Leitlinien über die Befugnisse und Arbeitsweisen der Polizei festgelegt. So geben beispielsweise in England und Wales der MoPI Code of Practice des College of Policing in Verbindung mit der APP Guidance on the Management of Police Information einen Rahmen vor, um einheitliche und risikobasierte Speicher-, Überprüfungs- und Entsorgungsverfahren für die Verwaltung von Informationen bei der operativen Polizeiarbeit sicherzustellen ([81]). Dieser Rahmen umfasst klare Vorgaben für alle Dienststellen in Bezug auf die Erstellung, den Austausch, die Nutzung und die Verwaltung von Informationen zwischen einzelnen Polizeidienststellen und anderen Behörden ([82]). Es wird erwartet, dass die Polizei den MoPI Code of Practice befolgt, und die Einhaltung der Vorgaben wird vom Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) kontrolliert ([83]).

(48) Der Police Service of Northern Ireland (PSNI) ist gesetzlich nicht dazu verpflichtet, den MoPI Code of Practice zu befolgen. Allerdings wird der 2011 angenommene MoPI-Rahmen durch ein Handbuch des Police Service of Northern Ireland ([84]) ergänzt, in dem festgelegt ist, nach welchen Grundsätzen und Verfahren der MoPI Code of Practice in Nordirland anzuwenden ist.

([76]) In Paragraf 205 DPA 2018 wird der Begriff „unrichtig" („inaccurate") definiert als fehlerhafte oder irreführende („incorrect or misleading") personenbezogene Daten. Die Behörden des Vereinigten Königreichs erläuterten, dass im Zusammenhang mit strafrechtlichen Ermittlungen erhobene Daten typischerweise zwar oftmals unvollständig, aber dennoch richtig sein können.

([77]) Paragraf 38 Absatz 1 Buchstabe b DPA 2018.

([78]) Paragraf 38 Absatz 4 DPA 2018. Des Weiteren muss die Qualität personenbezogener Daten nach Paragraf 38 Absatz 5 DPA 2018 vor ihrer Übermittlung oder Bereitstellung überprüft werden; bei jeder Übermittlung personenbezogener Daten müssen die erforderlichen Informationen beigefügt werden, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der personenbezogenen Daten sowie deren Aktualitätsgrad zu beurteilen; wird festgestellt, dass unrichtige personenbezogene Daten übermittelt worden sind oder dass die personenbezogenen Daten unrechtmäßig übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen.

([79]) Paragraf 38 Absatz 2 DPA 2018.

([80]) Paragraf 38 Absatz 3 DPA 2018.

([81]) Dieser Rahmen gewährleistet ein einheitliches Vorgehen bei der Speicherung der erhobenen personenbezogenen Daten. Die Dauer des Überprüfungszeitraums richtet sich nach den Straftaten, die in vier Gruppen eingeteilt werden: 1) bestimmte Angelegenheiten des Schutzes der Öffentlichkeit, 2) andere Sexualstraftaten und schwere Straftaten, 3) alle weiteren Straftaten, 4) Sonstiges. Weitere Informationen sind der APP Guidance on the Management of Police Information zu entnehmen (siehe Fußnote 26).

([82]) Den Angaben der britischen Behörden zufolge können sich andere Einrichtungen freiwillig nach den Grundsätzen des MoPI Code of Practice richten; zum Beispiel haben im Interesse einheitlicher Vorgehensweisen bei der Strafverfolgung Her Majesty's Revenue and Customs und die National Crime Agency viele Grundsätze aus dem MoPI Code of Practice übernommen. Im Allgemeinen stellen die meisten Einrichtungen ihrem Personal spezielle auf die betreffende Einrichtung zugeschnittene Richtlinien und Anweisungen für den Umgang mit personenbezogenen Daten bei der Wahrnehmung ihrer Aufgaben zur Verfügung. Dazu gehören zumeist auch obligatorische Schulungsmaßnahmen.

([83]) Der MoPI Code of Practice wurde im Rahmen der im Police Act 1996 verliehenen Befugnisse herausgegeben, wonach das College of Policing Verhaltenskodizes zur Förderung einer wirksamen Polizeiarbeit erstellen kann. Jeder nach dem Police Act erstellte Verhaltenskodex muss vom Secretary of State genehmigt werden; außerdem muss die National Crime Agency dazu konsultiert werden, bevor er dem Parlament vorgelegt wird. Gemäß Paragraf 39A Absatz 7 des Police Act 1996 ist die Polizei verpflichtet, nach diesem Gesetz erlassene Kodizes gebührend zu berücksichtigen.

([84]) PSNI MoPI Handbook, Kapitel 1 bis 6.

(49) In Schottland stützen sich die Polizeidienststellen auf eine Standard-Dienstanweisung zur Datenspeicherung, die sogenannte Retention Standard Operating Procedure (SOP) ([85]), die die Datenverwaltungsrichtlinie (Records Management Policy) ([86]) des Police Service of Scotland ergänzt. Die Standard Operating Procedure sieht spezielle Speicherregeln für von der schottischen Polizei verwahrte Daten vor.

(50) Neben der im gesamten Vereinigten Königreich geltenden übergeordneten Vorschrift, gespeicherte Daten regelmäßig zu überprüfen, sind in lokalen Vorschriften weitere Einzelheiten geregelt. Dazu einige Beispiele: In Bezug auf England und Wales regelt das Gesetz über polizeiliche und strafrechtliche Beweismittel (Police and Criminal Evidence Act) in der durch das Gesetz zum Schutz der Freiheiten (Protection of Freedom Act) von 2012 geänderten Fassung die Speicherung von Fingerabdrücken und DNA-Profilen und enthält eine besondere Regelung für nicht verurteilte Personen ([87]). Mit dem Protection of Freedom Act wurde zudem das Amt des Beauftragten für die Aufbewahrung und Verwendung von biometrischem Material (Commissioner for the Retention and Use of Biometric Material — im Folgenden „Biometrics Commissioner") geschaffen ([88]). Im Custody Image Review von 2017 sind besondere Vorschriften für bei der Festnahme aufgenommene Fotos festgelegt ([89]). Für Schottland sind die Vorschriften über die Einholung und Aufbewahrung von Fingerabdrücken und biologischen Proben im Strafverfahrensgesetz (Criminal Procedure (Scotland) Act) von 1995 festgelegt ([90]). Wie in England und Wales ist die Aufbewahrung von biometrischen Daten in verschiedenen Fällen gesetzlich geregelt ([91]).

2.4.5. *Datensicherheit*

(51) Personenbezogene Daten müssen in einer Weise verarbeitet werden, die ihre Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Zu diesem Zweck müssen die Behörden geeignete technische oder organisatorische Maßnahmen treffen, um personenbezogene Daten vor möglichen Bedrohungen zu schützen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik und der damit verbundenen Kosten bewertet werden.

(52) Diese Grundsätze schlagen sich in Paragraf 40 DPA 2018 nieder, wonach — ähnlich wie in Artikel 4 Absatz 1 Buchstabe f der Richtlinie (EU) 2016/680 — die Verarbeitung personenbezogener Daten für einen der Strafverfolgungszwecke in einer Weise erfolgen muss, die eine angemessene Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen gewährleistet. Dies umfasst den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter

([85]) Record Retention Standard Operating Procedure (SOP), abrufbar unter folgendem Link: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf

([86]) Weitere Informationen über die Datenverwaltung sind den Informationen über die National Records of Scotland zu entnehmen, abrufbar unter folgendem Link: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Die Aufbewahrungsfristen richten sich danach, ob eine Person verurteilt worden ist oder nicht (Paragrafen 63I bis 63KI PACE 1984). Zum Beispiel dürfen Fingerabdrücke und DNA-Proben eines Erwachsenen, der wegen einer meldepflichtigen Straftat verurteilt worden ist, unbegrenzt aufbewahrt werden (Paragraf 63I Absatz 2 PACE 1984), während die Aufbewahrung befristet ist, wenn der/die Verurteilte jünger als 18 Jahre ist, es sich um eine geringfügige („minor") meldepflichtige Straftat handelt und die Person zuvor noch nicht verurteilt wurde (Paragraf 63K PACE 1984). Bei festgenommenen oder angeklagten, aber nicht verurteilten Personen ist die Aufbewahrungsfrist auf drei Jahre begrenzt (Paragraf 63F PACE 1984). Die Verlängerung dieser Aufbewahrungsfrist muss von einer Justizbehörde genehmigt werden (Paragraf 63F Absatz 7 PACE 1984). Bei Personen, die wegen geringfügiger Straftaten festgenommen oder angeklagt, aber nicht verurteilt wurden, ist keine Aufbewahrung möglich (Paragraf 63D und Paragraf 63H PACE 1984).

([88]) Durch Paragraf 20 des Protection of Freedom Act 2012 wurde das Amt des Biometrics Commissioner geschaffen. Zu seinen Aufgaben gehört es unter anderem, zu entscheiden, ob die Polizei Daten zu DNA-Profilen und Fingerabdrücken von Personen speichern darf, die wegen einer einschlägigen Straftat festgenommenen aber nicht angeklagt worden sind (Paragraf 63G PACE 1984). Außerdem obliegt dem Biometrics Commissioner die allgemeine Zuständigkeit für die Überprüfung der Speicherung und Verwendung von DNA und Fingerabdrücken sowie der Speicherung aus Gründen der nationalen Sicherheit (Paragraf 20 Absatz 2 des Protection of Freedom Act 2012). Der Biometric Commissioner wird gemäß dem Kodex über die Besetzung öffentlicher Ämter (Code for Public Appointments) ernannt (unter folgendem Link abrufbar: Governance Code for Public Appointments - GOV.UK (www.gov.uk)) und aus den Bedingungen seiner Ernennung geht klar hervor, dass er nur vom Innenminister und unter bestimmten, eng gefassten Umständen seines Amtes enthoben werden darf, u. a. wenn er länger als drei Monate seinen amtlichen Pflichten nicht nachkommt, für eine Straftat verurteilt wird oder gegen die Bedingungen verstößt, denen seine Ernennung unterliegt.

([89]) Review of the Use and Retention of Custody Images, abrufbar unter folgendem Link: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

([90]) Paragraf 18 ff. des Criminal Procedure (Scotland) Act 1995.

([91]) Die Speicherfristen variieren je nachdem, ob eine Person verurteilt worden ist (Paragraf 18 Absatz 3 des Criminal Procedure (Scotland) Act 1995) oder ob sie minderjährig ist. Im Falle von Minderjährigen beträgt die Speicherfrist 3 Jahre ab dem Zeitpunkt der Verurteilung bei der Anhörung des Kindes (Paragraf 18E Absatz 8 des Criminal Procedure (Scotland) Act 1995). Daten festgenommenen aber nicht verurteilten Personen dürfen nicht gespeichert werden (Paragraf 18 Absatz 3 des Criminal Procedure (Scotland) Act 1995), ausgenommen in bestimmten Fällen und je nach Schwere der Straftat (Paragraf 18A des Criminal Procedure (Scotland) Act 1995). Mit dem Scottish Biometrics Commissioner Act 2020 (siehe https://www.legislation.gov.uk/asp/2020/8/contents) wurde das Amt des Schottischen Biometrics Commissioner geschaffen, der (vom schottischen Parlament zu genehmigende) Verhaltenskodizes betreffend die Erfassung, Speicherung, Verwendung und Löschung biometrischer Daten zu strafrechtlichen und polizeilichen Zwecken ausarbeitet und überprüft (Paragraf 7 des Scottish Biometrics Commissioner Act 2020).

Schädigung ([92]). Ferner ist in Paragraf 66 DPA 2018 festgelegt, dass jeder Verantwortliche und jeder Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen hat, um ein Schutzniveau zu gewährleisten, das den mit der Verarbeitung personenbezogener Daten verbundenen Risiken angemessen ist. Den Erläuterungen zufolge muss der Verantwortliche die Risiken ermitteln und auf der Grundlage dieser Risikobewertung angemessene Sicherheitsvorkehrungen treffen, wie etwa eine Verschlüsselung oder spezielle Sicherheitsfreigaben für das mit der Datenverarbeitung befasste Personal ([93]). Bei der Bewertung sind unter anderem auch die Art der verarbeiteten Daten sowie alle sonstigen relevanten Faktoren oder Umstände zu berücksichtigen, die sich auf die Sicherheit der Verarbeitung auswirken könnten.

(53) Die Regelungen zur Einhaltung der Datensicherheitsgrundsätze sind den entsprechenden Bestimmungen der Artikel 29 bis 31 der Richtlinie (EU) 2016/680 sehr ähnlich. Insbesondere muss der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten, für die der Verarbeiter verantwortlich ist, diese nach Paragraf 67 Absatz 1 DPA 2018 unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, dem Information Commissioner melden ([94]). Die Meldepflicht gilt nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt ([95]). Der Verantwortliche muss die im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen so dokumentieren, dass der Information Commissioner die Einhaltung der Bestimmungen des DPA überprüfen kann ([96]). Wenn einem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, hat er diese dem Verantwortlichen unverzüglich zu melden ([97]).

(54) Nach Paragraf 68 Absatz 1 DPA 2018 muss der Verantwortliche die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten unterrichten, wenn die betreffende Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat ([98]). Die Mitteilung muss dieselben Angaben enthalten wie die in Erwägungsgrund 53 beschriebene Meldung an den Information Commissioner. Diese Meldepflicht gilt nicht, wenn der Verantwortliche angemessene technische und organisatorische Maßnahmen ergriffen hat und diese Maßnahmen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt hat. Sie entfällt auch dann, wenn der Verantwortliche durch Folgemaßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht. Schließlich ist der Verantwortliche auch dann nicht zur Unterrichtung der betroffenen Person verpflichtet, wenn dies mit einem unverhältnismäßigen Aufwand verbunden wäre ([99]). In diesem Fall muss die betroffene Person auf eine andere vergleichbar wirksame Weise informiert werden, beispielsweise mittels öffentlicher Bekanntmachung ([100]). Hat der Verantwortliche die betroffene Person nicht von der Verletzung des Schutzes personenbezogener Daten unterrichtet, so kann der Information Commissioner — nach Erhalt der Meldung der Verletzung gemäß Paragraf 67 — unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, die betroffene Person von der Verletzung zu unterrichten ([101]).

([92]) Gemäß den Erläuterungen zum DPA 2018 (siehe Fußnote 45) müssen Verantwortliche insbesondere die Sicherheit der Daten in einer der Art der von ihnen gespeicherten personenbezogenen Daten und dem aus Sicherheitslücken potenziell erwachsenden Schaden angemessenen Weise gestalten und organisieren; klar regeln, wer in ihrer Organisation für die Gewährleistung der Informationssicherheit verantwortlich ist; sicherstellen, dass eine geeignete physische und technische Sicherheitsstruktur vorhanden ist, die durch solide Richtlinien und Verfahren sowie durch zuverlässiges, gut geschultes Personal gestützt wird; in der Lage sein, zügig und wirksam auf etwaige Verletzungen der Sicherheit zu reagieren.

([93]) Nummer 221 der Erläuterungen zum DPA 2018 (siehe Fußnote 45).

([94]) Nach Paragraf 67 Absatz 4 DPA 2018 muss die Meldung eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (soweit möglich mit Angabe der Kategorien und ungefähren Zahl betroffener Personen, der betroffenen Kategorien personenbezogener Daten und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), den Namen und die Kontaktdaten einer Anlaufstelle, eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten (und gegebenenfalls der Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen dieser Verletzung) umfassen.

([95]) Paragraf 67 Absatz 2 DPA 2018.

([96]) Paragraf 67 Absatz 6 DPA 2018.

([97]) Paragraf 67 Absatz 9 DPA 2018.

([98]) Nach Paragraf 68 Absatz 7 DPA 2018 kann der Verantwortliche die Unterrichtung der betroffenen Person ganz oder teilweise in dem Umfang und so lange einschränken, wie dies unter Berücksichtigung der Grundrechte und der berechtigten Interessen der betroffenen Person eine erforderliche und verhältnismäßige Maßnahme darstellt, um a) behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, c) zum Schutz der öffentlichen Sicherheit, d) zum Schutz der nationalen Sicherheit, e) zum Schutz der Rechte und Freiheiten anderer.

([99]) Paragraf 68 Absatz 3 DPA 2018.

([100]) Paragraf 68 Absatz 5 DPA 2018.

([101]) Paragraf 68 Absatz 6 DPA 2018, vorbehaltlich der Einschränkung gemäß Paragraf 68 Absatz 8 DPA 2018.

2.4.6. *Transparenz*

(55) Betroffene Personen müssen über die Hauptmerkmale der Verarbeitung ihrer personenbezogenen Daten unterrichtet werden. Dieser Datenschutzgrundsatz schlägt sich in Paragraf 44 DPA 2018 nieder, der — ähnlich wie Artikel 13 der Richtlinie (EU) 2016/680 — besagt, dass der Verantwortliche eine allgemeine Pflicht hat, betroffenen Personen Informationen über die Verarbeitung ihrer personenbezogenen Daten zur Verfügung zu stellen (indem die Informationen der Öffentlichkeit allgemein zugänglich gemacht oder auf andere Weise zur Verfügung gestellt werden) ([102]). Betroffenen Personen sind insbesondere folgende Informationen zur Verfügung zu stellen: a) der Name und die Kontaktdaten des Verantwortlichen, b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten, c) die Zwecke, für die der Verantwortliche die personenbezogenen Daten verarbeitet, d) das Recht auf Auskunft über personenbezogene Daten, auf Berichtigung oder Löschung personenbezogener Daten oder auf Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person durch den Verantwortlichen, und e) das Bestehen eines Beschwerderechts beim Information Commissioner sowie dessen Kontaktdaten ([103]).

(56) Der Verantwortliche muss die betroffene Person außerdem in bestimmten Fällen (etwa wenn die verarbeiteten personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden) und zur Ermöglichung der Ausübung ihrer Rechte nach dem DPA 2018 über Folgendes informieren: die Rechtsgrundlage der Verarbeitung, b) die Speicherfrist der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien, nach denen die Speicherfrist festgelegt wird, c) gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten (einschließlich Empfänger in Drittländern oder internationalen Organisationen), d) alle sonstigen Informationen, die notwendig sind, um die Ausübung der Rechte der betroffenen Person gemäß Teil 3 DPA 2018 zu ermöglichen ([104]).

2.4.7. *Rechte des Einzelnen*

(57) Den betroffenen Personen muss eine Reihe von durchsetzbaren Rechten eingeräumt werden. Teil 3 Kapitel 3 des DPA 2018 gewährt natürlichen Personen das Recht auf Auskunft und Berichtigung oder Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung ([105]). Diese Rechte sind mit den nach Kapitel 3 der Richtlinie (EU) 2016/680 gewährten Rechten vergleichbar.

(58) Das Auskunftsrecht ist in Paragraf 45 DPA 2018 geregelt. Erstens haben natürliche Personen das Recht, vom Verantwortlichen eine Bestätigung darüber zu erhalten, ob ihre personenbezogenen Daten verarbeitet werden oder nicht ([106]). Zweitens hat in dem Fall, dass personenbezogene Daten verarbeitet werden, die betroffene Person das Recht, Auskunft über die betreffenden Daten und zu folgenden Punkten zu erhalten: a) die Zwecke der Verarbeitung und deren Rechtsgrundlagen, b) die Datenkategorien, die verarbeitet werden, c) die Empfänger, gegenüber denen die personenbezogenen Daten offengelegt worden sind, d) die Dauer der Speicherung personenbezogener Daten; e) das Bestehen eines Rechts der betroffenen Person auf Berichtigung und Löschung personenbezogener Daten, f) das Bestehen eines Beschwerderechts sowie g) alle Informationen über die Herkunft der verarbeiteten personenbezogenen Daten ([107]).

(59) Nach Paragraf 46 DPA 2018 hat die betroffene Person das Recht, vom Verantwortlichen die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Der Verantwortliche muss die Daten unverzüglich berichtigen (bzw. vervollständigen, wenn die Daten wegen Unvollständigkeit unrichtig sind). Müssen die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden, so hat der Verantwortliche ihre Verarbeitung einzuschränken (anstatt die personenbezogenen Daten zu berichtigen) ([108]).

([102]) Im Leitfaden „Guide to Law Enforcement Processing" wird folgendes Beispiel genannt: „Sie verfügen über eine allgemeine Datenschutzerklärung auf Ihrer Website, die grundlegende Informationen über die Organisation, den Zweck der Datenverarbeitung, die Rechte der betroffenen Personen und deren Beschwerderecht beim Information Commissioner umfasst. Sie haben erfahren, dass eine Person zugegen war, als eine Straftat begangen wurde. Bei der ersten Befragung dieser Person müssen Sie ihr die allgemeinen Informationen ebenso wie die Zusatzinformationen mitteilen, damit die Person ihre Rechte ausüben kann. Sie dürfen die Aufklärung der Person über die Verarbeitung nach dem Grundsatz von Treu und Glauben nur dann einschränken, wenn dies Ihre Untersuchung beeinträchtigen würde (Guide to Law Enforcement Processing, „What information should we supply to an individual?", abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Im Leitfaden „Guide to Law Enforcement Processing" wird erklärt, dass die Informationen über die Verarbeitung personenbezogener Daten in präziser, verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache, die auch an die Bedürfnisse schutzbedürftiger Personen, z. B. Kinder, angepasst ist, und gebührenfrei zu übermitteln sind (Guide to Law Enforcement Processing, „How should we provide this information?", abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Paragraf 44 Absatz 2 DPA 2018.

([105]) Eine ausführliche Analyse der Rechte der betroffenen Personen bietet der Leitfaden „Guide to Law Enforcement Processing on individual rights", abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) Paragraf 45 Absatz 1 DPA 2018.

([107]) Paragraf 45 Absatz 2 DPA 2018.

([108]) Paragraf 46 Absatz 4 DPA 2018.

(60) Paragraf 47 DPA 2018 gewährt natürlichen Personen ein Recht auf Löschung und auf Einschränkung der Verarbeitung. Der Verantwortliche muss ([109]) personenbezogene Daten unverzüglich löschen, wenn die Verarbeitung der personenbezogenen Daten gegen einen der Datenschutzgrundsätze, gegen die Rechtsgrundlagen der Verarbeitung oder gegen die im Zusammenhang mit der Archivierung und der Verarbeitung sensibler Daten bestehenden Garantien verstoßen würde. Außerdem muss der Verantwortliche die Daten löschen, wenn er rechtlich dazu verpflichtet ist. Müssen die personenbezogenen Daten zu Beweiszwecken weiter aufbewahrt werden, so muss der Verantwortliche ihre Verarbeitung einschränken (anstatt die personenbezogenen Daten zu löschen) ([110]). Der Verantwortliche muss die Verarbeitung personenbezogener Daten einschränken, wenn eine betroffene Person die Richtigkeit personenbezogener Daten bestreitet, deren Richtigkeit oder Unrichtigkeit jedoch nicht festgestellt werden kann ([111]).

(61) Beantragt eine betroffene Person die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung ihrer Verarbeitung, so hat der Verantwortliche der betroffenen Person schriftlich mitzuteilen, ob dem Antrag Folge geleistet wurde; wird der Antrag abgelehnt, muss der Verantwortliche die betroffene Person über die entsprechenden Gründe und über die Rechtsbehelfsmöglichkeiten informieren (das Recht der betroffenen Person, beim Information Commissioner die Prüfung der rechtmäßigen Anwendung der Einschränkung zu beantragen, das Recht auf Beschwerde beim Information Commissioner und das Recht, bei Gericht eine Verfügung zu beantragen) ([112]).

(62) Berichtigt der Verantwortliche von einer anderen Behörde erhaltene personenbezogene Daten, so hat er die andere Behörde hierüber zu unterrichten ([113]). Berichtigt oder löscht der Verantwortliche personenbezogene Daten, die er offengelegt hat, oder schränkt er die Verarbeitung solcher Daten ein, muss der Verantwortliche die Empfänger benachrichtigen, und die Empfänger müssen die personenbezogenen Daten ihrerseits berichtigen, löschen bzw. deren Verarbeitung einschränken (soweit sie weiterhin für die Daten verantwortlich sind) ([114]).

(63) Darüber hinaus hat die betroffene Person das Recht, unverzüglich vom Verantwortlichen über eine Verletzung des Schutzes personenbezogener Daten informiert zu werden, wenn diese voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat ([115]).

(64) In Bezug auf alle genannten Rechte der betroffenen Person und analog zu den Bestimmungen des Artikels 12 der Richtlinie (EU) 2016/680 hat der Verantwortliche sicherzustellen, dass der betroffenen Person alle Informationen in präziser, verständlicher und leicht zugänglicher Form ([116]) und, soweit möglich, in derselben Form übermittelt werden, in der der Antrag gestellt wurde ([117]). Der Verantwortliche muss dem Antrag der betroffenen Person unverzüglich und in jedem Fall grundsätzlich spätestens binnen eines Monats nach Erhalt des Antrags nachkommen ([118]). Hat der Verantwortliche begründete Zweifel an der Identität einer natürlichen Person, so kann er zusätzliche Informationen anfordern und die Bearbeitung des Antrages zurückstellen, bis die Identität festgestellt ist. Der Verantwortliche kann eine angemessene Gebühr erheben oder sich weigern, den Antrag zu bearbeiten, wenn der Antrag offenkundig unbegründet ist ([119]). Das ICO hat Leitlinien herausgegeben, in denen dargelegt ist, wann ein Antrag offenkundig unbegründet oder exzessiv ist und wann eine Gebühr erhoben werden kann ([120]).

(65) Darüber hinaus kann der Secretary of State nach Paragraf 53 Absatz 4 DPA 2018 im Wege von Verordnungen einen Höchstbetrag für die Gebühr bestimmen.

([109]) Eine betroffene Person kann den Verantwortlichen auffordern, personenbezogene Daten zu löschen oder deren Verarbeitung einzuschränken (wobei der Verantwortliche unabhängig davon, ob ein solcher Antrag gestellt wird, zur Löschung der Daten bzw. zur Einschränkung ihrer Verarbeitung verpflichtet ist).

([110]) Paragraf 46 Absatz 4 und Paragraf 47 Absatz 2 DPA 2018.

([111]) Paragraf 47 Absatz 3 DPA 2018.

([112]) Paragraf 48 Absatz 1 DPA 2018.

([113]) Paragraf 48 Absatz 7 DPA 2018.

([114]) Paragraf 48 Absatz 9 DPA 2018.

([115]) Paragraf 68 DPA 2018.

([116]) Paragraf 52 Absatz 1 DPA 2018.

([117]) Paragraf 52 Absatz 3 DPA 2018.

([118]) Nach Paragraf 54 DPA 2018 gilt als anwendbarer Zeitraum („applicable time period") ein Zeitraum von einem Monat oder ein — mittels Vorschriften zu bestimmender — längerer Zeitraum, beginnend ab dem einschlägigen Zeitpunkt (d. h. Eingang des fraglichen Antrags beim Verantwortlichen, Eingang der (gegebenenfalls) in Verbindung mit einem Antrag nach Paragraf 52 Absatz 4 DPA angeforderten Informationen beim Verantwortlichen, oder der Zeitpunkt, zu dem (gegebenenfalls) die in Verbindung mit dem Antrag nach Paragraf 53 DPA 2018 erhobene Gebühr entrichtet wurde).

([119]) Paragraf 53 Absatz 1 DPA 2018.

([120]) Laut den Leitlinien des ICO kann ein Verantwortlicher beschließen, eine Gebühr von einer betroffenen Person bei offenkundig unbegründeten oder exzessiven Anträgen erheben, wenn der Verantwortliche dennoch darauf antworten möchte. Die Höhe der Gebühr muss angemessen sein und die Kosten rechtfertigen. Guide to Law Enforcement Processing, „Manifestly unfounded and excessive requests", abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/

2.4.7.1. Einschränkung der Rechte der betroffenen Person und Transparenzpflichten

(66) Eine zuständige Behörde kann unter bestimmten Umständen bestimmte Rechte der betroffenen Person einschränken: das Auskunftsrecht ([121]), das Recht auf Erhalt von Informationen ([122]), das Recht auf Benachrichtigung von einer Verletzung des Schutzes personenbezogener Daten ([123]) und das Recht auf Auskunft über die Gründe für die Ablehnung eines Antrags auf Berichtigung oder Löschung ([124]). Ähnlich der in Kapitel III der Richtlinie (EU) 2016/680 vorgesehenen Regelung darf eine zuständige Behörde die Einschränkung nur dann anwenden, wenn sie unter Berücksichtigung der Grundrechte und der berechtigten Interessen der betroffenen Person erforderlich und verhältnismäßig ist, um a) behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, c) zum Schutz der öffentlichen Sicherheit, d) zum Schutz der nationalen Sicherheit, e) zum Schutz der Rechte und Freiheiten anderer.

(67) Das ICO hat Leitlinien zur Anwendung dieser Einschränkungen herausgegeben. Diesen Leitlinien zufolge müssen Verantwortliche im Rahmen einer Einzelfallprüfung die Rechte der betroffenen Person gegen den bei einer Offenlegung zu erwartenden Schaden abwägen. Sie müssen insbesondere in jedem Fall begründen, dass eine Einschränkung notwendig und verhältnismäßig ist, und dürfen die bereitzustellenden Informationen nur einschränken, wenn deren Offenlegung die vorstehend genannten Zwecke beeinträchtigen würde ([125]).

(68) Darüber hinaus haben die zuständigen Behörden eine Reihe weiterer Leitlinien mit detaillierten Informationen zu allen Aspekten der Datenschutzgesetzgebung erstellt, auch zur Anwendung von Einschränkungen der Rechte der betroffenen Personen ([126]). So wird beispielsweise im Datenschutzhandbuch (Data Protection Manual) des National Police Chief Council im Zusammenhang mit Paragraf 45 Absatz 4 erklärt: „Es wird ausdrücklich darauf hingewiesen, dass die Einschränkungen nur so weit wie nötig angewandt und nur so lange wie nötig angewandt werden dürfen. Folglich sind eine pauschale Anwendung der Einschränkung auf alle personenbezogenen Daten eines Antragstellers oder eine dauerhafte Anwendung der Einschränkung unzulässig. In Bezug auf den letztgenannten Punkt müssen im Rahmen eines Ermittlungsverfahrens ohne Wissen der betroffenen Person erhobene personenbezogene Daten einer/eines Verdächtigen oftmals vor der Offenlegung gegenüber dieser Person geschützt werden, um laufende Ermittlungen nicht zu beeinträchtigen; zu einem späten Zeitpunkt hingegen würde die Offenlegung keinen Schaden verursachen, wenn die personenbezogenen Daten der betroffenen Person während der Vernehmung offengelegt worden wären. Die Polizeikräfte müssen Verfahren vorsehen, die sicherstellen, dass diese Einschränkungen nur im notwendigen Umfang und nur für die notwendige Dauer angewandt werden“ ([127]). In diesen Leitlinien wird auch anhand von Beispielen erklärt, wann die einzelnen Einschränkungen wahrscheinlich zum Tragen kommen ([128]).

(69) Darüber hinaus kann ein Verantwortlicher im Hinblick auf die Möglichkeit, die vorstehend genannten Rechte zum Schutz der „nationalen Sicherheit“ einzuschränken, eine von einem Kabinettsminister oder dem Generalstaatsanwalt (bzw. dem Generalanwalt für Schottland) unterzeichnete Bescheinigung beantragen, aus der hervorgeht, dass eine Einschränkung dieser Rechte eine notwendige und verhältnismäßige Maßnahme zum Schutz der nationalen Sicherheit darstellt ([129]). Die britische Regierung hat Leitlinien zu nationalen Sicherheitsbescheinigungen gemäß dem DPA 2018 herausgegeben, in denen ausdrücklich betont wird, dass jede Einschränkung der Rechte betroffener Personen aus Gründen des Schutzes der nationalen Sicherheit verhältnismäßig und notwendig sein muss ([130]) (nähere Informationen über nationale Sicherheitsbescheinigungen finden sich in den Erwägungsgründen 131 bis 134).

([121]) Paragraf 45 Absatz 4 DPA 2018.
([122]) Paragraf 44 Absatz 4 DPA 2018.
([123]) Paragraf 68 Absatz 7 DPA 2018.
([124]) Paragraf 48 Absatz 3 DPA 2018.
([125]) Siehe zum Beispiel den Leitfaden „Guide to Law Enforcement Processing“ zum Auskunftsrecht, abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8
([126]) Siehe zum Beispiel das vom National Police Chief Counsel herausgegebene Handbuch „Data Protection Manual for Police Data Protection Professional“ (siehe Fußnote 27), oder die Leitlinien des Serious Fraud Office, abrufbar unter folgendem Link: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/
([127]) National Police Chief Counsel, Data Protection Manual, S. 140 (siehe Fußnote 27).
([128]) Laut dem Datenschutzhandbuch des National Police Chief Counsel dürfte die Begründung, „behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern“, zum Tragen kommen, wenn personenbezogene Daten für gerichtliche Untersuchungen, familiengerichtliche Verfahren, nichtstrafrechtliche interne Disziplinarverfahren und Untersuchungen im Bereich Kindesmissbrauch verarbeitet werden; eine Einschränkung zum Schutz der „Rechte und Freiheiten anderer“ hingegen ist für personenbezogene Daten relevant, die nicht den Antragsteller, sondern auch andere natürliche Personen betreffen würden (Datenschutzhandbuch des National Police Chief Counsel, S. 140, siehe Fußnote 27).
([129]) Paragraf 79 DPA 2018.
([130]) UK Government Guidance on National Security Certificates, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

(70) Ferner muss die zuständige Behörde in dem Fall, dass eine Einschränkung der Rechte einer betroffenen Person zur Anwendung kommt, die betroffene Person unverzüglich über die Einschränkung ihrer Rechte, die Gründe hierfür und die Rechtsbehelfsmöglichkeiten in Kenntnis setzen, es sei denn, diese Auskunftserteilung würde den Grund für die Anwendung der Einschränkung beeinträchtigen ([131]). Als weitere Maßnahme zum Schutz vor dem Missbrauch der Einschränkungen muss der Verantwortliche die Gründe für die Einschränkung der Informationen aufzeichnen und dem Information Commissioner die Aufzeichnungen auf Verlangen vorlegen ([132]).

(71) Weigert sich der Verantwortliche, zusätzliche Transparenzinformationen bereitzustellen oder Auskünfte zu erteilen, oder lehnt er einen Antrag auf Berichtigung oder Löschung personenbezogener Daten oder auf Einschränkung der Verarbeitung ab, so kann die betroffene Person beim Information Commissioner beantragen, dass geprüft wird, ob der Verantwortliche die Einschränkung rechtmäßig angewandt hat ([133]). Die betroffene Person kann auch Beschwerde beim Information Commissioner einreichen oder bei Gericht beantragen, dass der Verantwortliche angewiesen wird, dem Antrag nachzukommen ([134]).

2.4.7.2. Automatisierte Entscheidungsfindung

(72) Die Paragrafen 49 und 50 des DPA 2018 befassen sich mit den Rechten im Zusammenhang mit der automatisierten Entscheidungsfindung bzw. den zugehörigen Schutzbestimmungen ([135]). Ähnlich wie Artikel 11 der Richtlinie (EU) 2016/680 darf der Verantwortliche bedeutende Entscheidungen nur dann ausschließlich auf der Grundlage einer automatisierten Verarbeitung personenbezogener Daten treffen, wenn dies nach dem Gesetz erforderlich oder zulässig ist ([136]). Eine Entscheidung ist bedeutend, wenn sie eine nachteilige Rechtsfolge für die betroffene Person haben oder sie erheblich beeinträchtigen würde ([137]).

(73) Für den Fall, dass der Verarbeiter gesetzlich verpflichtet oder befugt ist, eine bedeutende Entscheidung zu treffen, sind in Paragraf 50 DPA 2018 die Garantien genannt, die für eine als bedeutend eingestufte Entscheidung (eine „qualifying significant decision") gelten. Der Verarbeiter muss der betroffenen Person so bald wie nach vernünftigem Ermessen möglich mitteilen, dass eine solche Entscheidung getroffen wurde. Die betroffene Person kann dann binnen eines Monats beantragen, dass der Verantwortliche die Entscheidung überprüft oder eine neue Entscheidung trifft, die nicht ausschließlich auf einer automatisierten Verarbeitung beruht. Der Verantwortliche muss den Antrag prüfen und die betroffene Person über das Ergebnis dieser Prüfung informieren. Gemäß DPA 2018 ist der Secretary of State befugt, mittels Verordnungen weitere Garantien vorzusehen ([138]). Bislang wurden noch keine derartigen Verordnungen verabschiedet.

2.4.8. *Weiterübermittlungen*

(74) Das Schutzniveau für personenbezogene Daten, die von einer Strafverfolgungsbehörde in einem Mitgliedstaat an eine Strafverfolgungsbehörde im Vereinigten Königreich übermittelt werden, darf nicht durch die Weiterübermittlung dieser Daten an Empfänger in einem Drittland beeinträchtigt werden. Solche Weiterübermittlungen („onward transfers"), die aus Sicht einer britischen Strafverfolgungsbehörde internationale Übermittlungen aus dem Vereinigten Königreich darstellen, sollten nur dann zulässig sein, wenn der spätere Empfänger außerhalb des Vereinigten Königreichs selbst Vorschriften unterliegt, die ein ähnliches Schutzniveau gewährleisten, wie es in der Rechtsordnung des Vereinigten Königreichs garantiert ist.

([131]) Paragraf 44 Absätze 5 und 6; Paragraf 45 Absatz 5 und 6; Paragraf 48 Absatz 4 DPA 2018.
([132]) Paragraf 44 Absatz 7; Paragraf 45 Absatz 7; Paragraf 48 Absatz 6 DPA 2018.
([133]) Paragraf 51 DPA 2018.
([134]) Paragraf 167 DPA 2018.
([135]) Zum Umfang der automatisierten Verarbeitung heißt es in den Erläuterungen zum DPA 2018 wie folgt: „Diese Bestimmungen gelten für die vollständig automatisierte Entscheidungsfindung und für die automatisierte Verarbeitung. Eine automatisierte Verarbeitung (einschließlich Profiling) liegt vor, wenn Daten verarbeitet werden, ohne dass der Mensch eingreifen muss. Im Bereich der Strafverfolgung wird sie regelmäßig eingesetzt, um große Datenbestände gefiltert und auf eine überschaubare Menge zu reduzieren, damit sie von einem menschlichen Operator bearbeitet werden können. Die automatisierte Entscheidungsfindung ist eine Form der automatisierten Verarbeitung, bei der die endgültige Entscheidung ohne menschliches Eingreifen getroffen wird." (Erläuterungen zum DPA, Nummer 204, siehe Fußnote 45).
([136]) Zusätzlich zu den Schutzmaßnahmen, die der DPA vorsieht, gibt es im Rechtsrahmen des Vereinigten Königreichs weitere rechtliche Einschränkungen, die für Strafverfolgungsbehörden gelten und gegebenenfalls eine automatisierte Verarbeitung (einschließlich Profiling) verhindern würden, die zu rechtswidriger Diskriminierung führt. Mit dem Human Rights Act 1998 wurden die in der Europäischen Menschenrechtskonvention verbürgten Rechte in das Recht des Vereinigten Königreichs übernommen, einschließlich des Rechts in Artikel 14 der Konvention, bezüglich des Verbots der Benachteiligung. In ähnlicher Weise verbietet der Equality Act 2010 die Benachteiligung von Menschen mit schutzwürdigen Eigenschaften (u. a. Geschlecht, Rasse, Behinderung usw.).
([137]) Paragraf 49 Absatz 2 DPA 2018.
([138]) Paragraf 50 Absatz 4 DPA 2018.

(75) Die Bestimmungen des Vereinigten Königreichs über internationale Datenübermittlungen finden sich in Kapitel 5 Teil 3 DPA 2018 ([139]) und folgen dem in Kapitel V der Richtlinie (EU) 2016/680 gewählten Ansatz. Insbesondere muss eine zuständige Behörde drei Bedingungen erfüllen, um personenbezogene Daten an ein Drittland übermitteln zu dürfen: a) Die Datenübermittlung muss für einen Zweck der Strafverfolgung erforderlich sein; b) die Übermittlung muss auf der Grundlage i) einer Angemessenheitsvorschrift im Hinblick auf das Drittland, ii) geeigneter Garantien (wenn keine Angemessenheitsvorschrift vorliegt), oder iii) besonderer Umstände (wenn weder eine Angemessenheitsvorschrift noch geeignete Garantien bestehen) erfolgen; c) Empfänger der Datenübermittlung muss sein: i) eine relevante Behörde (d. h. die einer zuständigen Behörde entsprechende Stelle) des Drittlands, ii) eine relevante internationale Organisation („relevant international organisation"), d. h. eine internationale Einrichtung, die einem der Strafverfolgungszwecke entsprechende Funktionen ausübt, oder iii) eine andere Person als eine zuständige Behörde, jedoch nur, wenn die Datenübermittlung für die Erfüllung eines der Strafverfolgungszwecke unbedingt erforderlich ist, keine Grundrechte und -freiheiten der betroffenen Person gegenüber dem öffentlichen Interesse an einer Übermittlung überwiegen, eine Übermittlung der personenbezogenen Daten an eine relevante Behörde im Drittland wirkungslos und ungeeignet wäre und der Empfänger unverzüglich über die Zwecke, zu denen die Daten verarbeitet werden können, unterrichtet wird ([140]).

(76) Angemessenheitsvorschriften im Hinblick auf ein Drittland, ein Gebiet oder einen Sektor in einem Drittland, eine internationale Organisation oder eine Beschreibung ([141]) eines solchen Landes, Gebiets, Sektors oder einer internationalen Organisation werden vom Secretary of State erlassen. Was die zu erfüllenden Standards betrifft, so muss der Secretary of State beurteilen, ob ein solches Gebiet, ein solcher Sektor bzw. eine solche Organisation ein angemessenes Datenschutzniveau bietet. Nach Paragraf 74A Absatz 4 DPA 2018 muss der Secretary of State zu diesem Zweck eine Reihe von Elementen prüfen, die den in Artikel 36 der Richtlinie (EU) 2016/680 genannten Elementen entsprechen ([142]). Diesbezüglich stellt Teil 3 des DPA 2018 seit dem Ende des Übergangszeitraums eine aus Unionsrecht abgeleitete innerstaatliche Rechtsvorschrift („EU-derived domestic legislation") dar, die, wie bereits erläutert, von den britischen Gerichten im Einklang mit der einschlägigen Rechtsprechung des Gerichtshofs aus der Zeit vor dem EU-Austritt des Vereinigten Königreichs sowie mit den allgemeinen Grundsätzen des Unionsrechts ausgelegt werden soll, so wie sie unmittelbar vor dem Ende des Übergangszeitraums galten. Dazu gehört das Kriterium der wesentlichen Gleichwertigkeit („essential equivalence"), das somit für die von den britischen Behörden vorgenommenen Angemessenheitsbewertungen gelten wird.

(77) Was das Verfahren betrifft, so unterliegen die Vorschriften den allgemeinen („general") Verfahrensmodalitäten gemäß Paragraf 182 DPA 2018. Nach diesem Verfahren muss der Secretary of State bei einem Vorschlag zum Erlass

([139]) Dieser neue Rahmen, einschließlich der Befugnis des Secretary of State zum Erlass von Angemessenheitsvorschriften, ist am Ende des Übergangszeitraums in Kraft getreten. Allerdings sehen die DPPEC Regulations (insbesondere die Nummern 10 bis 12 des durch die DPPEC Regulations in den DPA 2018 eingefügten Anhangs 21) vor, dass bestimmte Übermittlungen personenbezogener Daten ab dem Ende des Übergangszeitraums so behandelt werden, als ob sie auf Angemessenheitsvorschriften beruhten. Diese Datenübermittlungen umfassen Übermittlungen an Drittländer, die Gegenstand eines Angemessenheitsbeschlusses der EU am Ende des Übergangszeitraums sind, sowie an EU-Mitgliedstaaten, die EFTA-Staaten und Gibraltar aufgrund ihrer Anwendung der Richtlinie zum Datenschutz bei der Strafverfolgung auf die Datenverarbeitung zu Strafverfolgungszwecken (die EFTA-Staaten wenden die Richtlinie (EU) 2016/680 aufgrund ihrer Verpflichtungen im Rahmen des Schengen-Besitzstands an). Damit können am Ende des Übergangszeitraums Datenübermittlungen an diese Länder in gleicher Weise durchgeführt werden wie vor dem EU-Austritt. Nach dem Ende des Übergangszeitraums muss der Secretary of State innerhalb von vier Jahren eine Überprüfung dieser Angemessenheitsfeststellungen vornehmen.

([140]) Paragrafen 73 und 77 DPA 2018.

([141]) Nach Angaben der britischen Behörden bezieht sich die Beschreibung eines Landes oder einer internationalen Organisation auf eine Situation, in der es notwendig wäre, eine spezifische und partielle Angemessenheitsfeststellung mit gezielten Beschränkungen vorzunehmen (z. B. Angemessenheitsvorschriften nur zu bestimmten Arten von Datenübermittlungen).

([142]) Siehe Paragraf 74A Absatz 4 DPA 2018, der vorsieht, dass der Secretary of State bei der Beurteilung der Angemessenheit des Schutzniveaus „insbesondere Folgendes zu prüfen hat: a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, auch in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, und den Zugang der Behörden zu personenbezogenen Daten sowie die Durchsetzung dieser Vorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden, b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit dem Information Commissioner zuständig sind, und c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Rechtsinstrumenten sowie aus der Teilnahme des Drittlandes oder der internationalen Organisation an multilateralen oder regionalen Systemen, insbesondere in Bezug auf den Schutz personenbezogener Daten, ergeben".

künftiger Angemessenheitsvorschriften im Vereinigten Königreich den Information Commissioner konsultieren ([143]). Nach ihrer Verabschiedung durch den Secretary of State werden die Vorschriften dem Parlament vorgelegt und dort dem negativen Abstimmungsverfahren („negative resolution procedure") unterzogen, bei dem beide Kammern des Parlaments die Vorschriften prüfen können und die Möglichkeit haben, innerhalb einer Frist von 40 Tagen einen Antrag auf deren Aufhebung zu stellen ([144]).

(78) Gemäß Paragraf 74B Absatz 1 DPA 2018 müssen die Angemessenheitsvorschriften mindestens alle vier Jahre überprüft werden; ferner muss der Secretary of State laufend die Entwicklungen in Drittländern und internationalen Organisationen beobachten, die sich auf Entscheidungen über den Erlass, die Änderung oder die Aufhebung von Angemessenheitsvorschriften auswirken könnten. Stellt der Secretary of State fest, dass ein bestimmtes Land oder eine bestimmte Organisation kein angemessenes Schutzniveau für personenbezogene Daten mehr gewährleistet, muss er, soweit erforderlich, die Vorschriften ändern oder aufheben und Konsultationen mit dem betreffenden Drittland oder der betreffenden internationalen Organisation aufnehmen, um dem Fehlen eines angemessenen Schutzniveaus abzuhelfen.

(79) Analog zu den Bestimmungen des Artikels 37 der Richtlinie (EU) 2016/680 wäre in Ermangelung einer Angemessenheitsvorschrift die Übermittlung personenbezogener Daten im Rahmen der Strafverfolgung möglich, wenn geeignete Garantien bestehen. Solche Garantien werden entweder a) durch ein rechtsverbindliches Instrument gewährleistet, das geeignete Garantien für den Schutz personenbezogener Daten umfasst, oder b) durch eine vom Verantwortlichen vorgenommene Beurteilung sichergestellt, in der dieser nach Prüfung aller Umstände der Übermittlung zu dem Schluss gelangt, dass geeignete Garantien zum Schutz der Daten bestehen ([145]). Bei Datenübermittlungen auf der Grundlage geeigneter Garantien sieht der DPA 2018 außerdem zusätzlich zur normalen Aufsichtsfunktion des ICO vor, dass die zuständigen Behörden dem ICO spezifische Informationen über die Datenübermittlungen bereitstellen müssen ([146]).

(80) Beruht eine Übermittlung nicht auf einem Angemessenheitsbeschluss oder geeigneten Garantien, darf sie nur unter bestimmten, festgelegten Umständen („special circumstances") erfolgen ([147]). Besondere Umstände liegen vor, wenn die Übermittlung aus einem der folgenden Gründe erforderlich ist: a) zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person, b) zur Wahrung berechtigter Interessen der betroffenen Person, c) zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Drittlandes, d) im Einzelfall für einen der Zwecke der Strafverfolgung, oder e) im Einzelfall für einen rechtlichen Zweck (z. B. im Zusammenhang mit einem Gerichtsverfahren oder zur Einholung rechtlicher Beratung) ([148]). Es sei darauf hingewiesen, dass die Buchstaben d und e nicht gelten, wenn die Rechte und Freiheiten der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen ([149]). Diese Umstände entsprechen den bestimmten Fällen und Bedingungen, die nach Artikel 38 der Richtlinie (EU) 2016/680 als „Ausnahmen" gelten.

(81) Unter diesen Umständen müssen Datum und Uhrzeit der Übermittlung, die Begründung, der Name und alle anderen einschlägigen Informationen über den Empfänger sowie eine Beschreibung der übermittelten personenbezogenen Daten dokumentiert und dem Information Commissioner auf Anfrage zur Verfügung gestellt werden ([150]).

(82) Paragraf 78 DPA 2018 regelt das Szenario der späteren Übermittlung („subsequent transfer"), d. h. den Fall, dass personenbezogene Daten, die vom Vereinigten Königreich an ein Drittland übermittelt wurden, anschließend an ein weiteres Drittland oder an eine internationale Organisation weitergegeben werden. Gemäß Paragraf 78 Absatz 1 muss der übermittelnde Verantwortliche im Vereinigten Königreich die Datenübermittlung an die Bedingung knüpfen, dass die Daten nicht ohne die Genehmigung des übermittelnden Verantwortlichen an ein Drittland weiterübermittelt werden dürfen. Darüber hinaus gelten gemäß Paragraf 78 Absatz 3 und analog zu Artikel 35 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/680 eine Reihe wesentlicher Anforderungen, wenn eine solche Genehmigung erforderlich ist. Konkret muss eine zuständige Behörde bei der Entscheidung über die Genehmigung einer Übermittlung sicherstellen, dass die Weiterübermittlung für einen Zweck der Strafverfolgung erforderlich ist,

([143]) Siehe die Absichtserklärung 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 hinsichtlich der neuen Angemessenheitsbewertung des Vereinigten Königreichs, abrufbar unter folgendem Link: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) In diesem 40-tägigen Zeitraum haben beide Kammern des Parlaments die Möglichkeit, gegen die Vorschriften zu stimmen, falls sie dies wünschen. Im Falle eines solchen Votums verlieren die Vorschriften endgültig jede Rechtswirkung.

([145]) Paragraf 75 DPA 2018.

([146]) Nach Paragraf 75 Absatz 3 DPA 2018 gilt für den Fall einer Datenübermittlung auf der Grundlage geeigneter Garantien Folgendes: a) Die Übermittlung muss dokumentiert werden, b) die Dokumentation muss dem Information Commissioner auf Anfrage zur Verfügung gestellt werden und c) die Dokumentation muss insbesondere i) Datum und Zeitpunkt der Übermittlung, ii) den Namen und alle anderen einschlägigen Informationen über den Empfänger, iii) die Begründung der Übermittlung und iv) eine Beschreibung der übermittelten personenbezogenen Daten umfassen.

([147]) Guide to Law Enforcement Processing, „Are there any special circumstances?", abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) Paragraf 76 DPA 2018.

([149]) Paragraf 76 DPA 2018.

([150]) Paragraf 76 Absatz 3 DPA 2018.

und dabei unter anderem folgende Faktoren prüfen: die Schwere der Umstände, die zu dem Genehmigungsantrag führen, b) den Zweck, zu dem die personenbezogenen Daten ursprünglich übermittelt wurden, und c) die in dem Drittland oder bei der internationalen Organisation, an die die personenbezogenen Daten weiterübermittelt werden sollen, geltenden Datenschutzstandards.

(83) Ferner gelten zusätzliche Garantien, wenn die Daten, die einer Weiterübermittlung aus dem Vereinigten Königreich unterliegen, ursprünglich aus der Europäischen Union übermittelt wurden.

(84) Erstens besagt Paragraf 73 Absatz 1 Buchstabe b DPA 2018 — analog zu Artikel 35 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680 —, dass im Falle einer ursprünglichen Übermittlung oder in anderer Weise erfolgten Bereitstellung personenbezogener Daten an den Verantwortlichen oder eine andere zuständige Behörde durch einen Mitgliedstaat der betreffende Mitgliedstaat oder eine andere Person mit Sitz im betreffenden Mitgliedstaat, bei der es sich um eine zuständige Behörde für die Zwecke der Richtlinie (EU) 2016/680 handelt, die Datenübermittlung gemäß dem Recht des Mitgliedstaats genehmigt haben muss.

(85) Ähnlich wie in Artikel 35 Absatz 2 der Richtlinie (EU) 2016/680 wird eine solche Genehmigung jedoch nicht verlangt, wenn a) die Datenübermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und b) die Genehmigung nicht rechtzeitig eingeholt werden kann. In diesem Fall ist die Behörde, die im Mitgliedstaat über die Erteilung der Genehmigung hätte entscheiden müssen, unverzüglich zu unterrichten ([151]).

(86) Zweitens gilt derselbe Ansatz im Fall von Daten, die ursprünglich aus der Europäischen Union an das Vereinigte Königreich übermittelt wurden, und anschließend vom Vereinigten Königreich an ein Drittland weiterübermittelt werden, das diese dann an ein weiteres Drittland weitergibt. In diesem Fall kann gemäß Paragraf 78 Absatz 4 die zuständige britische Behörde die letztgenannte Übermittlung nicht genehmigen, in Übereinstimmung mit Paragraf 78 Absatz 1, es sei denn, der „Mitgliedstaat [der die betreffenden Daten ursprünglich übermittelt hat] oder eine andere Person mit Sitz im betreffenden Mitgliedstaat, bei der es sich um eine zuständige Behörde für die Zwecke der Strafverfolgungsrichtlinie handelt, hat die Datenübermittlung gemäß dem Recht des Mitgliedstaats genehmigt". Diese Garantien sind wichtig, da sie die Behörden der Mitgliedstaaten in die Lage versetzen, die Kontinuität des Schutzes in Übereinstimmung mit dem Datenschutzrecht der EU, über die „Übermittlungskette" hinweg, zu gewährleisten.

(87) Dieser neue Rahmen für internationale Übermittlungen ist am Ende des Übergangszeitraums in Kraft getreten ([152]). Allerdings sehen die Nummern 10 bis 12 des (durch die DPPEC Regulations eingeführten) Anhangs 21 vor, dass bestimmte Übermittlungen personenbezogener Daten ab dem Ende des Übergangszeitraums so behandelt werden, als ob sie auf Angemessenheitsvorschriften beruhten. Zu diesen Übermittlungen zählen Übermittlungen an einen Mitgliedstaat, einen EFTA-Staat und an Drittländer, die am Ende des Übergangszeitraums Gegenstand eines Angemessenheitsbeschlusses der EU waren, und Gibraltar. Folglich können Übermittlungen an diese Länder weiterhin wie vor dem Austritt des Vereinigten Königreichs aus der Union durchgeführt werden. Nach dem Ende des Übergangszeitraums muss der Secretary of State innerhalb von vier Jahren, d. h. bis Ende Dezember 2024, eine Überprüfung dieser Angemessenheitsfeststellungen vornehmen. Laut den Erläuterungen der britischen Behörden muss der Secretary of State zwar bis Ende Dezember 2024 eine solche Überprüfung durchführen, allerdings umfassen die Übergangsbestimmungen keine „Sunset"-Klausel und die entsprechenden Übergangsbestimmungen treten nicht automatisch außer Kraft, wenn die Überprüfung nicht bis Ende Dezember 2024 abgeschlossen ist.

2.4.9. *Rechenschaftspflicht*

(88) Nach dem Grundsatz der Rechenschaftspflicht müssen Daten verarbeitende Behörden geeignete technische und organisatorische Maßnahmen treffen, um ihren Datenschutzverpflichtungen wirksam nachzukommen und dies, insbesondere gegenüber der zuständigen Aufsichtsbehörde, nachweisen zu können.

(89) Dieser Grundsatz schlägt sich in Paragraf 56 DPA 2018 nieder, mit dem eine allgemeine Rechenschaftspflicht für den Verantwortlichen eingeführt wird, d. h. die Pflicht, geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Verarbeitung personenbezogener Daten die Anforderungen von Teil 3 des DPA 2018 erfüllt, und dies nachweisen zu können. Die umgesetzten Maßnahmen müssen überprüft und gegebenenfalls aktualisiert werden und, sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, geeignete Datenschutzvorkehrungen umfassen.

([151]) Paragraf 73 Absatz 5 DPA 2018.

([152]) Die Anwendbarkeit dieses neuen Rahmens ist im Lichte von Artikel 782 des Handels- und Kooperationsabkommens zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits (L 444/14 vom 31.12.2020) auszulegen, das unter folgendem Link abrufbar ist: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN

(90) Analog zu Kapitel IV der Richtlinie (EU) 2016/680 sehen die Paragrafen 55 bis 71 DPA 2018 verschiedene Mechanismen vor, um die Rechenschaftspflicht zu gewährleisten und es den Verantwortlichen und Auftragsverarbeitern zu ermöglichen, die Einhaltung der Vorschriften nachzuweisen. Die Verantwortlichen sind insbesondere verpflichtet, Datenschutzmaßnahmen durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen umzusetzen, also sicherzustellen, dass die Datenschutzgrundsätze wirksam umgesetzt werden; ferner müssen sie ein Verzeichnis aller Kategorien von Tätigkeiten führen, für die der Verantwortliche zuständig ist (einschließlich der Identität des Verantwortlichen, der Kontaktdaten des Datenschutzbeauftragten, der Zwecke der Verarbeitung, der Kategorien von Empfängern von Offenlegungen und einer Beschreibung der Kategorien von betroffenen Personen sowie von personenbezogenen Daten), und müssen dieses Verzeichnis auf Anfrage für den Information Commissioner bereithalten. Verantwortlicher und Auftragsverarbeiter müssen außerdem bestimmte Verarbeitungsvorgänge protokollieren und dem Information Commissioner die Protokolle zur Verfügung stellen ([153]). Die Verantwortlichen sind zudem ausdrücklich verpflichtet, mit dem Information Commissioner bei der Erfüllung seiner Aufgaben zusammenzuarbeiten.

(91) Der DPA 2018 sieht zusätzliche Anforderungen für eine Verarbeitung vor, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dazu zählen die Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen und zur Konsultation des Information Commissioner vor der Verarbeitung, wenn aus der Folgenabschätzung hervorgeht, dass die Verarbeitung (sofern keine Maßnahmen zur Eindämmung des Risikos getroffen werden) ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hätte.

(92) Darüber hinaus müssen die Verantwortlichen einen Datenschutzbeauftragten ernennen, es sei denn, es handelt sich bei dem Verantwortlichen um ein Gericht oder eine andere Justizbehörde, das bzw. die im Rahmen ihrer justiziellen Tätigkeit handelt ([154]). Der Verantwortliche muss dafür sorgen, dass der Datenschutzbeauftragte in alle mit dem Schutz personenbezogener Daten zusammenhängende Fragen eingebunden wird, über die erforderlichen Ressourcen verfügt und Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen hat, und dass er seine Aufgaben unabhängig ausüben kann. Die Aufgaben des Datenschutzbeauftragten sind in Paragraf 71 DPA 2018 festgelegt und umfassen die Aufklärung und Beratung, die Überwachung der Einhaltung der Vorschriften sowie die Zusammenarbeit dem Information Commissioner, für den der Datenschutzbeauftragten als Anlaufstelle dient. Der Datenschutzbeauftragte muss bei der Ausübung seiner Aufgaben den mit Verarbeitungsvorgängen verbundenen Risiken Rechnung tragen und dabei Art, Umfang, Umstände und Zwecke der Verarbeitung berücksichtigen.

2.5. **Aufsicht und Durchsetzung**

2.5.1. *Unabhängige Aufsicht*

(93) Um sicherzustellen, dass auch in der Praxis ein angemessenes Datenschutzniveau gewährleistet ist, muss eine unabhängige Aufsichtsbehörde mit der Befugnis zur Überwachung und Durchsetzung der Einhaltung der Datenschutzvorschriften eingerichtet werden. Diese Behörde hat bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse vollkommen unabhängig und unparteiisch zu handeln.

(94) Im Vereinigten Königreich ist der Information Commissioner für die Überwachung und Durchsetzung der Einhaltung der UK GDPR und des DPA 2018 zuständig ([155]). Der Information Commissioner überwacht außerdem die Verarbeitung personenbezogener Daten durch zuständige Behörden, die in den Anwendungsbereich von Teil 3 des DPA 2018 fallen ([156]). Der Information Commissioner ist eine „Corporation Sole": d. h. ein eigenständiges Rechtssubjekt, das aus einer einzigen Person besteht. Der Information Commissioner wird bei seiner Arbeit von einem Büro unterstützt. Am 31. März 2020 waren im Büro des Information Commissioner 768 Festangestellte tätig ([157]). Der Information Commissioner wird vom britischen Ministerium für Digitales, Kultur, Medien und Sport gefördert ([158]).

([153]) Paragraf 62 DPA 2018.
([154]) Paragraf 69 DPA 2018.
([155]) Artikel 36 Absatz 2 Buchstabe b der Richtlinie (EU) 2016/680.
([156]) Paragraf 116 DPA 2018.
([157]) Jahresbericht und Jahresabschluss 2019–2020 des Information Commissioner, abrufbar unter folgendem Link: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf
([158]) Die Beziehung zwischen den beiden Institutionen ist in einer Verwaltungsvereinbarung geregelt. Als Fördereinrichtung ist das Ministerium für Digitales, Kultur, Medien und Sport insbesondere dafür zuständig, sicherzustellen, dass das ICO mit ausreichenden Mitteln und Ressourcen ausgestattet ist, die Interessen des ICO gegenüber dem Parlament und anderen Regierungsstellen zu vertreten, sicherzustellen, dass ein solider nationaler Datenschutzrahmen vorhanden ist, das ICO bei internen Fragen wie Immobilienangelegenheiten, Mietverträgen und Beschaffungen zu beraten und zu unterstützen (vgl. Verwaltungsvereinbarung 2018–2021, abrufbar unter folgendem Link: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Die Unabhängigkeit des Information Commissioner ist in Artikel 52 UK GDPR ausdrücklich festgelegt, der die in Artikel 52 Absatz 1 bis 3 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([159]) genannten Bestimmungen widerspiegelt. Bei der Erfüllung seiner Aufgaben und der Ausübung seiner Befugnisse gemäß der UK GDPR muss der Information Commissioner völlig unabhängig handeln; er darf weder direkter noch indirekter Beeinflussung von außen unterliegen und weder um Weisung ersuchen noch Weisungen entgegennehmen. Zudem muss er von allen mit den Aufgaben seines Amtes nicht zu vereinbarenden Handlungen absehen und darf während seiner Amtszeit keine andere mit seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit ausüben.

(96) Die Bedingungen für die Ernennung und Abberufung des Information Commissioner sind in Anhang 12 des DPA 2018 festgelegt. Der Information Commissioner wird von der Königin auf Empfehlung der Regierung im Wege eines fairen und offenen Auswahlverfahrens ernannt. Der Kandidat muss über geeignete Qualifikationen, Fähigkeiten und Kompetenzen verfügen. Gemäß dem Kodex der Regierung über die Besetzung öffentlicher Ämter (Governance Code on Public Appointments) ([160]) erstellt ein beratendes Bewertungsgremium eine Liste mit infrage kommenden Kandidaten. Bevor der Secretary of State im Ministerium für Digitales, Kultur, Medien und Sport seine Entscheidung trifft, muss der zuständige Sonderausschuss des Parlaments im Vorfeld der Ernennung eine Prüfung durchführen. Die entsprechende Stellungnahme des Ausschusses wird veröffentlicht ([161]).

(97) Die Amtszeit des Information Commissioner dauert bis zu sieben Jahre. Der Information Commissioner kann von Ihrer Majestät nach einer Meinungsäußerung („Address“) beider Kammern des Parlaments seines Amtes enthoben werden ([162]). Ein Antrag auf Entlassung des Information Commissioner kann nur dann einer der beiden Kammern des Parlaments vorgelegt werden, wenn ein Minister der betreffenden Kammer einen Bericht vorgelegt hat, in dem er erklärt, dass sich der Information Commissioner seiner Überzeugung nach eines schweren Fehlverhaltens schuldig gemacht hat und/oder nicht mehr die Voraussetzungen für die Ausübung seiner Funktionen erfüllt ([163]).

(98) Der Information Commissioner bezieht seine finanziellen Mittel aus drei Quellen: i) von den Verantwortlichen entrichtete Datenschutzgebühren, die durch Verordnungen des Secretary of State ([164]) festgelegt werden und 85 % bis 90 % des Jahreshaushalts des ICO ([165]) ausmachen, ii) Zuschüsse, die die Regierung dem Information Commissioner gewähren kann und hauptsächlich der Finanzierung der Betriebskosten des Information Commissioner für nicht datenschutzbezogene Aufgaben dienen ([166]), iii) für Dienstleistungen erhobene Gebühren ([167]). Derzeit werden keine derartigen Gebühren erhoben.

(99) Die allgemeinen Aufgaben des Information Commissioner im Zusammenhang mit der Verarbeitung personenbezogener Daten, die in den Anwendungsbereich von Teil 3 des DPA 2018 fallen, sind in Anhang 13 des DPA 2018 festgelegt. Zu seinen Aufgaben zählen die Überwachung und Durchsetzung der Bestimmungen von Teil 3 des DPA 2018, die Sensibilisierung der Öffentlichkeit, die Beratung des Parlaments, der Regierung und

([159]) 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) (ABl. L 119 vom 4.5.2016, S. 1).

([160]) Governance Code on Public Appointments, abrufbar unter folgendem Link: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Zweiter Bericht der Sitzungsperiode 2015–2016 des Ausschusses für Kultur, Medien und Sport im Unterhaus, abrufbar unter folgendem Link: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([162]) Eine „Address“ ist ein dem Parlament vorgelegter Antrag, mit dem der Monarch über die Ansichten des Parlaments zu einem bestimmten Thema unterrichtet wird.

([163]) Anhang 12 Nummer 3 des DPA 2018.

([164]) Paragraf 137 DPA 2018.

([165]) Paragrafen 137 und 138 DPA 2018 enthalten eine Reihe von Garantien, um sicherzustellen, dass die Gebühren in angemessener Höhe festgelegt werden. Insbesondere Paragraf 137 Absatz 4 DPA 2018 enthält Punkte, die der Secretary of State beim Erlass von Verordnungen berücksichtigen muss, in denen die von verschiedenen Organisationen zu zahlenden Beträge festgelegt sind. Darüber hinaus ist der Secretary of State gemäß Paragraf 138 Absatz 1 und Paragraf 182 DPA 2018 gesetzlich dazu verpflichtet, vor dem Erlass von Verordnungen den Information Commissioner und andere Vertreter von Personen, die voraussichtlich davon betroffen sein werden, zu konsultieren, damit ihre Ansichten berücksichtigt werden können. Des Weiteren ist der Information Commissioner gemäß Paragraf 138 Absatz 2 DPA 2018 verpflichtet, die Verordnungen bezüglich der Gebühren laufend zu überprüfen, und kann dem Secretary of State Vorschläge für Änderungen der Verordnungen unterbreiten. Schließlich gilt: Sofern die Verordnungen nicht lediglich zur Berücksichtigung einer Erhöhung des Einzelhandelspreisindexes erlassen werden (in diesem Fall unterliegen sie dem negativen Abstimmungsverfahren („negative resolution procedure“)), unterliegen sie dem positiven Abstimmungsverfahren („affirmative resolution procedure“) und dürfen erst dann verabschiedet werden, wenn sie von beiden Kammern des Parlaments gebilligt wurden.

([166]) In der Verwaltungsvereinbarung wurde klargestellt, dass „der Secretary of State Zahlungen an den Information Commissioner aus Geldern leisten kann, die vom Parlament gemäß Anhang 12 Nummer 9 des DPA 2018 bereitgestellt werden. Nach Rücksprache mit dem Information Commissioner zahlt das Ministerium für Digitales, Kultur, Medien und Sport dem ICO angemessene Beträge (Zuschüsse) für die Verwaltungskosten seines Büros und die Ausübung seiner Tätigkeiten im Zusammenhang mit einer Reihe spezifischer Funktionen, einschließlich der Informationsfreiheit“ (Verwaltungsvereinbarung 2018–2021, Nummer 1.12, siehe Fußnote 158).

([167]) Paragraf 134 DPA 2018.

anderer Einrichtungen zu rechtlichen und administrativen Maßnahmen, die Förderung des Bewusstseins der Verantwortlichen und Auftragsverarbeiter für ihre Pflichten, die Aufklärung betroffener Personen über die Ausübung der Rechte betroffener Personen und die Durchführung von Untersuchungen. Damit die Unabhängigkeit der Justiz gewahrt bleibt, ist der Information Commissioner nicht befugt, seine Aufgaben im Zusammenhang mit der Verarbeitung personenbezogener Daten durch eine Person, die im Rahmen einer justiziellen Tätigkeit handelt, oder ein Gericht, das im Rahmen seiner justiziellen Tätigkeit handelt, auszuüben. Die Aufsicht über die Justiz wird jedoch, wie unten dargelegt, durch spezialisierte Stellen gewährleistet.

2.5.1.1 Durchsetzung, einschließlich Sanktionen

(100) Der Information Commissioner besitzt allgemeine Ermittlungs-, Berichtigungs-, Genehmigungs- und Beratungsbefugnisse im Hinblick auf die Verarbeitung personenbezogener Daten, die Gegenstand von Teil 3 des DPA 2018 sind. Der Information Commissioner ist befugt, den Verantwortlichen oder den Auftragsverarbeiter auf einen mutmaßlichen Verstoß gegen Teil 3 in Kenntnis zu setzen, einen Verantwortlichen oder Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen Teil 3 verstoßen, und einen Verantwortlichen oder Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen Teil 3 verstoßen hat. Darüber hinaus kann der Information Commissioner zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das Parlament, die Regierung oder sonstige Einrichtungen und Stellen des Vereinigten Königreichs sowie an die Öffentlichkeit richten ([168]).

(101) Außerdem hat der Information Commissioner die Befugnis,

— im Wege eines Informationsbescheides („information notice“) den Verantwortlichen und den Auftragsverarbeiter (und unter bestimmten Umständen jede andere Person) anzuweisen, erforderliche Informationen bereitzustellen ([169]);

— Untersuchungen und Überprüfungen durchzuführen, indem er einen Bewertungsbescheid erlässt, mit dem der Verantwortliche oder der Auftragsverarbeiter aufgefordert werden kann, dem Information Commissioner zu gestatten, bestimmte Räumlichkeiten zu betreten, Dokumente oder Ausrüstung in Augenschein zu nehmen oder zu prüfen, oder Personen zu befragen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten („assessment notice“) ([170]);

— anderweitig Zugriff auf Dokumente von Verantwortlichen und Auftragsverarbeitern zu erhalten und Zugang zu deren Räumlichkeiten gemäß Paragraf 154 DPA 2018 zu erhalten („powers of entry and inspection“);

— Abhilfebefugnisse auszuüben, unter anderem durch Warnungen und Verwarnungen, oder im Wege eines Durchsetzungsbescheides Anweisungen zu erteilen, um Verantwortliche bzw. Auftragsverarbeiter aufzufordern, bestimmte Maßnahmen zu ergreifen oder zu unterlassen („enforcement notice“); ([171]) und

— im Wege eines Bußgeldbescheides Geldbußen zu verhängen („penalty notice“) ([172]).

(102) In den Leitlinien des ICO zu regulatorischen Maßnahmen (Regulatory Action Policy) ist festgelegt, unter welchen Umständen der Information Commissioner einen Informations-, Bewertungs-, Durchsetzungs- oder Bußgeldbescheid erteilt ([173]). In einem Durchsetzungsbescheid darf der Information Commissioner Auflagen erteilen, die er zur Behebung des Verstoßes für angemessen hält. Ein Bußgeldbescheid verpflichtet eine Person, einen im Bescheid genannten Betrag an den Information Commissioner zu zahlen. Ein Bußgeldbescheid kann erteilt werden, wenn bestimmte Bestimmungen des DPA 2018 ([174]) nicht eingehalten wurden, oder er kann einem Verantwortlichen oder Auftragsverarbeiter erteilt werden, der einem Informations-, Bewertungs- oder Durchsetzungsbescheid nicht nachgekommen ist.

(103) Konkret muss der Information Commissioner bei der Entscheidung, ob und in welcher Höhe einem Verantwortlichen oder Auftragsverarbeiter ein Bußgeldbescheid erteilt wird, die in Paragraf 155 Absatz 3 DPA 2018 aufgeführten Punkte berücksichtigen, darunter die Art und Schwere des Verstoßes, die Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes, alle vom Verantwortlichen oder Auftragsverarbeiter gegebenenfalls zur Minderung des

([168]) Anhang 13 Nummer 2 DPA 2018.
([169]) Paragraf 142 DPA 2018 (vorbehaltlich der in Paragraf 143 DPA 2018 genannten Einschränkungen).
([170]) Paragraf 146 DPA 2018 (vorbehaltlich der in Paragraf 147 DPA 2018 genannten Einschränkungen).
([171]) Paragrafen 149 bis 151 DPA 2018 (vorbehaltlich der in Paragraf 152 DPA 2018 genannten Einschränkungen).
([172]) Paragraf 155 DPA 2018 (vorbehaltlich der in Paragraf 156 DPA 2018 genannten Einschränkungen).
([173]) Regulatory Action Policy, abrufbar unter folgendem Link: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) Das ICO kann einen Bußgeldbescheid insbesondere bei Nichteinhaltung der in Paragraf 149 Absätze 2, 3, 4 oder 5 DPA 2018 genannten Bestimmungen erteilen.

den betroffenen Personen entstandenen Schadens getroffenen Maßnahmen, den Grad der Verantwortung des Verantwortlichen oder Auftragsverarbeiters (unter Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen) sowie etwaige einschlägige frühere Verstöße des Verantwortlichen bzw. Auftragsverarbeiters; ferner ist zu berücksichtigen, welche Kategorien personenbezogener Daten von dem Verstoß betroffen sind, und zu prüfen, ob das Bußgeld wirksam, verhältnismäßig und abschreckend wäre.

(104) Der Höchstbetrag der Geldbuße, die durch einen Bußgeldbescheid verhängt werden kann, beträgt a) 17 500 000 GBP bei Verstößen gegen die Datenschutzgrundsätze (Paragrafen 35, 36, 37, Paragraf 38 Absatz 1, Paragraf 39 Absatz 1 und Paragraf 40 DPA 2018), die Transparenzpflichten und die Rechte des Einzelnen (Paragrafen 44, 45, 46, 47, 48, 49, 52 und 53 DPA 2018), sowie gegen die für internationale Datenübermittlungen geltenden Grundsätze (Paragrafen 73, 75, 76, 77 oder 78 DPA 2018), und b) 8 700 000 GBP in allen anderen Fällen ([175]). Wird einem Informationsbescheid, Bewertungsbescheid oder Durchsetzungsbescheid nicht nachgekommen, kann eine Geldbuße von bis zu 17 500 000 GBP verhängt werden.

(105) Laut seinen letzten Jahresberichten (für die Zeiträume 2018–2019 ([176]) und 2019–2020 ([177])) hat der Information Commissioner im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden eine Reihe von Untersuchungen durchgeführt. So hat er beispielsweise eine Untersuchung zum Einsatz von Gesichtserkennungstechnologie durch Strafverfolgungsbehörden an öffentlichen Orten durchgeführt und im Oktober 2019 eine entsprechende Stellungnahme veröffentlicht. Im Fokus der Untersuchung stand insbesondere der Einsatz von Technologien zur Gesichtserkennung in Echtzeit durch die Polizei von South Wales und den Metropolitan Police Service (MPS). Im Rahmen einer Untersuchung der „Gangs-Matrix" ([178]) des Metropolitan Police Service stellte der Information Commissioner außerdem eine Reihe von schwerwiegenden Verstößen gegen das Datenschutzrecht fest, die geeignet waren, das Vertrauen der Öffentlichkeit in die Matrix und in die Verwendung der Daten zu untergraben.

(106) Im November 2018 erließ der Information Commissioner einen Durchsetzungsbescheid, woraufhin der Metropolitan Police Service die erforderlichen Schritte unternahm, um die Sicherheit und Rechenschaftspflicht zu verbessern und eine verhältnismäßige Nutzung der Daten zu gewährleisten.

(107) In einem weiteren Fall verhängte der Information Commissioner im Mai 2018 als Durchsetzungsmaßnahme eine Geldbuße in Höhe von 325 000 GBP gegen den Crown Prosecution Service wegen des Verlusts unverschlüsselter DVDs, auf denen Vernehmungsprotokolle gespeichert waren. Darüber hinaus führte der Information Commissioner Untersuchungen zu allgemeineren Fragen durch und befasste sich beispielsweise im ersten Halbjahr 2020 mit der Verwendung von Mobilfunkdaten für polizeiliche Zwecke und der Verarbeitung der Daten von Opfern durch die Polizei.

(108) Zusätzlich zu diesen Durchsetzungsbefugnissen des Information Commissioner gelten bestimmte Verstöße gegen die Datenschutzvorschriften als Straftat und können daher strafrechtlich geahndet werden (Paragraf 196 DPA 2018). Beispiele hierfür sind die Erlangung oder Offenlegung personenbezogener Daten ohne Zustimmung des Verantwortlichen und die Veranlassung der Offenlegung personenbezogener Daten gegenüber einer anderen Person ohne Zustimmung des Verantwortlichen ([179]), die Re-Identifizierung von anonymisiert vorliegenden personenbezogen Daten ohne die Zustimmung des für die Anonymisierung der personenbezogenen Daten zuständigen Verantwortlichen ([180]), die vorsätzliche Behinderung des Information Commissioner bei der Ausübung seiner Befugnisse in Bezug auf die Einsichtnahme in personenbezogene Daten gemäß internationalen Verpflichtungen ([181]), die Abgabe falscher Erklärungen bei der Erwiderung auf einen Informationsbescheid oder die Vernichtung von Informationen im Zusammenhang mit Informations- und Bewertungsbescheiden ([182]).

(109) Der Information Commissioner ist ferner gemäß Paragraf 139 DPA 2018 verpflichtet, jeder Kammer des Parlaments einen Gesamtbericht über die Wahrnehmung seiner Aufgaben im Rahmen des Datenschutzgesetzes vorzulegen ([183]).

([175]) Paragraf 157 DPA 2018.

([176]) Jahresbericht und Jahresabschluss 2018-2019 des Information Commissioner, abrufbar unter folgendem Link: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf

([177]) Jahresbericht 2019–2020 des Information Commissioner (siehe Fußnote 157).

([178]) Eine Datenbank, in der Erkenntnisse über mutmaßliche Bandenmitglieder und Opfer von Bandenkriminalität erfasst wurden.

([179]) Paragraf 170 DPA 2018.

([180]) Paragraf 171 DPA 2018.

([181]) Paragraf 119 DPA 2018.

([182]) Paragrafen 144 und 148 DPA 2018.

([183]) Nach Maßgabe der Verwaltungsvereinbarung muss der Jahresbericht: i) alle Unternehmen, Zweigstellen oder Joint Ventures umfassen, die der Kontrolle des ICO unterliegen, ii) den Vorgaben des Handbuchs zur Rechnungslegung (Financial Reporting Manual — FReM) des Finanzministeriums entsprechen, iii) eine Erklärung zur Verwaltungsführung umfassen, die aufzeigt, wie der Accounting Officer die in der Organisation während des Jahres verwendeten Mittel verwaltet und kontrolliert hat, und aus der hervorgeht, wie gut die Organisation die Risiken bewältigt, die für die Erreichung ihrer Ziele bestehen, und iv) eine Beschreibung der wichtigsten Tätigkeiten und Ergebnisse im vorangegangenen Geschäftsjahr und eine Zusammenfassung der Vorausplanung enthalten (Verwaltungsvereinbarung 2018–2021, Nummer 3.26, siehe Fußnote 158).

2.5.2. *Aufsicht über die Justiz*

(110) Die Aufsicht über die Verarbeitung personenbezogener Daten durch die Gerichte und die Justiz erfolgt über zwei Wege. Wenn ein Inhaber eines richterlichen Amtes oder ein Gericht nicht im Rahmen seiner justiziellen Tätigkeit handelt, wird die Aufsichtsfunktion durch den Information Commissioner wahrgenommen. Wenn der Verantwortliche im Rahmen einer justiziellen Tätigkeit handelt, kann das ICO seine Aufsichtsfunktionen ([184]) nicht wahrnehmen und die Aufsicht erfolgt durch spezielle Stellen. Dies entspricht dem in Artikel 32 der Richtlinie (EU) 2016/680 gewählten Ansatz.

(111) Insbesondere im zweiten Szenario — für die Gerichte von England und Wales sowie die First-tier und Upper Tribunals von England und Wales — wird diese Aufsichtsfunktion durch ein richterliches Datenschutzgremium (Judicial Data Protection Panel) ([185]) wahrgenommen. Darüber hinaus haben der Lordoberrichter (Lord Chief Justice) und der Leitende Präsident der Tribunale (Senior President of Tribunals) eine Datenschutzerklärung ([186]) herausgegeben, in der dargelegt ist, wie die Gerichte in England und Wales personenbezogene Daten für eine richterliche Funktion verarbeiten. Die Justizbehörden in Nordirland ([187]) und Schottland ([188]) haben ähnliche Erklärungen herausgegeben.

(112) In Nordirland hat der Lord Chief Justice of Northern Ireland zudem einen Richter des High Court zum Richter für Datenaufsicht (Data Supervisory Judge — DSJ) ([189]) ernannt. Darüber hinaus erhielt die nordirische Justiz Leitlinien dazu, was im Falle eines Datenverlustes oder eines potenziellen Datenverlustes zu tun ist und wie mit den daraus resultierenden Problemen umzugehen ist ([190]).

(113) In Schottland hat der Lord President einen Data Supervisory Judge ernannt, der sämtliche Beschwerden aus Gründen des Datenschutzes untersucht. Dies ist in den Vorschriften für gerichtliche Beschwerden geregelt, die denen für England und Wales entsprechen ([191]).

(114) Schließlich wird einer der Richter des Supreme Court ernannt, um die Aufsicht über den Datenschutz zu führen.

([184]) Paragraf 117 DPA 2018.

([185]) Das Gremium ist für die Beratung und Schulung der Richterschaft verantwortlich. Darüber hinaus befasst es sich mit Beschwerden betroffener Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Gerichte, Tribunale und natürliche Personen, die im Rahmen ihrer justiziellen Tätigkeit handeln. Das Gremium soll geeignete Mittel bereitstellen, mit denen für jede Beschwerde eine Lösung gefunden werden kann. Wenn ein Beschwerdeführer mit einer Entscheidung des Gremiums nicht zufrieden ist und zusätzliche Beweise vorlegt, kann das Gremium seine Entscheidung überdenken. Das Gremium selbst kann zwar keine finanziellen Sanktionen verhängen, doch es kann, wenn es der Ansicht ist, dass ein hinreichend schwerwiegender Verstoß gegen den DPA 2018 vorliegt, die Beschwerde an das zuständige Büro, das Judicial Conduct Investigation Office (im Folgenden „JCIO"), zur Untersuchung weiterleiten. Wird die Beschwerde als begründet erachtet, obliegt es dem Lordkanzler (Lord Chancellor) und dem Lordoberrichter (Lord Chief Justice) (oder einem anderen hochrangigen Richter, der beauftragt ist, in seinem Namen zu handeln), zu entscheiden, welche Maßnahmen gegen den Amtsinhaber ergriffen werden sollten. Diese können von weniger streng bis sehr streng reichen und einen formellen Rat, eine formelle Verwarnung und einen Verweis sowie schließlich die Amtsenthebung umfassen. Ist eine Person mit der Untersuchung der Beschwerde durch das JCIO nicht zufrieden, kann sie sich an den zuständigen Bürgerbeauftragten (Judicial Appointments and Conduct Ombudsman) wenden (siehe https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Der Bürgerbeauftragte ist befugt, das JCIO aufzufordern, eine Beschwerde erneut zu untersuchen, und kann vorschlagen, dass dem Beschwerdeführer eine Entschädigung gezahlt wird, wenn er der Meinung ist, dass dieser durch einen Missstand in der Verwaltung einen Schaden erlitten hat.

([186]) Die Datenschutzerklärung des Lord Chief Justice und des Senior President of Tribunals ist unter folgendem Link abrufbar: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([187]) Die Datenschutzerklärung des Lord Chief Justice von Nordirland ist unter folgendem Link abrufbar: https://judiciaryni.uk/data-privacy.

([188]) Die Datenschutzerklärung für schottische Gerichte und Tribunale ist unter folgendem Link abrufbar: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([189]) Der Data Supervisory Judge gibt der Justiz Leitlinien an die Hand und untersucht Verstöße und/oder Beschwerden im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Gerichte oder natürliche Personen, die im Rahmen ihrer justiziellen Tätigkeit handeln.

([190]) Wird die Beschwerde oder der Verstoß als schwerwiegend erachtet, wird die Angelegenheit an die für richterliche Beschwerden zuständige Stelle, den Judicial Complaints Officer, zur weiteren Untersuchung in Übereinstimmung mit dem Verhaltenskodex für Beschwerden des Lord Chief Justice of Northern Ireland verwiesen. Eine derartige Beschwerde kann unter anderem Folgendes nach sich ziehen: keine weiteren Maßnahmen, Erteilung eines Rates, Schulungs- oder Mentoringmaßnahmen, eine informelle Verwarnung, eine formelle Verwarnung, eine endgültige Verwarnung, eine Einschränkung der Amtsausübung oder die Verweisung an ein Statutory Tribunal. Der Verhaltenskodex für Beschwerden des Lord Chief Justice of Northern Ireland ist unter folgendem Link abrufbar: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf.

([191]) Jede begründete Beschwerde wird vom Data Supervisory Judge untersucht und an den Lord President weitergeleitet; dieser hat die Befugnis, eine Empfehlung, eine formelle Warnung oder einen Verweis auszusprechen, wenn er dies für notwendig erachtet. (Vergleichbare Vorschriften existieren für Mitglieder des Gerichts und sind unter folgendem Link abrufbar: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Rechtsbehelfe*

(115) Um einen angemessenen Schutz und insbesondere die Durchsetzung der Rechte des Einzelnen zu gewährleisten, sollten der betroffenen Person wirksame behördliche und gerichtliche Rechtsbehelfe, einschließlich Schadensersatz, zur Verfügung stehen.

(116) Erstens hat eine betroffene Person das Recht auf Beschwerde beim Information Commissioner, wenn sie der Ansicht ist, dass im Zusammenhang mit sie betreffenden personenbezogenen Daten ein Verstoß gegen Teil 3 des DPA 2018 ([192]) vorliegt. Wie in den Erwägungsgründen 100 und 109 beschrieben, hat der Information Commissioner die Befugnis, die Einhaltung des DPA 2018 durch den Verantwortlichen und den Auftragsverarbeiter zu bewerten, sie im Falle der Nichteinhaltung aufzufordern, notwendige Maßnahmen zu ergreifen bzw. zu unterlassen, und Geldbußen zu verhängen.

(117) Zweitens besteht gemäß dem DPA 2018 das Recht auf einen Rechtsbehelf gegen den Information Commissioner. Versäumt es der Information Commissioner, eine von der betroffenen Person eingereichte Beschwerde angemessen weiterzuverfolgen („progress") ([193]), so hat der Beschwerdeführer Zugang zu einem gerichtlichen Rechtsbehelf; er kann bei einem First-tier Tribunal ([194]) beantragen, den Information Commissioner anzuweisen, geeignete Schritte zur Beantwortung der Beschwerde zu unternehmen oder den Beschwerdeführer über den Stand der Bearbeitung der Beschwerde zu informieren ([195]). Darüber hinaus kann jede Person, die vom Commissioner einen der genannten Bescheide (Informations-, Bewertungs-, Durchsetzungs- oder Bußgeldbescheid) erhält, beim First-tier Tribunal Widerspruch dagegen einlegen. Ist das Gericht der Ansicht, dass der Beschluss des Commissioner rechtswidrig ist oder dieser seinen Ermessensspielraum anders hätte nutzen sollen, muss es der Berufung stattgeben oder einen anderen Bescheid oder Beschluss ersetzen, den der Information Commissioner hätte erlassen können ([196]).

(118) Drittens können natürliche Personen gemäß Paragraf 167 DPA 2018 unmittelbar vor den Gerichten Rechtsbehelfe gegen Verantwortliche und Auftragsverarbeiter einlegen. Wenn ein Gericht aufgrund einer Beschwerde einer betroffenen Person zu der Überzeugung gelangt, dass eine Verletzung der Rechte der betroffenen Person gemäß den Datenschutzvorschriften vorliegt, kann es anordnen, dass der Verantwortliche oder ein Auftragsverarbeiter, der im Namen dieses Verantwortlichen handelt, die in der Anordnung genannten Maßnahmen zu ergreifen oder zu unterlassen hat. Darüber hinaus hat gemäß Paragraf 169 DPA 2018 jede Person, die wegen Verstoßes gegen eine Anforderung der Datenschutzvorschriften (einschließlich Teil 3 des DPA 2018), mit Ausnahme der UK GDPR, einen Schaden erlitten hat, Anspruch auf Ersatz dieses Schadens durch den Verantwortlichen oder Auftragsverarbeiter, es sei denn, der Verantwortliche bzw. der Auftragsverarbeiter weist nach, dass er in keiner Weise für den Vorfall verantwortlich ist, der den Schaden verursacht hat. Als Schaden gilt sowohl ein finanzieller als auch ein nichtfinanzieller Schaden, wie z. B. seelisches Leid.

(119) Viertens kann jede Person, die der Ansicht ist, dass ihre Rechte, einschließlich der Rechte auf Privatsphäre und Datenschutz, von Behörden verletzt wurden, vor den Gerichten des Vereinigten Königreichs auf der Grundlage des Human Rights Act 1998 einen Rechtsbehelf einlegen. Bei den Verantwortlichen im Sinne von Teil 3 des DPA 2018, d. h. den zuständigen Behörden, handelt es sich immer um staatliche Stellen im Sinne des Human Rights Act 1998. Ist eine Person der Ansicht, dass eine Behörde in einer Weise gehandelt hat (oder zu handeln beabsichtigt), die mit einem Konventionsrecht unvereinbar und folglich gemäß Paragraf 6 Absatz 1 des Human Rights Act 1998 rechtswidrig ist, kann sie die Behörde vor dem zuständigen Gericht verklagen oder sich in einem Gerichtsverfahren auf die betreffenden Rechte berufen, wenn sie Opfer der rechtswidrigen Handlung ist (oder wäre) ([197]).

([192]) Paragraf 165 DPA 2018.

([193]) In Paragraf 166 DPA 2018 sind konkret folgende Situationen genannt: a) der Information Commissioner unternimmt keine angemessenen Schritte zur Beantwortung der Beschwerde, b) der Information Commissioner unterrichtet den Beschwerdeführer nicht vor Ablauf des Zeitraums von drei Monaten ab dem Eingang der Beschwerde beim Information Commissioner über den Stand ihrer Bearbeitung oder ihr Ergebnis, oder c) der Information Commissioner schließt die Prüfung der Beschwerde nicht innerhalb dieses Zeitraums ab und versäumt es, den Beschwerdeführer hierüber innerhalb eines weiteren Zeitraums von drei Monaten zu unterrichten.

([194]) Das First-tier Tribunal ist das Gericht, das für die Behandlung von Widersprüchen gegen Entscheidungen von staatlichen Regulierungsbehörden zuständig ist. Im Falle von Entscheidungen des Information Commissioner ist die zuständige Kammer die General Regulatory Chamber, die für das gesamte Vereinigte Königreich zuständig ist.

([195]) Paragraf 166 DPA 2018.

([196]) Paragrafen 161 und 162 DPA 2018.

([197]) Siehe die Rechtssache Brown/Commissioner of the Met (2016), in der das Gericht im Rahmen einer gegen die Polizei erhobenen Klage der Klägerin in der Datenschutzfrage Wiedergutmachung gewährte. Das Gericht entschied zugunsten der Klägerin und bestätigte ihre Ansprüche wegen Verstoßes gegen die Verpflichtungen aus dem DPA 1998, wegen Verstoßes gegen den Human Rights Act 1998 (und das damit verbundene Recht aus Artikel 8 EMRK) und wegen des Missbrauchs privater Informationen (der Beklagte räumte letztlich ein, gegen den DPA und die EMRK verstoßen zu haben, sodass sich das Urteil mit der Frage nach der angemessenen Abhilfe befasste). Das Gericht sprach der Klägerin eine finanzielle Entschädigung für die genannten Verstöße zu.

(120) Befindet das Gericht eine Handlung einer Behörde für rechtswidrig, so kann es im Rahmen seiner Befugnisse den Rechtsbehelf oder die Abhilfe gewähren oder die Anordnung treffen, die es für gerecht und angemessen hält ([198]). Des Weiteren kann das Gericht eine Bestimmung des Primärrechts für unvereinbar mit einem durch die EMRK verbürgten Recht erklären.

(121) Schließlich kann eine natürliche Person, wenn alle nationalen Rechtsmittel ausgeschöpft wurden, vor dem Europäischen Gerichtshof für Menschenrechte aufgrund der Verletzung ihrer nach der Europäischen Menschenrechtskonvention garantierten Rechte einen Rechtsbehelf einlegen.

2.6. **Weitergabe**

(122) Nach britischem Recht ist die Weitergabe von Daten durch eine Strafverfolgungsbehörde an andere britische Behörden zu anderen Zwecken als denen, für die sie ursprünglich erhoben wurden (die sogenannte Weitergabe — „onward sharing") unter bestimmten Voraussetzungen gestattet.

(123) Ähnlich zu den Bestimmungen des Artikels 4 Absatz 2 der Richtlinie (EU) 2016/680 dürfen nach Paragraf 36 Absatz 3 DPA 2018 personenbezogene Daten, die von einer zuständigen Behörde für einen Strafverfolgungszweck erhoben wurden, für jeden anderen Strafverfolgungszweck weiterverarbeitet werden (sei es durch den ursprünglichen Verantwortlichen oder durch einen anderen Verantwortlichen), sofern der Verantwortliche gesetzlich befugt ist, Daten für diesen anderen Zweck zu verarbeiten, und sofern die Verarbeitung für diesen Zweck erforderlich und verhältnismäßig ist ([199]). In diesem Fall gelten für die Verarbeitung durch die empfangende Behörde alle in Teil 3 des DPA 2018 vorgesehenen und vorstehend analysierten Garantien.

(124) Die britische Rechtsordnung umfasst eine Reihe von Gesetzen, nach denen die Weitergabe ausdrücklich gestattet ist. Dabei handelt es sich insbesondere um i) das Gesetz über die digitale Wirtschaft (Digital Economy Act) von 2017, das den Informationsaustausch zwischen Behörden für verschiedene Zwecke erlaubt, z. B. im Falle eines Betrugs zulasten des öffentlichen Sektors, der mit einem Schaden oder möglichen Schaden für eine Behörde einhergehen würde ([200]), oder im Falle einer Schuld gegenüber einer Behörde oder der Krone ([201]), ii) das Straf- und Gerichtsgesetz (Crime and Courts Act) von 2013, das den Austausch von Informationen mit der National Crime Agency (NCA) ([202]) zur Bekämpfung, Ermittlung und Verfolgung von schwerer und organisierter Kriminalität gestattet, iii) das Gesetz über schwere Straftaten (Serious Crime Act) von 2007, nach dem Behörden zum Zwecke der Betrugsverhinderung ([203]) Informationen an Betrugsbekämpfungsstellen weitergeben dürfen.

(125) Diese Gesetze sehen ausdrücklich vor, dass die Weitergabe von Informationen in Übereinstimmung mit den im DPA 2018 festgelegten Vorschriften erfolgen muss. Darüber hinaus hat das College of Policing Leitlinien über zugelassene dienstliche Vorgehensweisen beim Austausch von Informationen (Authorised Professional Practice on Information Sharing) ([204]) herausgegeben, um die Polizei bei der Einhaltung ihrer Datenschutzverpflichtungen gemäß der UK GDPR, dem DPA und dem Human Rights Act 1998 zu unterstützen. Die Frage, ob der betreffende Informationsaustausch den geltenden Datenschutzvorschriften entspricht, kann selbstverständlich der gerichtlichen Überprüfung unterliegen ([205]).

(126) Darüber hinaus ist im DPA 2018 ähnlich wie in Artikel 9 der Richtlinie (EU) 2016/680 vorgesehen, dass personenbezogene Daten, die für einen Strafverfolgungszweck erhoben wurden, für einen anderen Zweck als den der Strafverfolgung verarbeitet werden dürfen, sofern die Verarbeitung gesetzlich zulässig ist ([206]). Diese Art der Datenweitergabe bezieht sich auf die folgenden beiden Szenarien: 1. Eine Strafverfolgungsbehörde gibt Daten an eine andere Durchsetzungsbehörde, ausgenommen Nachrichtendienste, weiter (z. B. an eine Finanz- oder

([198]) Paragraf 8 Absatz 1 des Human Rights Act 1998.
([199]) Paragraf 36 Absatz 3 DPA 2018.
([200]) Paragraf 56 des Digital Economy Act 2017, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2017/30/contents.
([201]) Paragraf 48 des Digital Economy Act 2017.
([202]) Paragraf 7 des Crime and Courts Act 2013, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2013/22/contents.
([203]) Paragraf 68 des Serious Crime Act 2007, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2007/27/contents.
([204]) Authorised Professional Practice on Information Sharing, abrufbar unter folgendem Link: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.
([205]) Siehe z. B. die Rechtssache *M/the Chief Constable of Sussex Police*, [2019] EWHC 975 (Admin), in der der High Court ersucht wurde, den Datenaustausch zwischen der Polizei und einer Partnerschaft zur Reduzierung der Wirtschaftskriminalität (Business Crime Reduction Partnership — BCRP) zu prüfen, einer Organisation, die befugt ist, Ausschlussverfahren zu verwalten, mit denen Personen das Betreten der Geschäftsräume ihrer Mitglieder untersagt wird. Das Gericht überprüfte die Weitergabe der Daten, die auf der Grundlage einer Vereinbarung zum Schutz der Öffentlichkeit und zur Verhinderung von Straftaten erfolgte, und gelangte letztlich zu dem Schluss, dass die meisten Aspekte der Weitergabe rechtmäßig waren, mit Ausnahme des Austauschs einiger sensibler Informationen zwischen der Polizei und der BCRP. Ein weiteres Beispiel ist die Rechtssache *Cooper/NCA* [2019] EWCA Civ 16, in der der Court of Appeal ein Urteil über den Datenaustausch zwischen der Polizei und der Serious Organised Crime Agency (SOCA), einer Strafverfolgungsbehörde, die derzeit Teil der NCA ist, bestätigte.
([206]) Paragraf 36 Absatz 4 DPA 2018.

Steuerbehörde, eine Wettbewerbsbehörde oder ein Jugendamt). 2. Eine Strafverfolgungsbehörde gibt Daten an einen Nachrichtendienst weiter. Im ersten Szenario fällt die Verarbeitung personenbezogener Daten sowohl in den Anwendungsbereich der UK GDPR als auch unter Teil 2 des DPA 2018. Wie in dem auf Grundlage der Verordnung (EU) 2016/679 erlassenen Beschluss XXX dargelegt, bieten die in der UK GDPR und in Teil 2 des DPA 2018 festgelegten Garantien ein Schutzniveau, das dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist ([207]).

(127) Im zweiten Szenario, das die Weitergabe von durch eine Strafverfolgungsbehörde erhobenen Daten an einen Nachrichtendienst für Zwecke der nationalen Sicherheit betrifft, bildet das Gesetz zur Terrorismusbekämpfung (Counter Terrorism Act) von 2008 die Rechtsgrundlage für die Weitergabe ([208]). Nach dem Counter Terrorism Act 2008 kann jede Person Informationen an einen der Nachrichtendienste zum Zwecke der Erfüllung einer der Aufgaben dieses Dienstes weitergeben, einschließlich für Zwecke der „nationalen Sicherheit".

(128) Was die Bedingungen anbelangt, unter denen Daten für Zwecke der nationalen Sicherheit weitergegeben werden können, so sind die Möglichkeiten der Nachrichtendienste zum Erhalt von Daten gemäß dem Gesetz über Nachrichtendienste (Intelligence Services Act) und dem Gesetz über Sicherheitsdienste (Security Services Act) auf das zur Erfüllung ihrer gesetzlichen Aufgaben erforderliche Maß beschränkt. Zuständige Behörden, die in den Anwendungsbereich von Teil 3 des DPA 2018 fallen und Daten mit den Nachrichtendiensten austauschen möchten, müssen zusätzlich zu den gesetzlichen Aufgaben der Behörden, die im Intelligence Services Act und im Security Services Act festgelegt sind, eine Reihe von Faktoren/Einschränkungen berücksichtigen ([209]). In Paragraf 20 des Counter Terrorism Act 2008 ist klar geregelt, dass jeder Datenaustausch gemäß Paragraf 19 dieses Gesetzes grundsätzlich auch den Datenschutzvorschriften entsprechen muss, was bedeutet, dass sämtliche Einschränkungen und Anforderungen des DPA 2018 Anwendung finden. Darüber hinaus sind Strafverfolgungsbehörden und Nachrichtendienste staatliche Stellen im Sinne des Human Rights Act 1998 und müssen somit sicherstellen, dass sie im Einklang mit den durch die EMRK garantierten Rechten einschließlich Artikel 8 handeln. Anders ausgedrückt bedeuten diese Vorgaben, dass die Weitergabe von Daten zwischen Strafverfolgungsbehörden und Nachrichtendiensten grundsätzlich mit den Datenschutzvorschriften und den Bestimmungen der EMRK in Einklang stehen muss.

(129) Die Verarbeitung personenbezogener Daten durch die Nachrichtendienste, die diese zu Zwecken der nationalen Sicherheit bei Strafverfolgungsbehörden bezogen oder von diesen erhalten haben, ist an eine Reihe von Bedingungen und Garantien geknüpft ([210]). Teil 4 des DPA 2018 gilt für jede durch Nachrichtendienste oder in deren Namen durchgeführte Verarbeitung. Darin sind die wesentlichen Datenschutzgrundsätze (Rechtmäßigkeit,

([207]) Durchführungsbeschluss der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, C(2021) 4800.

([208]) Paragraf 19 des Counter Terrorism Act 2008, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) In Paragraf 2 Absatz 2 des Intelligence Service Act 1994 (siehe https://www.legislation.gov.uk/ukpga/1994/13/contents) heißt es wie folgt: „Der Leiter des Nachrichtendienstes ist für die Leistungsfähigkeit dieses Dienstes verantwortlich, und es ist seine Pflicht, dafür zu sorgen, — a) dass Vorkehrungen getroffen werden, um sicherzustellen, dass der Nachrichtendienst nur dann Informationen erhält, wenn dies für die ordnungsgemäße Erfüllung seiner Aufgaben erforderlich ist, und dass er nur dann Informationen weitergibt, wenn dies — i) für diesen Zweck, ii) im Interesse der nationalen Sicherheit, iii) für die Verhütung oder Aufdeckung von schweren Straftaten oder iv) für die Zwecke eines Strafverfahrens erforderlich ist, und b) dass der Nachrichtendienst keine Maßnahmen zur Förderung der Interessen einer politischen Partei des Vereinigten Königreichs ergreift"; in Paragraf 2 Absatz 2 des Security Service Act 1989 (siehe https://www.legislation.gov.uk/ukpga/1989/5/contents) heißt es hingegen wie folgt: „Der Generaldirektor ist für die Leistungsfähigkeit dieses Dienstes verantwortlich, und es ist seine Pflicht, dafür zu sorgen, — a) dass Vorkehrungen getroffen werden, mit denen sichergestellt wird, dass der Dienst nur dann Informationen erhält, wenn dies für die ordnungsgemäße Erfüllung seiner Aufgaben erforderlich ist, und dass er nur dann Informationen weitergibt, wenn dies für diesen Zweck oder für die Verhütung oder Aufdeckung von schweren Straftaten oder für die Zwecke eines Strafverfahrens erforderlich ist, und b) dass der Dienst keine die Interessen einer politischen Partei des Vereinigten Königreichs begünstigende Maßnahmen ergreift, und c) dass mit dem Generaldirektor der National Crime Agency abgestimmte Vorkehrungen getroffen werden, um die Tätigkeiten des Dienstes gemäß Paragraf 1 Absatz 4 dieses Gesetzes mit den Tätigkeiten der Polizeikräfte, der National Crime Agency und anderer Strafverfolgungsbehörden zu koordinieren."

([210]) Die Garantien und Einschränkungen bezüglich der Befugnisse der Nachrichtendienste sind auch im Gesetz über Ermittlungsbefugnisse (Investigatory Powers Act) von 2016 geregelt, das zusammen mit den im Jahr 2000 für England, Wales und Nordirland einerseits und für Schottland andererseits verabschiedeten Gesetzen über die Regelung der Ermittlungsbefugnisse (Regulation of Investigatory Powers Act und Regulation of Investigatory Powers (Scotland) Act) die Rechtsgrundlage für die Wahrnehmung dieser Befugnisse bildet. Diese Befugnisse sind jedoch im Zusammenhang mit der „Weitergabe" unerheblich, weil sie sich auf die direkte Erhebung personenbezogener Daten durch Nachrichtendienste erstrecken. Eine Bewertung der den Nachrichtendiensten im Rahmen des Investigatory Powers Act verliehenen Befugnisse ist dem Durchführungsbeschluss der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, C(2021) 4800 zu entnehmen.

Verarbeitung nach Treu und Glauben sowie Transparenz ([211]), Zweckbindung ([212]), Datenminimierung ([213]), Genauigkeit ([214]); Speicherbegrenzung ([215]) und Sicherheit ([216])), die Bedingungen für die Verarbeitung besonderer Kategorien von Daten ([217]), die Rechte der betroffenen Person ([218]), die Verpflichtung zum Datenschutz durch Technikgestaltung ([219]) und die internationale Übermittlung personenbezogener Daten ([220]) geregelt.

(130) Gleichzeitig ist in Paragraf 110 DPA 2018 eine Ausnahme von bestimmten Bestimmungen von Teil 4 des DPA 2018 vorgesehen, wenn eine solche Ausnahme zum Schutz der nationalen Sicherheit erforderlich ist. In Paragraf 110 Absatz 2 DPA 2018 sind die Bestimmungen aufgeführt, von denen eine Ausnahme zulässig ist. Dazu zählen die Datenschutzgrundsätze (mit Ausnahme des Grundsatzes der Rechtmäßigkeit), die Rechte der betroffenen Person, die Verpflichtung, den Information Commissioner über eine Datenschutzverletzung zu informieren, die Kontrollbefugnisse des Information Commissioner gemäß internationalen Verpflichtungen, bestimmte Durchsetzungsbefugnisse des Information Commissioner, die Bestimmungen, nach denen bestimmte Datenschutzverletzungen eine Straftat darstellen, und die Bestimmungen über besondere Zwecke der Verarbeitung, wie journalistische, wissenschaftliche oder künstlerische Zwecke. Diese Ausnahme kann auf der Grundlage einer Einzelfallprüfung in Anspruch genommen werden ([221]). Wie von den britischen Behörden erläutert und durch die Rechtsprechung der britischen Gerichte bestätigt, „muss ein Verantwortlicher berücksichtigen, welche konkreten Folgen die Einhaltung der jeweiligen Datenschutzbestimmung für die nationale Sicherheit oder Verteidigung hätte; ferner muss er berücksichtigten, ob er die übliche Vorschrift nach vernünftigem Ermessen befolgen könnte, ohne die nationale Sicherheit oder Verteidigung zu beeinträchtigen“ ([222]). Das ICO beurteilt im Rahmen seiner Aufsichtsfunktion, ob die Ausnahmeregelung ordnungsgemäß angewandt wurde ([223]).

([211]) Nach Paragraf 86 Absatz 6 DPA 2018 muss bei der Prüfung dessen, ob eine Verarbeitung nach Treu und Glauben sowie transparent erfolgt, berücksichtigt werden, auf welche Weise die Daten erhoben wurden. In diesem Sinne ist das Erfordernis der Verarbeitung nach Treu und Glauben und der Transparenz erfüllt, wenn die Daten von einer Person bezogen werden, die rechtmäßig befugt oder verpflichtet ist, sie bereitzustellen.

([212]) Nach Paragraf 87 DPA 2018 müssen die Zwecke der Verarbeitung genau festgelegt, eindeutig und rechtmäßig sein. Die Daten dürfen nicht in einer Weise verarbeitet werden, die mit den Zwecken, für die sie erhoben wurden, unvereinbar ist. Gemäß Paragraf 87 Absatz 3 ist eine vereinbare Weiterverarbeitung personenbezogener Daten nur zulässig, wenn der Verantwortliche gesetzlich befugt ist, die Daten für diesen Zweck zu verarbeiten, und die Verarbeitung für diesen anderen Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung wird als vereinbar erachtet, wenn es sich um eine Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken handelt, die geeigneten Garantien unterliegt (Paragraf 87 Absatz 4 DPA 2018).

([213]) Die personenbezogenen Daten müssen dem Zweck angemessen und dafür erheblich sein und dürfen das notwendige Maß nicht überschreiten (Paragraf 88 DPA 2018).

([214]) Die personenbezogenen Daten müssen sachlich richtig und auf dem neuesten Stand sein (Paragraf 89 DPA 2018).

([215]) Die personenbezogenen Daten dürfen nicht länger als erforderlich aufbewahrt werden (Paragraf 90 DPA 2018).

([216]) Der sechste Datenschutzgrundsatz besagt, dass personenbezogene Daten in einer Weise verarbeitet werden müssen, die geeignete Sicherheitsmaßnahmen in Bezug auf die mit der Verarbeitung personenbezogener Daten verbundenen Risiken umfasst. Zu diesen Risiken zählen unter anderem (aber nicht ausschließlich) der unbeabsichtigte oder unbefugte Zugang zu personenbezogenen Daten, Vernichtung, Verlust, Verwendung oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, von personenbezogenen Daten oder die unbeabsichtigte oder unbefugte Offenlegung von personenbezogenen Daten (Paragraf 91 DPA 2018). Des Weiteren ist in Paragraf 107 vorgesehen, dass jeder Verantwortliche zum einen geeignete Sicherheitsmaßnahmen ergreifen muss, die den mit der Verarbeitung personenbezogener Daten verbundenen Risiken angemessen sind, und dass jeder Verantwortliche und jeder Auftragsverarbeiter zum anderen bei einer automatisierten Verarbeitung vorbeugende oder schadensbegrenzende Maßnahmen auf der Grundlage einer Risikobewertung ergreifen muss.

([217]) Paragraf 86 Absatz 2 Buchstabe b und Anhang 10 des DPA 2018.

([218]) Teil 4 Kapitel 3 des DPA 2018, insbesondere die Rechte auf Auskunft, auf Berichtigung und Löschung, auf Widerspruch gegen die Verarbeitung und darauf, nicht einer automatisierten Entscheidungsfindung unterworfen zu werden, auf Eingriff in die automatisierte Entscheidungsfindung und darauf, über die Entscheidungsfindung unterrichtet zu werden. Darüber hinaus muss der Verantwortliche die betroffene Person über die Verarbeitung ihrer personenbezogenen Daten informieren.

([219]) Paragraf 103 DPA 2018.

([220]) Paragraf 109 DPA 2018. Übermittlungen personenbezogener Daten an internationale Organisationen oder Länder außerhalb des Vereinigten Königreichs sind möglich, wenn die Übermittlung eine notwendige und verhältnismäßige Maßnahme darstellt, die zur Erfüllung der gesetzlichen Aufgaben des Verantwortlichen durchgeführt wird, oder für andere Zwecke, die in spezifischen Paragrafen des Gesetzes über den Security Service (Security Service Act) von 1989 und des Gesetzes über die Nachrichtendienste (Intelligence Services Act) von 1994 vorgesehen sind.

([221]) Siehe Rechtssache Baker/Secretary of State for the Home Department, [2001] UKIT NSA2 („Baker/Secretary of State“).

([222]) Explanatory Framework for Adequacy Discussions, Section H: National Security Data Protection and Investigatory Powers Framework, S. 15 und 16, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Siehe auch die Rechtssache Baker/Secretary of State (siehe Fußnote 220); darin hob das Tribunal eine vom Innenminister ausgestellte nationale Sicherheitsbescheinigung, in der die Anwendung der Ausnahme für Zwecke der nationalen Sicherheit bestätigt worden war, mit der Begründung auf, dass es keinen Grund gab, eine pauschale Ausnahme von der Pflicht zur Auskunftserteilung vorzusehen und dass die Zulassung einer solchen Ausnahme in allen Fällen ohne Einzelfallprüfung über das zum Schutz der nationalen Sicherheit erforderliche und verhältnismäßige Maß hinausging.

([223]) Siehe die Absichtserklärung zwischen dem ICO und der UK Intelligence Community (UKIC), nach der „sich das ICO nach Erhalt einer Beschwerde von einer betroffenen Person davon vergewissern sollte, dass die Angelegenheit korrekt behandelt und eine etwaige Ausnahme gegebenenfalls angemessen angewandt wurde“ (Absichtserklärung zwischen dem Büro des Information Commissioner und der UK Intelligence Community, Nummer 16, abrufbar unter folgendem Link: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Darüber hinaus sieht Paragraf 79 des DPA 2018 im Hinblick auf die Möglichkeit, die vorstehend genannten Rechte zum Schutz der „nationalen Sicherheit" einzuschränken, die Möglichkeit vor, dass ein Verantwortlicher eine von einem Kabinettsminister oder dem Generalstaatsanwalt unterzeichnete Bescheinigung beantragt, in der bestätigt wird, dass eine Einschränkung dieser Rechte eine notwendige und verhältnismäßige Maßnahme zum Schutz der nationalen Sicherheit darstellt oder zu irgendeinem Zeitpunkt darstellte ([224]). Die britische Regierung hat Leitlinien zu nationalen Sicherheitsbescheinigungen gemäß dem DPA 2018 herausgegeben, in denen ausdrücklich betont wird, dass jede Einschränkung der Rechte betroffener Personen aus Gründen des Schutzes der nationalen Sicherheit verhältnismäßig und notwendig sein muss ([225]). Alle nationalen Sicherheitsbescheinigungen sind auf der Website des ICO zu veröffentlichen ([226]).

(132) Die Bescheinigung sollte für einen festen Zeitraum von höchstens fünf Jahren gültig sein und regelmäßig von der Exekutive überprüft werden ([227]). In einer Bescheinigung wird angegeben, welche personenbezogenen Daten oder Kategorien personenbezogener Daten Gegenstand der jeweiligen Ausnahme sind und für welche Bestimmungen des DPA 2018 die Ausnahme gilt ([228]).

(133) Es wird ausdrücklich darauf hingewiesen, dass die nationalen Sicherheitsbescheinigungen keine zusätzliche Möglichkeit vorsehen, Datenschutzrechte aus Gründen der nationalen Sicherheit einzuschränken. Mit anderen Worten: Der Verantwortliche oder der Auftragsverarbeiter kann sich nur dann auf eine Bescheinigung berufen, wenn er zu dem Schluss gelangt, dass es notwendig ist, die Ausnahme zum Schutz der nationalen Sicherheit in Anspruch zu nehmen, die auf Einzelfallbasis anzuwenden ist. Selbst wenn eine nationale Sicherheitsbescheinigung auf die betreffende Angelegenheit anwendbar ist, kann das ICO untersuchen, ob die Inanspruchnahme der Ausnahme zum Schutz der nationalen Sicherheit in einem bestimmten Fall gerechtfertigt war oder nicht ([229]).

(134) Jede Person, die von der Ausstellung der Bescheinigung unmittelbar betroffen ist, kann beim Upper Tribunal ([230]) Rechtsmittel gegen die Bescheinigung ([231]) einlegen oder, wenn in der Bescheinigung bestimmte Daten in Form einer allgemeinen Beschreibung ausgewiesen werden, die Anwendung der Bescheinigung auf diese Daten ([232]) anfechten.

(135) Das Gericht überprüft daraufhin die Entscheidung zur Ausstellung einer Bescheinigung und entscheidet, ob berechtigte Gründe für die Ausstellung der Bescheinigung vorlagen ([233]). Dabei kann das Gericht eine Vielzahl unterschiedlicher Aspekte berücksichtigen, darunter die Notwendigkeit, Verhältnismäßigkeit und Rechtmäßigkeit, jeweils unter Berücksichtigung der Folgen für die Rechte betroffener Personen und Abwägung der Notwendigkeit, die nationale Sicherheit zu schützen. Das Tribunal kann zu dem Schluss kommen, dass die Bescheinigung nicht für bestimmte personenbezogene Daten gilt, die Gegenstand der Beschwerde sind ([234]).

([224]) Im DPA 2018 ist die Möglichkeit aufgehoben, eine Bescheinigung nach Paragraf 28 Absatz 2 des Data Protection Act 1998 auszustellen. Es besteht jedoch weiterhin die Möglichkeit, „alte Bescheinigungen" auszustellen, insofern im Rahmen des Gesetzes von 1998 eine historische Anfechtung erfolgt (siehe Nummer 17 in Anhang 20 Teil 5 des DPA 2018). Es scheint sich hierbei jedoch um eine Möglichkeit zu handeln, die sehr selten eintritt und nur in begrenzten Fällen gilt, etwa wenn eine betroffene Person die Verwendung der Ausnahme zum Schutz der nationalen Sicherheit in Bezug auf eine Verarbeitung durch eine öffentliche Behörde anfechtet, die die Verarbeitung im Rahmen des Gesetzes von 1998 durchgeführt hat. Es ist zu beachten, dass in diesen Fällen Paragraf 28 des DPA 1998 in seiner Gesamtheit Anwendung findet, einschließlich der Möglichkeit der betroffenen Person, die Bescheinigung anzufechten. Aktuell gibt es keine gemäß DPA 1998 ausgestellten nationalen Sicherheitsbescheinigungen.

([225]) United Kingdom Government Guidance on National Security Certificates under the Data Protection Act 2018, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

([226]) Nach Paragraf 130 DPA 2018 kann das ICO entscheiden, den Wortlaut oder Teile des Wortlauts der Bescheinigung nicht zu veröffentlichen, wenn dies den nationalen Sicherheitsinteressen oder dem öffentlichen Interesse zuwiderläuft oder die Sicherheit einer Person aufs Spiel setzen könnte. In diesen Fällen veröffentlicht das ICO jedoch den Umstand, dass die Bescheinigung ausgestellt worden ist.

([227]) United Kingdom Government Guidance on National Security Certificates, Nummer 15, siehe Fußnote 225.

([228]) United Kingdom Government Guidance on National Security Certificates, Nummer 5, Fußnote 225.

([229]) Gemäß Paragraf 102 DPA 2018 muss der Verantwortliche in der Lage sein, nachzuweisen, dass er die Bestimmungen des DPA 2018 eingehalten hat. Das bedeutet, dass ein Nachrichtendienst gegenüber dem ICO nachweisen müsste, dass er bei der Inanspruchnahme der Ausnahme die besonderen Umstände des jeweiligen Falles berücksichtigt hat. Das ICO veröffentlicht zudem eine Auflistung der nationalen Sicherheitsbescheinigungen, die unter folgendem Link abrufbar ist: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Das Upper Tribunal ist für Beschwerden gegen Entscheidungen der unteren Verwaltungsgerichte zuständig und hat eine besondere Zuständigkeit für direkte Beschwerden gegen die Beschlüsse bestimmter Regierungsstellen.

([231]) Paragraf 111 Absatz 3 DPA 2018.

([232]) Paragraf 111 Absatz 5 DPA 2018.

([233]) In der Rechtssache Baker/Secretary of State (siehe Fußnote 221) hob das Information Tribunal eine vom Innenminister ausgestellte nationale Sicherheitsbescheinigung mit der Begründung auf, dass es keinen Grund gab, eine pauschale Ausnahme von der Pflicht zur Auskunftserteilung vorzusehen und dass die Zulassung einer solchen Ausnahme in allen Fällen ohne Einzelfallprüfung über das zum Schutz der nationalen Sicherheit erforderliche und verhältnismäßige Maß hinausging.

([234]) United Kingdom Government Guidance on National Security Certificates, Nummer 25, Fußnote 225.

(136) Weitere mögliche Einschränkungen betreffen diejenigen, die nach Anhang 11 des DPA 2018 für gewisse Bestimmungen von Teil 4 des DPA 2018 ([235]) gelten, um den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses oder geschützter Interessen zu gewährleisten, wie zum Beispiel die parlamentarischen Vorrechte, die Vertraulichkeit der anwaltlichen Korrespondenz, die Durchführung von Gerichtsverfahren oder die Schlagkraft der Streitkräfte. Die Anwendung dieser Bestimmungen ist entweder bei bestimmten Kategorien von Informationen („class based") ausgenommen, oder ist in dem Umfang ausgenommen, in dem die Anwendung dieser Bestimmungen das geschützte Interesse voraussichtlich beeinträchtigen würde („prejudice based") ([236]). Die Ausnahme aufgrund einer voraussichtlichen Beeinträchtigung des geschützten Interesses darf nur in dem Umfang in Anspruch genommen werden, in dem die genannte Datenschutzbestimmung das in Rede stehende spezifische Interesse voraussichtlich beeinträchtigen würde. Die Inanspruchnahme einer Ausnahme muss somit immer durch Verweis auf die im Einzelfall zu erwartende Beeinträchtigung begründet werden. Die Ausnahme für bestimmte Kategorien von Informationen darf nur in Bezug auf die spezielle, eng gefasste Kategorie von Informationen in Anspruch genommen werden, für die die Ausnahme gewährt wird. Diese sind im Hinblick auf den Zweck und die Wirkung mit mehreren Ausnahmen von der UK GDPR (nach Anhang 2 des DPA 2018) vergleichbar, die wiederum den in Artikel 23 DSGVO genannten Ausnahmen entsprechen.

(137) Aus den vorstehenden Ausführungen ergibt sich, dass in den geltenden Rechtsvorschriften des Vereinigten Königreichs Einschränkungen und Bedingungen festgelegt sind, die in diesem Sinne auch von den Gerichten und vom Information Commissioner ausgelegt werden, und mit denen gewährleistet wird, dass diese Ausnahmen und Einschränkungen auf das zum Schutz der nationalen Sicherheit erforderliche und verhältnismäßige Maß begrenzt bleiben.

(138) Die Verarbeitung personenbezogener Daten durch die Nachrichtendienste gemäß Teil 4 des DPA 2018 wird durch den Information Commissioner beaufsichtigt ([237]).

(139) Die allgemeinen Aufgaben des Information Commissioner im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Nachrichtendienste gemäß Teil 4 des DPA 2018 sind in Anhang 13 des DPA 2018 festgelegt. Zu seinen Aufgaben gehören unter anderem insbesondere die Überwachung und Durchsetzung der Bestimmungen von Teil 4 des DPA 2018, die Sensibilisierung der Öffentlichkeit, die Beratung des Parlaments, der Regierung und anderer Einrichtungen zu rechtlichen und administrativen Maßnahmen, die Förderung des Bewusstseins der Verantwortlichen und Auftragsverarbeiter für ihre Pflichten, die Aufklärung betroffener Personen über die Ausübung der Rechte betroffener Personen und die Durchführung von Untersuchungen.

(140) Wie im Hinblick auf Teil 3 des DPA 2018 ist der Information Commissioner befugt, Verantwortliche oder Auftragsverarbeiter auf einen mutmaßlichen Verstoß hinzuweisen, Warnungen dahin gehend auszusprechen, dass eine Verarbeitung voraussichtlich gegen Vorschriften verstößt, und Verweise zu erteilen, wenn der Verstoß bestätigt wird. Ferner kann er Durchsetzungs- und Bußgeldbescheide für Verstöße gegen bestimmte Bestimmungen des Rechtsaktes erteilen ([238]). Anders als bei anderen Teilen des DPA 2018 kann der Information Commissioner jedoch keinen Bewertungsbescheid an eine nationale Sicherheitsbehörde erteilen ([239]).

(141) Darüber hinaus sieht Paragraf 110 DPA 2018 bezüglich der Ausübung bestimmter Befugnisse des Information Commissioner eine Ausnahme vor, wenn dies zum Schutz der nationalen Sicherheit erforderlich ist. Dies betrifft die Befugnis des Information Commissioner, Bescheide (Informations-, Bewertungs-, Durchsetzungs- und

([235]) Dies umfasst: i) die Datenschutzgrundsätze nach Teil 4, mit Ausnahme der Rechtmäßigkeit der Verarbeitung im Rahmen des ersten Grundsatzes und des Umstands, dass die Verarbeitung eine der in den Anhängen 9 und 10 dargelegten einschlägigen Voraussetzungen erfüllen muss, ii) die Rechte betroffener Personen, und iii) die Pflichten im Zusammenhang mit der Meldung von Verletzungen des Schutzes personenbezogener Daten an das ICO.

([236]) Dem UK Explanatory Framework zufolge gelten folgende Ausnahmen als „class based": i) Informationen über die Verleihung königlicher Ehren und Würden, ii) Vertraulichkeit der anwaltlichen Korrespondenz, iii) vertrauliche Beschäftigungs- oder Aus- und Weiterbildungszeugnisse und iv) Prüfungsarbeiten und -zensuren. Folgende Sachverhalte fallen unter die als „preference based" geltenden Ausnahmen: i) Verhütung oder Aufdeckung von Straftaten, Ergreifung und Verfolgung von Straftätern, ii) parlamentarische Vorrechte, iii) Gerichtsverfahren, iv) die Schlagkraft der Streitkräfte der Krone, v) das wirtschaftliche Wohl des Vereinigten Königreichs, vi) Verhandlungen mit der betroffenen Person, vii) wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, viii) Archivierung im öffentlichen Interesse. Explanatory Framework for Adequacy Discussions, Section H: National Security, S. 13, siehe Fußnote 222.

([237]) Paragraf 116 DPA 2018.

([238]) Gemäß Paragraf 149 Absatz 2 in Verbindung mit Paragraf 155 DPA 2018 können einem Verantwortlichen oder Auftragsverarbeiter Durchsetzungs- und Bußgeldbescheide aufgrund folgender Verstöße erteilt werden: Verstoß gegen Teil 4 Kapitel 2 des DPA 2018 (Grundsätze der Verarbeitung), Verstoß gegen eine Bestimmung von Teil 4 DPA 2018, mit dem betroffenen Personen Rechte gewährt werden, Verstoß gegen die Verpflichtung, dem Information Commissioner eine Verletzung des Schutzes personenbezogener Daten gemäß Paragraf 108 DPA 2018 zu melden, und Verstoß gegen die Grundsätze für die Übermittlung personenbezogener Daten an Drittländer, Länder, die nicht dem Übereinkommen angehören, und internationale Organisationen gemäß Paragraf 109 DPA 2018. (weitere Einzelheiten zu Durchsetzungs- oder Bußgeldbescheiden finden sich in den Erwägungsgründen 102 bis 103).

([239]) Gemäß Paragraf 147 Absatz 6 DPA 2018 darf der Information Commissioner einer in Paragraf 23 Absatz 3 des Freedom of Information Act 2000 genannten Stelle keinen Bewertungsbescheid erteilen. Hierzu zählen der Security Service (MI5), der Secret Intelligence Service (MI6) und das Government Communications Headquarter.

Bußgeldbescheide) gemäß dem DPA zu erteilen, die Befugnis zur Einsichtnahme gemäß internationalen Verpflichtungen, die Befugnis zum Zugang zu Räumlichkeiten und zur Durchführung von Kontrollen („powers of entry and inspection") sowie die Vorschriften über Straftaten ([240]). Wie in Erwägungsgrund 136 erläutert, gelten diese Ausnahmen nur im Einzelfall und nur dann, wenn sie notwendig und verhältnismäßig sind. Die Anwendung dieser Ausnahmen kann gerichtlich überprüft werden ([241]).

(142) Das ICO und die britischen Nachrichtendienste haben eine Absichtserklärung ([242]) unterzeichnet, die den Rahmen für die Zusammenarbeit in einer Reihe von Bereichen bildet, unter anderem in Bezug auf die Meldung von Datenschutzverletzungen und die Bearbeitung von Beschwerden betroffener Personen. Darin ist insbesondere vorgesehen, dass das ICO nach Eingang einer Beschwerde prüft, ob die Inanspruchnahme einer Ausnahme zum Schutz der nationalen Sicherheit angemessen war. Anfragen, die das ICO im Rahmen der Prüfung einzelner Beschwerden stellt, müssen innerhalb von 20 Arbeitstagen vom betreffenden Nachrichtendienst beantwortet werden; wenn es sich um Verschlusssachen im Sinne der Leitlinien der britischen Regierung über nationale Sicherheitsbescheinigungen nach dem DPA (UK Government Guidance on National Security Certificates under the Data Protection Act) handelt, sind hierfür geeignete sichere Kanäle zu nutzen. Von April 2018 bis heute hat das ICO 21 Beschwerden von Einzelpersonen erhalten, die Nachrichtendienste betrafen. Jede Beschwerde wurde geprüft, und das Ergebnis wurde der betroffenen Person mitgeteilt ([243]).

(143) Darüber hinaus übt der Ausschuss für Nachrichtendienste und Sicherheit (Intelligence and Security Committee — im Folgenden „ISC") die parlamentarische Aufsicht über die Datenverarbeitung durch die Nachrichtendienste aus. Die Rechtsgrundlage für die Arbeit des Ausschusses bildet das Justiz- und Sicherheitsgesetz (Justice and Security Act) von 2013 ([244]). Durch das Gesetz wurde der ISC als Ausschuss des britischen Parlaments eingerichtet. Der ISC setzt sich aus Mitgliedern beider Kammern des Parlaments zusammen, die vom Premierminister nach Konsultation des Oppositionsführers ernannt werden ([245]). Der ISC muss dem Parlament einen jährlichen Tätigkeitsbericht und weitere Berichte vorlegen, die er für angebracht hält ([246]).

(144) Der ISC hat seit 2013 erweiterte Befugnisse erhalten, darunter die Aufsicht über die operativen Tätigkeiten der Nachrichtendienste. Nach Paragraf 2 JSA 2013 hat der ISC die Aufgabe, die Ausgaben, die Verwaltung, die Strategien und die operativen Maßnahmen der nationalen Sicherheitsbehörden zu überwachen. Im JSA 2013 ist festgelegt, dass der ISC Untersuchungen zu operativen Angelegenheiten durchführen kann, wenn diese sich nicht

([240]) Folgende Bestimmungen können Gegenstand der Ausnahme sein: Paragraf 108 (Meldung einer Verletzung des Schutzes personenbezogener Daten an den Information Commissioner), Paragraf 119 (Einsichtnahme gemäß internationalen Verpflichtungen), Paragrafen 142 bis 154 sowie Anhang 15 (Bescheide des Information Commissioner sowie Befugnisse zum Zugang zu Räumlichkeiten und zur Durchführung von Kontrollen) und Paragrafen 170 bis 173 (Straftaten im Zusammenhang mit personenbezogenen Daten). Zusätzlich in Bezug auf die Verarbeitung durch die Nachrichtendienste gemäß Anhang 13 (weitere allgemeine Aufgaben des Information Commissioner), Nummer 1 Buchstaben a und g sowie Nummer 2.

([241]) Siehe zum Beispiel Rechtssache Baker/Secretary of State for the Home Department (siehe Fußnote 221).

([242]) Zwischen dem ICO und der UK Intelligence Community vereinbarte Absichtserklärung, siehe Fußnote 231.

([243]) In sieben dieser Fälle riet das ICO dem Beschwerdeführer, das Anliegen gegenüber dem Verantwortlichen vorzubringen (dies geschieht dann, wenn eine Person ein Anliegen beim ICO vorgebracht hat, es aber zuerst beim Verantwortlichen hätte vorbringen sollen); in einem Fall gab das ICO dem Verantwortlichen allgemeine Empfehlungen (dies geschieht dann, wenn der Verantwortliche zwar offensichtlich nicht gegen die Rechtsvorschriften verstoßen hat, aber durch eine Verbesserung der Verfahrensweisen womöglich hätte vermieden werden können, dass das Anliegen beim ICO vorgebracht wird); in den anderen 13 Fällen waren keine Maßnahmen seitens des Verantwortlichen erforderlich (dies ist dann der Fall, wenn die von der Person vorgebrachten Anliegen zwar unter den Data Protection Act 2018 fallen, da sie die Verarbeitung personenbezogener Daten betreffen, der Verantwortliche jedoch auf der Grundlage der bereitgestellten Informationen offenbar nicht gegen die Rechtsvorschriften verstoßen hat).

([244]) Wie von den britischen Behörden erläutert, wurde das Aufgabengebiet des ISC durch den JSA ausgeweitet und umfasst nunmehr auch die Überwachung der Nachrichtendienstgemeinschaft insgesamt — d. h. über die drei Nachrichtendienste hinaus — und die Möglichkeit einer rückwirkenden Kontrolle der operativen Tätigkeiten der Nachrichtendienste in Angelegenheiten von bedeutendem nationalem Interesse.

([245]) Paragraf 1 des Justice and Security Act 2013. Minister sind von der Mitgliedschaft ausgeschlossen. Die Mitglieder bekleiden ihr Amt im ISC für die Dauer der Legislaturperiode, in der sie ernannt wurden. Sie können auf Beschluss der Kammer, von der sie ernannt wurden, abberufen werden oder müssen ihr Amt niederlegen, wenn sie aus dem Parlament ausscheiden oder das Amt eines Ministers antreten. Die Mitglieder können auch zurücktreten.

([246]) Die Berichte und Stellungnahmen des Ausschusses sind unter folgendem Link abrufbar: http://isc.independent.gov.uk/committee-reports. Im Jahr 2015 hat der ISC einen Bericht über Datenschutz und Sicherheit mit dem Titel „Privacy and Security: A modern and transparent legal framework" (siehe https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf) erstellt, in dem sich der Ausschuss mit dem Rechtsrahmen für die von den Nachrichtendiensten angewandten Überwachungsmethoden befasste und eine Reihe von Empfehlungen aussprach, die anschließend erörtert und in den Entwurf des Gesetzes über Ermittlungsbefugnisse (Investigatory Powers Bill) aufgenommen wurden, der mit dem Investigatory Powers Act von 2016 in ein Gesetz umgewandelt wurde. Die Antwort der Regierung auf den Bericht über Datenschutz und Sicherheit ist unter folgendem Link abrufbar: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

auf laufende Operationen beziehen ([247]). In der gemeinsamen Absichtserklärung des Premierministers und des ISC ([248]) ist im Einzelnen dargelegt, welche Elemente zu berücksichtigen sind, wenn geprüft wird, ob eine Tätigkeit Teil einer laufenden Operation ist ([249]). Der ISC kann zudem vom Premierminister zur Untersuchung laufender Operationen aufgefordert werden und von den Nachrichtendiensten freiwillig bereitgestellte Informationen überprüfen.

(145) Nach Anhang 1 des Justice and Security Act 2013 kann der ISC die Leitung jeder der drei Nachrichtendienste zur Offenlegung jeder Art von Informationen auffordern. Der Dienst muss die entsprechenden Informationen vorlegen, sofern der Secretary of State dem nicht widerspricht ([250]). Den Angaben der britischen Behörden zufolge werden dem ISC in der Praxis nur sehr selten Informationen vorenthalten ([251]).

(146) Was Rechtsmittel anbelangt, so hat eine betroffene Person gemäß Paragraf 165 Absatz 2 DPA 2018 die Möglichkeit, beim ICO Beschwerde einzulegen, wenn sie der Auffassung ist, dass im Zusammenhang mit sie betreffenden personenbezogenen Daten ein Verstoß gegen Teil 4 des DPA 2018 vorliegt, einschließlich einer missbräuchlichen Verwendung der Ausnahmeregelungen und Einschränkungen.

(147) Darüber hinaus sind natürliche Personen nach Teil 4 des DPA 2018 berechtigt, beim High Court (bzw. beim Court of Session in Schottland) den Erlass einer Anordnung zu beantragen, die den Verantwortlichen verpflichtet, dem Recht auf Auskunft über personenbezogene Daten ([252]), auf Widerspruch gegen die Verarbeitung ([253]) und auf Berichtigung oder Löschung nachzukommen.

(148) Ferner sind natürliche Personen berechtigt, vom Verantwortlichen oder von einem Auftragsverarbeiter Ersatz für einen Schaden zu verlangen, den sie aufgrund eines Verstoßes gegen eine Anforderung von Teil 4 des DPA 2018 erlitten haben ([254]). Als Schaden gilt sowohl ein finanzieller als auch ein nichtfinanzieller Schaden, wie z. B. seelisches Leid ([255]).

(149) Schließlich kann eine natürliche Person wegen Handlungen der oder im Namen der britischen Nachrichtendienste ([256]) beim Investigatory Powers Tribunal Beschwerde einlegen. Das Investigatory Powers Tribunal (IPT) wurde durch das Gesetz von 2000 über die Regelung der Ermittlungsbefugnisse für England, Wales und Nordirland (Regulation of Investigatory Powers Act) und durch das Gesetz von 2000 über die Regelung der Ermittlungsbefugnisse für Schottland (Regulation of Investigatory Powers (Scotland) Act) (im Folgenden zusammen „RIPA 2000“) eingerichtet und ist von der Exekutive unabhängig ([257]). Gemäß Paragraf 65 RIPA 2000 werden die Mitglieder des Tribunals von Ihrer Majestät für einen Zeitraum von fünf Jahren ernannt.

(150) Ein Mitglied des Tribunals kann von Ihrer Majestät nach einer Meinungsäußerung („Address“) ([258]) beider Kammern des Parlaments seines Amtes enthoben werden ([259]).

(151) Möchte eine natürliche Person vor dem Investigatory Powers Tribunal Klage erheben („standing requirement“), so muss sie nach Paragraf 65 RIPA 2000 der Überzeugung sein, dass i) Handlungen eines Nachrichtendienstes in Bezug auf sie selbst, ihr Eigentum, von ihr übermittelte oder empfangene oder für sie bestimmte Kommunikationsvorgänge, oder auf ihre Nutzung eines Postdienstes, Telekommunikationsdienstes oder Telekommunikationssystems ([260]) stattgefunden haben, und dass ii) die Handlungen unter anfechtbaren Umständen („challengeable

([247]) Paragraf 2 JSA 2013.
([248]) Absichtserklärung zwischen Premierminister und ISC, abrufbar unter folgendem Link: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Absichtserklärung zwischen dem Premierminister und dem ISC, Nummer 14, siehe Fußnote 248.
([250]) Der Secretary of State darf der Offenlegung nur aus zwei Gründen widersprechen, nämlich wenn es sensible Informationen geht, die gegenüber dem ISC aus Gründen der nationalen Sicherheit nicht offengelegt werden sollten, oder die fraglichen Informationen so beschaffen sind, dass der Secretary of State es (nicht nur aus Gründen der nationalen Sicherheit) nicht für angemessen hält, sie bei entsprechender Aufforderung einem Sonderausschuss des Unterhauses vorzulegen (Anhang 1 Nummer 4 Ziffer 2 des JSA 2013).
([251]) UK Explanatory Framework — Section H: National Security, S. 43.
([252]) Paragraf 94 Absatz 11 DPA 2018.
([253]) Paragraf 99 Absatz 4 DPA 2018.
([254]) Nach Paragraf 169 DPA 2018 kann „eine Person, die aufgrund eines Verstoßes gegen eine Anforderung der Datenschutzvorschriften einen Schaden erleidet“, Ansprüche geltend machen.
([255]) Paragraf 169 Absatz 5 DPA 2018.
([256]) Siehe Paragraf 65 Absatz 2 Buchstabe b RIPA.
([257]) Nach Anhang 3 des RIPA 2000 müssen die Mitglieder über fachspezifische richterliche Erfahrungen verfügen und können wiederernannt werden.
([258]) Erläuterungen zum Begriff „Address“ siehe Fußnote 183.
([259]) Anhang 3 Nummer 1 Ziffer 5 RIPA 2000.
([260]) Paragraf 65 Absatz 4 RIPA 2000.

circumstances") ([261]) erfolgt sind oder durch oder im Namen der Nachrichtendienste ausgeführt wurden („carried out by or on behalf of the intelligence services") ([262]). Da insbesondere dieses Kriterium der Überzeugung („belief") recht weit ausgelegt worden ist ([263]), sind die Anforderungen für eine Klageerhebung vor dem Tribunal vergleichsweise niedrig.

(152) Prüft das Tribunal eine bei ihm eingegangene Beschwerde, so ist es verpflichtet, zu untersuchen, ob die Personen, gegen die in der Beschwerde Vorwürfe erhoben werden, gegenüber dem Beschwerdeführer tätig geworden sind; ferner muss das Tribunal die Behörde untersuchen, die die Verstöße begangen haben soll, und es muss prüfen, ob die angeblichen Handlungen stattgefunden haben ([264]). Kommt es vor dem Tribunal zu einem Verfahren, so muss das Tribunal bei seiner Entscheidungsfindung dieselben Grundsätze anwenden, die ein Gericht bei einer Anfechtungsklage zugrunde legen würde ([265]).

(153) Das Tribunal muss dem Beschwerdeführer mitteilen, ob zu seinen Gunsten entschieden wurde oder nicht ([266]). Gemäß Paragraf 67 Absätze 6 und 7 RIPA 2000 ist das Gericht befugt, einstweilige Verfügungen zu erlassen und eine Entschädigung zu gewähren oder andere Beschlüsse zu treffen, die es für angemessen hält ([267]). Nach Paragraf 67A RIPA 2000 kann gegen eine Entscheidung des Tribunals Berufung eingelegt werden, sofern das Tribunal oder das zuständige Berufungsgericht seine Erlaubnis erteilt.

(154) Eine natürliche Person kann insbesondere dann Klage vor dem Investigatory Powers Tribunal erheben — und Abhilfe erhalten —, wenn sie der Ansicht ist, dass eine Behörde in einer Weise gehandelt hat (oder zu handeln beabsichtigt), die mit einem in der Europäischen Menschenrechtskonvention verbürgten Recht unvereinbar und folglich nach Paragraf 6 Absatz 1 des Human Rights Act 1998 unrechtmäßig ist. Das Investigatory Powers Tribunal besitzt die ausschließliche Zuständigkeit für alle auf der Grundlage des Human Rights Act gegen Nachrichtendienste erhobenen Klagen. Dem High Court zufolge bedeutet dies, dass „die Frage, ob in einem bestimmten Fall ein Verstoß gegen den Human Rights Act vorliegt, grundsätzlich von einem unabhängigen Gericht gestellt und entschieden werden kann, das Zugang zu allen relevanten Materialien, einschließlich Verschlusssachen, haben kann. […] Wir bedenken in diesem Zusammenhang auch, dass inzwischen auch gegen Entscheidungen des Investigatory Powers Tribunal selbst bei einem zuständigen Berufungsgericht (in England und Wales wäre das der Court of Appeal) ein Rechtsbehelf eingelegt werden kann; und dass der Supreme Court unlängst entschieden hat, dass das Investigatory Powers Tribunal grundsätzlich gerichtlich überprüfbar ist: siehe R (Privacy International)/Investigatory Powers Tribunal, [2019] UKSC 22; [2019] 2 WLR 1219" ([268]). Befindet das Investigatory Powers Tribunal die Handlung einer Behörde für unrechtmäßig, so kann es im Rahmen seiner Befugnisse den Rechtsbehelf oder die Abhilfe gewähren oder die Anordnung treffen, die es für gerecht und angemessen hält ([269]).

([261]) „Anfechtbare Umstände" beziehen sich auf mit Befugnis ausgeführte behördliche Handlungen (z. B. Anordnungen, Genehmigungen/Bescheide zur Beschaffung von Kommunikationsdaten usw.), oder sie liegen vor, wenn eine Handlung (unabhängig davon, ob eine Befugnis tatsächlich erteilt wurde) ohne Vorliegen einer solchen Befugnis — oder zumindest ohne gebührende Prüfung der Frage, ob eine Befugnis eingeholt werden müsste — nicht ordnungsgemäß gewesen wäre. Von einem Judicial Commissioner genehmigte Handlungen gelten als unter anfechtbaren Umständen erfolgt (Paragraf 65 Absatz 7ZA RIPA 2000); andere Handlungen hingegen, die von einer Person, die ein richterliches Amt innehat, genehmigt wurden, gelten als nicht unter anfechtbaren Umständen erfolgt (Paragraf 65 Absätze 7 und 8 RIPA 2000).

([262]) Den Angaben der britischen Behörden zufolge ist es aufgrund der niedrigen Schwelle für die Einreichung einer Beschwerde nicht ungewöhnlich, dass das Tribunal im Zuge seiner Untersuchung feststellt, dass der Beschwerdeführer tatsächlich nie Gegenstand einer Untersuchung durch eine öffentliche Behörde war. Dem jüngsten statistischen Bericht des Investigatory Powers Tribunal ist zu entnehmen, dass 2016 insgesamt 209 Beschwerden beim Tribunal eingingen, von denen 52 % als leichtfertig oder schikanös eingestuft wurden und 25 % ohne Feststellungen blieben („no determination"). Die britischen Behörden erläuterten, dass dies entweder bedeutet, dass in Bezug auf den Beschwerdeführer keine verdeckten Aktivitäten/Befugnisse angewandt wurden oder dass zwar verdeckte Methoden angewandt wurden, diese jedoch nach Auffassung des Tribunals rechtmäßig waren. Weitere 11 % der Fälle lagen den Feststellungen zufolge außerhalb der gerichtlichen Zuständigkeit, wurden zurückgezogen oder waren ungültig, 5 % waren verjährt und 7 % der Fälle wurden zugunsten des Beschwerdeführers entschieden. Statistischer Bericht 2016 des Investigatory Powers Tribunal, abrufbar unter folgendem Link: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([263]) Siehe Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH In diesem Fall kam das Investigatory Powers Tribunal unter Verweis auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu dem Schluss, dass der angemessene Maßstab für die Einschätzung, ob eine unter Paragraf 68 Absatz 5 RIPA 2000 fallende Handlung durch einen der oder im Namen eines der Nachrichtendienste durchgeführt wurde, die Frage ist, ob eine Grundlage für eine solche Einschätzung vorliegt; dies umfasst auch den Umstand, dass eine natürliche Person nur dann behaupten kann, aufgrund der bloßen Existenz nachrichtendienstlicher Maßnahmen oder von Rechtsvorschriften, die nachrichtendienstliche Maßnahmen erlauben, Opfer einer Verletzung geworden zu sein, wenn sie nachweisen kann, dass sie aufgrund ihrer persönlichen Situation potenziell Gefahr läuft, Gegenstand derartiger Maßnahmen zu werden (siehe *Human Rights Watch/Secretary of State*, Rn. 41).

([264]) Paragraf 67 Absatz 3 RIPA 2000.

([265]) Paragraf 67Absatz 2 RIPA 2000.

([266]) Paragraf 68 Absatz 4 RIPA 2000.

([267]) Dazu gehören auch Anordnungen zur Vernichtung aller Informationen, die eine Behörde zu einer Person gespeichert hat.

([268]) High Court of Justice, *Liberty*, [2019] EWHC 2057 (Admin), Rn. 170.

([269]) Paragraf 8 Absatz 1 des Human Rights Act 1998.

(155) Schließlich kann eine natürliche Person, wenn alle nationalen Rechtsmittel ausgeschöpft wurden, vor dem Europäischen Gerichtshof für Menschenrechte aufgrund der Verletzung ihrer nach der Europäischen Menschenrechtskonvention garantierten Rechte, einschließlich des Rechts auf Privatsphäre und Datenschutz, einen Rechtsbehelf einlegen.

(156) Aus den vorstehenden Ausführungen lässt sich schließen, dass die Weitergabe von gemäß diesem Beschluss übermittelten Daten durch britische Strafverfolgungsbehörden an andere Behörden, auch Nachrichtendienste, durch Einschränkungen und Bedingungen begrenzt ist, sodass sichergestellt wird, dass eine solche Weitergabe erforderlich und verhältnismäßig ist und spezifischen Datenschutzgarantien im Sinne des DPA 2018 unterliegt. Darüber hinaus wird die Verarbeitung von Daten durch die betroffenen Behörden von unabhängigen Stellen überwacht, und die betroffenen natürlichen Personen haben Zugang zu wirksamen gerichtlichen Rechtsbehelfen.

3. **SCHLUSSFOLGERUNG**

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

(158) 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.

(159) 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 natürlichen Personen, deren personenbezogene Daten aus der Europäischen Union an das Vereinigte Königreich zu Zwecken des öffentlichen Interesses, auch im Rahmen des Austauschs personenbezogener Daten zwischen Strafverfolgungsbehörden und anderen Behörden, wie nationalen Sicherheitsorganen, übermittelt werden, auf das zur Erreichung des betreffenden rechtmäßigen Ziels unbedingt erforderliche Maß beschränkt ist und dass ein wirksamer Rechtsschutz gegen derartige Eingriffe besteht.

(160) Daher sollte beschlossen werden, dass das Vereinigte Königreich 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.

(161) Diese Schlussfolgerung beruht sowohl auf der einschlägigen innerstaatlichen Regelung 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.

4. **AUSWIRKUNGEN DIESES BESCHLUSSES UND MAßNAHMEN DER DATENSCHUTZBEHÖRDEN**

(162) 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.

(163) 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 dieses Beschlusses 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.

(164) Gleichzeitig sei daran erinnert, dass gemäß Artikel 47 Absatz 5 der Richtlinie (EU) 2016/680 und wie vom Gerichtshof im Urteil in der Rechtssache Schrems 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 Rügen vor einem nationalen Gericht geltend zu machen, das gegebenenfalls ein Vorabentscheidungsverfahren beim Gerichtshof einleiten muss. ([270])

([270]) Schrems, Rn. 65.

5. ÜBERWACHUNG, AUSSETZUNG, AUFHEBUNG ODER ÄNDERUNG DIESES BESCHLUSSES

(165) Gemäß Artikel 36 Absatz 4 der Richtlinie (EU) 2016/680 überwacht die Kommission nach Erlass dieses Beschlusses fortlaufend die einschlägigen Entwicklungen im Vereinigten Königreich, um festzustellen, ob das Vereinigte Königreich weiterhin ein der Sache nach gleichwertiges Schutzniveau gewährleistet. Eine solche Überwachung ist im vorliegenden Fall von besonderer Bedeutung, da das Vereinigte Königreich eine neue Datenschutzregelung erlassen, anwenden und durchsetzen wird, die nicht mehr dem Recht der Union unterliegt, das sich möglicherweise weiterentwickeln wird. Diesbezüglich wird ein besonderes Augenmerk auf der praktischen Anwendung der Vorschriften des Vereinigten Königreichs über die Übermittlung personenbezogener Daten an Drittländer liegen, unter anderem durch den Abschluss internationaler Übereinkünfte, und den möglichen Folgen für das Schutzniveau der gemäß diesem Beschluss übermittelten Daten; wie auch darauf, inwieweit die Rechte des Einzelnen in den Bereichen, die unter diesen Beschluss fallen, wirksam ausgeübt werden können. Neben anderen Elementen werden in die Überwachung durch die Kommission die Entwicklungen in der Rechtsprechung und die Aufsichtstätigkeit durch das ICO und andere unabhängige Stellen einfließen.

(166) Zur Vereinfachung dieser Überwachung sollten die Behörden des Vereinigten Königreichs die Kommission unverzüglich und regelmäßig über jede wesentliche Änderung der Rechtsordnung des Vereinigten Königreichs, die sich auf den Rechtsrahmen, der Gegenstand dieses Beschlusses ist, auswirkt, sowie über jede Entwicklung der in diesem Beschluss bewerteten Verfahrensweisen im Zusammenhang mit der Verarbeitung personenbezogener Daten unterrichten, insbesondere im Hinblick auf die in Erwägungsgrund 165 genannten Elemente.

(167) 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.

(168) Lassen verfügbare Informationen — insbesondere Informationen, die sich aus der Überwachung dieses Beschlusses ergeben oder vom Vereinigten Königreich oder Mitgliedstaaten zur Verfügung gestellt 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.

(169) 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.

(170) 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.

(171) 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. GELTUNGSDAUER UND VERLÄNGERUNG DIESES BESCHLUSSES

(172) Es gilt zu berücksichtigen, dass das Vereinigte Königreich mit dem Ende des im Austrittsabkommen vorgesehenen Übergangszeitraums und dem Außerkrafttreten der Übergangsbestimmung gemäß Artikel 782 des Handels- und Kooperationsabkommens zwischen der EU und dem Vereinigten Königreich eine neue Datenschutzregelung erlassen, anwenden und durchsetzen wird, die nicht mehr der Regelung entsprechen wird, die galt, als das Vereinigte Königreich noch an Unionsrecht gebunden war. Vor diesem Hintergrund können insbesondere Ergänzungen oder Änderungen des in diesem Beschluss bewerteten Datenschutzrahmens vorgenommen werden und andere relevante Entwicklungen stattfinden.

(173) Daher sollte dieser Beschluss ab seinem Inkrafttreten für einen Zeitraum von vier Jahren gelten.

(174) Ergibt sich insbesondere aus der Überwachung dieses Beschlusses, dass die Feststellungen zur 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 weitere vier Jahre verlängert. Ein solcher Durchführungsrechtsakt zur Änderung dieses Beschlusses ist nach dem in Artikel 58 Absatz 2 der Richtlinie (EU) 2016/680 genannten Verfahren zu erlassen.

7. **SCHLUSSBEMERKUNGEN**

(175) Der Europäische Datenschutzausschuss hat seine Stellungnahme ([271]) veröffentlicht, der bei der Ausarbeitung dieses Beschlusses Rechnung getragen wurde.

(176) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 58 der Richtlinie (EU) 2016/680 eingesetzten Ausschusses.

(177) 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. Darüber hinaus ist die Richtlinie (EU) 2016/680 aufgrund des Durchführungsbeschlusses (EU) 2020/1745 des Rates ([272]) ab dem 1. Januar 2021 vorläufig in Kraft zu setzen und auf Irland anzuwenden. Irland ist daher durch diesen Durchführungsbeschluss 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 Schengen-Besitzstand, an dem es sich beteiligt.

(178) 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 dieses Durchführungsbeschlusses verpflichtet.

(179) Für Island und Norwegen stellt dieser Durchführungsbeschluss 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 ([273]) dar.

(180) Für die Schweiz stellt dieser Durchführungsbeschluss 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 ([274]) dar.

(181) Für Liechtenstein stellt dieser Durchführungsbeschluss 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 ([275]) dar.

([271]) Stellungnahme 15/2021 hinsichtlich des Entwurfs eines Durchführungsbeschlusses der Kommission gemäß der Richtlinie (EU) 2016/680 zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, abrufbar unter folgendem Link: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) 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).

([273]) ABl. L 176 vom 10.7.1999, S. 36.

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

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

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Für die Zwecke des Artikels 36 der Richtlinie (EU) 2016/680 gewährleistet das Vereinigte Königreich ein angemessenes Schutzniveau für personenbezogene Daten, die aus der Europäischen Union an Behörden im Vereinigten Königreich, die für die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zuständig sind, übermittelt werden.

Artikel 2

Üben die zuständigen Aufsichtsbehörden in den Mitgliedstaaten zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ihre Befugnisse nach Artikel 47 der Richtlinie (EU) 2016/680 im Hinblick auf die Übermittlung von Daten an Behörden im Vereinigten Königreich im Rahmen des Anwendungsbereichs gemäß Artikel 1 aus, so unterrichtet der betreffende Mitgliedstaat unverzüglich die Kommission.

Artikel 3

(1) Die Kommission überwacht fortlaufend die Anwendung des Rechtsrahmens, auf den sich dieser Beschluss stützt, einschließlich der Bedingungen, unter denen Weiterübermittlungen vorgenommen und Rechte des Einzelnen ausgeübt werden, um zu prüfen, ob das Vereinigte Königreich weiter ein angemessenes Schutzniveau im Sinne des Artikels 1 bietet.

(2) Die Mitgliedstaaten und die Kommission unterrichten einander über Fälle, in denen der Information Commissioner oder eine andere zuständige Behörde des Vereinigten Königreichs die Einhaltung des Rechtsrahmens, auf den sich dieser Beschluss stützt, nicht gewährleistet.

(3) Die Mitgliedstaaten und die Kommission unterrichten einander über Hinweise darauf, dass Eingriffe von Behörden des Vereinigten Königreichs in das Recht natürlicher Personen auf Schutz ihrer personenbezogenen Daten über den unbedingt erforderlichen Umfang hinausgehen oder dass es keinen wirksamen Rechtsschutz gegen solche Eingriffe gibt.

(4) Liegen der Kommission Hinweise darauf vor, dass ein angemessenes Schutzniveau nicht mehr gewährleistet ist, so unterrichtet sie die zuständigen Behörden des Vereinigten Königreichs und kann diesen Beschluss aussetzen, aufheben oder ändern.

(5) Die Kommission kann diesen Beschluss auch aussetzen, aufheben oder ändern, wenn sie aufgrund mangelnder Kooperation der Regierung des Vereinigten Königreichs nicht feststellen kann, ob die Feststellung in Artikel 1 berührt ist.

Artikel 4

Die Geltungsdauer dieses Beschlusses endet am 27. Juni 2025, sofern sie nicht nach dem in Artikel 58 Absatz 2 der Richtlinie (EU) 2016/680 genannten Verfahren verlängert wird.

Artikel 5

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 28. Juni 2021

Für die Kommission
Didier REYNDERS
Mitglied der Kommission