067407/EU XXVII. GP
Eingelangt am 01/07/21

EUROPÄISCHE
KOMMISSION

Brüssel, den 28.6.2021
C(2021) 4800 final

DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION

vom 28.6.2021

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

(Text von Bedeutung für den EWR)

www.parlament.gv.at

DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION

vom 28.6.2021

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

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

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

in Erwägung nachstehender Gründe:

1. EINLEITUNG

(1) Die Verordnung (EU) 2016/679 enthält die Vorschriften für die Übermittlung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter in der Europäischen Union an Drittländer und internationale Organisationen, soweit die betreffenden Übermittlungen in ihren Anwendungsbereich fallen. Die Vorschriften für internationale Übermittlungen personenbezogener Daten sind in Kapitel V dieser Verordnung, d. h. in den Artikeln 44 bis 50, festgelegt. Der Fluss personenbezogener Daten in Drittländer und aus Drittländern ist zwar für die Ausweitung der internationalen Zusammenarbeit und des grenzüberschreitenden Handels wesentlich, dennoch darf das unionsweit gewährleistete Schutzniveau für personenbezogene Daten bei Übermittlungen in Drittländer nicht untergraben werden.[2]

(2) Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 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 45 Absatz 1 und Erwägungsgrund 103 dieser Verordnung ohne weitere Genehmigung an ein Drittland übermittelt werden.

(3) Wie in Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 festgelegt, muss die Annahme eines Angemessenheitsbeschlusses auf einer umfassenden Analyse der Rechtsordnung des Drittlands beruhen, und zwar sowohl in Bezug auf die für die Datenimporteure geltenden Vorschriften als auch auf die Beschränkungen und Garantien für den Zugang der Behörden zu personenbezogenen Daten. Im Rahmen ihrer Prüfung muss die Kommission feststellen, ob das betreffende Drittland ein Schutzniveau garantiert, das dem innerhalb der Europäischen Union gewährleisteten

[1] ABl. L 119 vom 4.5.2016, S. 1.

[2] Siehe Erwägungsgrund 101 der Verordnung (EU) 2016/679.

www.parlament.gv.at

Schutzniveau „der Sache nach gleichwertig“ ist (Erwägungsgrund 104 der Verordnung (EU) 2016/679). Die Frage, ob ein Schutzniveau „der Sache nach gleichwertig“ ist, wird anhand des Maßstabs beurteilt, der in den Rechtsvorschriften der Europäischen Union, insbesondere in der Verordnung (EU) 2016/679, festgelegt und durch die Rechtsprechung des Gerichtshofs der Europäischen Union[3] entwickelt wurde. Die vom Europäischen Datenschutzausschuss (EDPB) herausgegebene Referenzgrundlage für Angemessenheit[4] ist in diesem Zusammenhang ebenfalls von Bedeutung.

(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 Datenschutz sowie ihrer wirksamen Anwendung, Überwachung und Durchsetzung das erforderliche Maß an Schutz bietet.[7]

(5) Die Kommission hat Recht und Praxis im Vereinigten Königreich sorgfältig analysiert. Ausgehend von den Feststellungen in den Erwägungsgründen 8 bis 270 gelangt die Kommission zu dem Schluss, dass das Vereinigte Königreich ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die im Rahmen der Verordnung (EU) 2016/679 aus der Europäischen Union in das Vereinigte Königreich übermittelt werden.

(6) Diese Schlussfolgerung betrifft nicht personenbezogene Daten, die zu Zwecken der Einwanderungskontrolle des Vereinigten Königreichs übermittelt werden oder aus anderen Gründen in den Anwendungsbereich der Ausnahme von bestimmten Rechte betroffener Personen zu Zwecken der Aufrechterhaltung einer wirksamen Einwanderungskontrolle (im Folgenden „Ausnahme im Bereich der Einwanderung“) gemäß Anhang 2 Nummer 4 Ziffer 1 des UK Data Protection Act fallen. Ob die im britischem Recht vorgesehene Ausnahme im Bereich der Einwanderung gültig ist und wie sie auszulegen ist, ist nach einem Beschluss des Court of Appeal in England and Wales vom 26. Mai 2021 nicht entschieden. Der Court of Appeal hat erkannt, dass die Rechte betroffener Personen zu Zwecken der Einwanderungskontrolle „als wichtiger Aspekt des öffentlichen Interesses“ grundsätzlich zwar eingeschränkt werden dürfen, die Ausnahme im Bereich der Einwanderung in ihrer jetzigen Form aber mit dem britischen Recht unvereinbar ist, da in der Gesetzgebungsmaßnahme spezifische Bestimmungen mit den in Artikel 23 Absatz 2 der Datenschutzgrundverordnung des

---

3 Siehe zuletzt Rechtssache C-311/18, Facebook Ireland und Schrems (im Folgenden „Schrems II“) ECLI:EU:C:2020:559.

4 Europäischer Datenschutzausschuss, Referenzgrundlage für Angemessenheit, WP 254 rev. 01., abrufbar unter folgendem Link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

5 Rechtssache C-362/14, Schrems (im Folgenden „Schrems I“), ECLI:EU:C:2015:650, Rn. 73.

6 Schrems I, Rn. 74.

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

www.parlament.gv.at

Vereinigten Königreichs (UK GDPR) genannten Garantien fehlen.[8] Deshalb sollte die Übermittlung personenbezogener Daten aus der Union in das Vereinigte Königreich, auf die die Ausnahme im Bereich der Einwanderung angewendet werden kann, aus dem Anwendungsbereich des vorliegenden Beschlusses ausgeklammert werden.[9] Sobald die Unvereinbarkeit mit dem britischen Recht beseitigt ist, sollten sowohl die Ausnahme im Bereich der Einwanderung als auch die Notwendigkeit der Einschränkung des Anwendungsbereichs des vorliegenden Beschlusses erneut bewertet werden.

(7) Dieser Beschluss sollte die unmittelbare Anwendung der Verordnung (EU) 2016/679 auf Organisationen mit Sitz im Vereinigten Königreich nicht berühren, wenn die in Artikel 3 der Verordnung festgelegten Bedingungen für den räumlichen Anwendungsbereich der Verordnung erfüllt sind.

2. VORSCHRIFTEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

2.1. Der konstitutionelle Rahmen

(8) Das Vereinigte Königreich ist eine parlamentarische Demokratie, deren Staatsoberhaupt ein konstitutioneller Souverän ist. 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 rechenschaftspflichtig gegenüber beiden Kammern des Parlaments, die für die Kontrolle der Regierung und die Erörterung sowie Verabschiedung von Gesetzesinitiativen verantwortlich sind.

(9) Das britische Parlament hat dem schottischen Parlament, dem walisischen Parlament (Senedd Cymru) und der parlamentarischen Versammlung für Nordirland die Verantwortung für die Gesetzgebung in denjenigen inneren Angelegenheiten in Schottland, Wales und Nordirland übertragen, die es sich nicht selbst vorbehalten hat. 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, an das schottische Parlament bzw. die parlamentarische Versammlung für Nordirland übertragen. Das Vereinigte Königreich besitzt keine kodifizierte Verfassung im Sinne eines konkreten Verfassungsdokuments. Die Verfassungsgrundsätze haben sich im Laufe der Zeit auf der Grundlage der Rechtsprechung und insbesondere des Gewohnheitsrechts fortentwickelt. Der Verfassungsrang bestimmter Dokumente wie der Magna Carta, der

---

[8] Court of Appeal (Civil Division), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport,* [2021] EWCA Civ 800, Rn. 53 bis 56. Der Court of Appeal hob die Entscheidung des High Court of Justice auf, der die Ausnahme im Lichte der Verordnung (EU) 2016/679 (insbesondere ihres Artikels 23) und der Charta der Grundrechte der Europäischen Union bewertet und die Ausnahme für rechtmäßig befunden hatte (*Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

[9] Sofern die geltenden Bedingungen erfüllt sind, sind Übermittlungen zu Zwecken der Einwanderungskontrolle des Vereinigten Königreichs im Einklang mit den Übermittlungsmechanismen der Artikel 46 bis 49 der Verordnung (EU) 2016/679 zulässig.

www.parlament.gv.at

Bill of Rights von 1689 und des Gesetzes über Menschenrechte von 1998 (Human Rights Act 1998) wurde von Gerichten 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]

(10) Mit dem Human Rights Act 1998 wurden die in der Europäischen Menschenrechtskonvention verbürgten Rechte in das Recht des Vereinigten Königreichs übernommen. Durch den Human Rights Act werden jeder Person die Grundrechte und -freiheiten gewährt, die in den Artikeln 2 bis 12 und 14 der Europäischen Menschenrechtskonvention, in den Artikeln 1, 2 und 3 ihres Ersten Protokolls und in Artikel 1 ihres Dreizehnten Protokolls in Verbindung mit den Artikeln 16, 17 und 18 dieser Konvention vorgesehen sind. Dazu zählen das Recht auf Achtung des Privat- und Familienlebens (und das Recht auf Datenschutz als Teil dieses Rechts) und das Recht auf ein faires Verfahren.[11] Insbesondere darf eine Behörde gemäß Artikel 8 dieser Konvention 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.

(11) Gemäß dem Human Rights Act 1998 muss jede Handlung von Behörden mit einem Konventionsrecht vereinbar sein.[12] Darüber hinaus sind primärrechtliche und nachrangige Bestimmungen so zu lesen und umzusetzen, dass sie mit den Konventionsrechten vereinbar sind.[13]

2.2. Der Datenschutzrechtsrahmen des Vereinigten Königreichs

(12) 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

---

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 Datenschutzgesetz von 2018 (Data Protection Act 2018) ersetzt, das in Verbindung mit der UK GDPR 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).

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), abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN.

www.parlament.gv.at

während des Übergangszeitraums bis zum 31. Dezember 2020 weiterhin Anwendung. Vor dem Austritt und während des Übergangszeitraums bestand der Rechtsrahmen für den Schutz personenbezogener Daten im Vereinigten Königreich aus den einschlägigen EU-Rechtsvorschriften (insbesondere der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates[15]) sowie nationalen Rechtsvorschriften, insbesondere dem Gesetz über den Datenschutz von 2018 (Data Protection Act 2018 – im Folgenden „DPA 2018“)[16]; Letzteres sah nationale Vorschriften vor, mit denen die Anwendung der Bestimmungen der Verordnung (EU) 2016/679 und der umgesetzten Richtlinie (EU) 2016/680 präzisiert und eingeschränkt wurde, soweit dies gemäß der Verordnung (EU) 2016/679 zulässig war.

(13) Zur Vorbereitung auf den Austritt aus der Europäischen Union erließ die Regierung des Vereinigten Königreichs das Gesetz über den Austritt aus der Europäischen Union von 2018 (European Union (Withdrawal) Act 2018)[17], mit dem unmittelbar geltende Rechtsvorschriften der Union in das Recht des Vereinigten Königreichs übernommen wurden.[18] Dieses beibehaltene EU-Recht („retained EU law“) umfasst die Verordnung (EU) 2016/679 in all ihren Teilen (einschließlich ihrer Erwägungsgründe).[19] Laut diesem Gesetz muss das unverändert beibehaltene EU-Recht von den Gerichten des Vereinigten Königreichs gemäß der einschlägigen Rechtsprechung des Europäischen Gerichtshofs und den allgemeinen Grundsätzen des Unionsrechts ausgelegt werden, so wie sie unmittelbar vor dem Ende des Übergangszeitraums gelten (bezeichnet als „beibehaltene EU-Rechtsprechung“ („retained EU case law“) bzw. als „beibehaltene allgemeine Grundsätze des EU-Rechts“ („retained general principles of EU law“)).[20]

(14) Gemäß dem European Union (Withdrawal) Act 2018 sind die Minister des Vereinigten Königreichs befugt, im Wege von Verordnungen abgeleitete

---

15 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89), abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680&from=EN.

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

17 European Union (Withdrawal) Act 2018, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/16/contents.

18 Absicht und Wirkung des European Union (Withdrawal) Act 2018 bestanden darin, alle unmittelbar geltenden Rechtsvorschriften der Union, die am Ende der Übergangszeit in das Recht des Vereinigten Königreichs aufgenommen wurden, so in das Recht des Vereinigten Königreichs aufzunehmen, wie sie unmittelbar vor dem Ende des Übergangszeitraums im EU-Recht galten, siehe Paragraf 3 des European Union (Withdrawal) Act 2018.

19 In den Erläuterungen zum Gesetz von 2018 über den Austritt aus der EU (European Union (Withdrawal) Act 2018) heißt es dazu: Wenn Rechtsvorschriften gemäß diesem Paragrafen umgewandelt werden, ist der Wortlaut der Rechtsvorschriften selbst Teil des innerstaatlichen Rechts. Dazu zählt auch der vollständige Wortlaut eines jeden EU-Instruments (einschließlich seiner Erwägungsgründe). (Explanatory Notes to the European Union (Withdrawal) Act 2018, Nummer 83, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Nach Angaben der britischen Behörden war es nicht erforderlich, die Erwägungsgründe in der gleichen Weise zu ändern, wie die Artikel der Verordnung (EU) 2016/679 durch die DPPEC Regulations geändert wurden, da die Erwägungsgründe nicht den Status verbindlicher Rechtsvorschriften haben.

20 Paragraf 6 des European Union (Withdrawal) Act 2018.

www.parlament.gv.at

Rechtsvorschriften einzuführen, um die Änderungen am beibehaltenen Recht der Europäischen Union vorzunehmen, die infolge des Austritts des Vereinigten Königreichs aus der Europäischen Union notwendig geworden sind. Sie übten diese Befugnis durch den Erlass der Verordnungen von 2019 über Datenschutz, Privatsphäre und elektronische Kommunikation (Änderungen usw.) (EU-Austritt) (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 – im Folgenden „DPPEC Regulations“) aus.[21] Durch die DPPEC Regulations wurde die Verordnung (EU) 2016/679, die durch den European Union (Withdrawal) Act 2018, den DPA 2018 und andere Datenschutzgesetze in das britische Recht übernommen wurde, geändert, um sie an den nationalen Kontext anzupassen.[22]

(15) Folglich besteht der rechtliche Rahmen für den Schutz personenbezogener Daten im Vereinigten Königreich nach dem Ende der Übergangszeit aus folgenden Elementen:

– UK GDPR, wie sie durch den European Union (Withdrawal) Act 2018 in das Recht des Vereinigten Königreichs übernommen und durch die DPPEC Regulations geändert wurde,[23] und

– DPA 2018[24], wie er durch die DPPEC Regulations geändert wurde.

(16) Da die UK GDPR auf einem EU-Rechtsakt basiert, geben die Datenschutzvorschriften im Vereinigten Königreich in vielen Aspekten weitgehend die entsprechenden innerhalb der Europäischen Union geltenden Vorschriften wieder.

(17) Zusätzlich zu den Befugnissen, die dem Secretary of State (Minister des Kabinetts) durch den European Union (Withdrawal) Act 2018 eingeräumt wurden, geben mehrere Bestimmungen des DPA 2018 dem Secretary of State die Befugnis, abgeleitete Rechtsvorschriften zu erlassen, um einzelne Bestimmungen des Gesetzes zu ändern oder ergänzende sowie zusätzliche Vorschriften einzuführen.[25] Der Secretary of State hat bisher nur von der Befugnis nach Paragraf 137 DPA 2018 Gebrauch gemacht und die Verordnungen von 2019 über Datenschutz (Gebühren und Informationen) (Änderung) (Data Protection (Charges and Information) (Amendment) Regulations

---

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

22 Diese Änderungen an der UK GDPR und dem DPA 2018 sind überwiegend technischer Art, etwa die Streichung von Verweisen auf „Mitgliedstaaten“ oder die Anpassung der Terminologie, z. B. die Ersetzung von Verweisen auf die Verordnung (EU) 2016/679 durch Verweise auf die UK GDPR. In einigen Fällen waren Änderungen erforderlich, um dem rein innerstaatlichen Kontext der Bestimmungen Rechnung zu tragen, z. B. in Bezug auf die Frage, „wer“ („who“) die „Angemessenheitsvorschriften“ („adequacy regulations“) für die Zwecke des britischen Datenschutzrechtsrahmens erlässt (siehe Paragraf 17A DPA 2018); diese werden vom Secretary of State anstelle der Europäischen Kommission erlassen.

23 General Data Protection Regulation, Keeling Schedule, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

24 Data Protection Act 2018, Keeling Schedule, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

25 Derartige Befugnisse finden sich beispielsweise in Paragraf 16 (Befugnis, in bestimmten, eng umschriebenen Situationen weitere Ausnahmen von einzelnen Bestimmungen der UK GDPR zu machen), Paragraf 17A (Befugnis, Angemessenheitsvorschriften zu erlassen), Paragrafen 212 und 213 (Befugnisse, Rechtsvorschriften auf den Weg zu bringen und Übergangsbestimmungen zu erlassen) und Paragraf 211 (Befugnis, geringfügige Änderungen und Folgeänderungen vorzunehmen) des DPA 2018.

www.parlament.gv.at

2019) erlassen, in denen festgelegt ist, unter welchen Umständen Verantwortliche eine jährliche Gebühr an die unabhängige Datenschutzbehörde des Vereinigten Königreichs, den Information Commissioner, zahlen müssen.

(18) Weitere Hinweise zu den Datenschutzgesetzen des Vereinigten Königreichs finden sich schließlich in den Verhaltenskodizes und anderen vom Information Commissioner verabschiedeten Leitlinien. Obwohl sie formal nicht rechtsverbindlich sind, sind diese Leitlinien maßgeblich für Zwecke der Auslegung und legen dar, wie die Datenschutzgesetze in der Praxis angewendet und vom Commissioner durchgesetzt werden. Insbesondere ist der Information Commissioner gemäß den Paragrafen 121 bis 125 DPA 2018 verpflichtet, Verhaltenskodizes zu Datenaustausch, Direktwerbung, altersgerechter Gestaltung und altersgerechtem Datenschutz sowie Journalismus zu erstellen.

(19) Somit ist der britische Rechtsrahmen für Daten, die gemäß diesem Beschluss übermittelt werden, seiner Struktur und seinen wesentlichen Bestandteilen nach dem in der Europäischen Union 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

(20) Ähnlich wie die Verordnung (EU) 2016/679 gilt die UK GDPR für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten oder für andere Arten der Verarbeitung, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind.[26] Die Begriffsbestimmungen der Begriffe „personenbezogene Daten“ („personal data“), „betroffene Person“ („data subject“) und „Verarbeitung“ („processing“) der UK GDPR sind identisch mit denen der Verordnung (EU) 2016/679.[27] Darüber hinaus gilt die UK GDPR für die manuelle, unstrukturierte Verarbeitung personenbezogener Daten[28], die sich im Besitz bestimmter Behörden des Vereinigten Königreichs befinden[29], wenngleich die Grundsätze und Rechte der UK GDPR, die für derartige personenbezogene Daten nicht relevant sind, durch die Paragrafen 24 und 25 DPA 2018 außer Kraft gesetzt werden. Ähnlich wie die Verordnung (EU) 2016/679 gilt die UK GDPR nicht für die Verarbeitung

---

26 Artikel 2 Absätze 1 und 5 UK GDPR.

27 Artikel 4 Absätze 1 und 2 UK GDPR.

28 Die manuelle, unstrukturierte Verarbeitung personenbezogener Daten wird in Artikel 2 Absatz 5 Buchstabe b definiert als die Verarbeitung personenbezogener Daten, die nicht der automatisierten oder strukturierten Verarbeitung personenbezogener Daten entspricht.

29 Gemäß Artikel 2 Absatz 1A UK GDPR gilt die Verordnung auch für die manuelle, unstrukturierte Verarbeitung von personenbezogenen Daten, die sich im Besitz einer Behörde im Sinne des Gesetzes über die Informationsfreiheit (Freedom of Information Act) befindet. Der Verweis auf derartige Behörden bezieht sich auf alle Behörden im Sinne des Freedom of Information Act 2000 bzw. alle schottischen Behörden im Sinne des Freedom of Information (Scotland) Act 2002 (asp 13). Paragraf 21 Absatz 5 DPA 2018.

www.parlament.gv.at

personenbezogener Daten durch eine Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.[30]

(21) Der Anwendungsbereich der UK GDPR erstreckt sich zudem auf die Verarbeitung zur Ausübung einer Tätigkeit, die unmittelbar vor dem Ende des Übergangszeitraums nicht im Anwendungsbereich des Unionsrechts lag (z. B. nationale Sicherheit)[31] oder in den Anwendungsbereich von Titel 5 Kapitel 2 des Vertrags über die Europäische Union fiel (Tätigkeiten der Gemeinsamen Außen- und Sicherheitspolitik).[32] Wie im System der Europäischen Union gilt die UK GDPR nicht für die Verarbeitung personenbezogener Daten durch eine zuständige Behörde 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 („Zwecke der Strafverfolgung“ („law enforcement purposes“)) – eine derartige Verarbeitung wird stattdessen durch Teil 3 des DPA 2018 geregelt, so wie es nach dem Recht der Europäischen Union auch für die Richtlinie (EU) 2016/680 der Fall ist – oder für die Verarbeitung personenbezogener Daten durch Nachrichtendienste (den Security Service, den Secret Intelligence Service und die Government Communications Headquarters), die Gegenstand von Teil 4 des DPA 2018 ist.[33]

(22) Der räumliche Anwendungsbereich der UK GDPR ist in Artikel 3 der UK GDPR festgelegt[34] und erstreckt sich auf die Verarbeitung personenbezogener Daten (unabhängig davon, wo sie stattfindet), soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters im Vereinigten Königreich erfolgt, sowie auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich im Vereinigten Königreich aufhalten, wenn die Verarbeitungstätigkeiten mit dem Angebot von Waren oder Dienstleistungen für diese betroffenen Personen oder der Beobachtung ihres Verhaltens im Zusammenhang stehen.[35] Dies entspricht dem Ansatz von Artikel 3 der Verordnung (EU) 2016/679.

---

30 Artikel 2 Absatz 2 Buchstabe a der UK GDPR.

31 Tätigkeiten im Bereich der nationalen Sicherheit fallen nur insoweit in den Anwendungsbereich der UK GDPR, als sie nicht von einer zuständigen Behörde zu Strafverfolgungszwecken durchgeführt werden – in diesem Fall gilt Teil 3 des DPA 2018 – oder nicht von einem Nachrichtendienst oder im Auftrag eines Nachrichtendienstes durchgeführt werden, dessen Tätigkeiten gemäß Artikel 2 Absatz 2 Buchstabe c UK GDPR aus dem Anwendungsbereich der UK GDPR herausgenommen sind und Teil 4 des DPA 2018 unterliegen. Zum Beispiel kann die Polizei Sicherheitsüberprüfungen bei einem Mitarbeiter durchführen, um sicherzustellen, dass er vertrauenswürdig ist, um Zugang zu für die nationale Sicherheit relevanten Materialien zu erhalten. Obwohl die Polizei eine zuständige Behörde für Strafverfolgungszwecke ist, dient die fragliche Verarbeitung nicht einem Strafverfolgungszweck und somit würde die UK GDPR gelten. Siehe Explanatory Framework for Adequacy Discussions, Section H: National Security Data Protection and Investigatory Powers Framework, S. 8, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

32 Artikel 2 Absatz 1 Buchstaben a und b UK GDPR.

33 Artikel 2 Absatz 2 Buchstaben b und c UK GDPR.

34 Der gleiche räumliche Anwendungsbereich gilt für die Verarbeitung personenbezogener Daten gemäß Teil 2 des DPA 2018, der die UK GDPR ergänzt (Paragraf 207 Absatz 1A).

35 Somit finden der DPA 2018 und folglich auch dieser Beschluss keine Anwendung auf die unmittelbar der britischen Krone unterstehenden Gebiete (Jersey, Guernsey und die Insel Man) und die überseeischen Gebiete des Vereinigten Königreichs wie z. B. die Falklandinseln und das Gebiet Gibraltar.

www.parlament.gv.at

2.4. Bestimmung der Begriffe „personenbezogene Daten“ sowie „Verantwortlicher“ und „Auftragsverarbeiter“

(23) Die Definitionen der Begriffe „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“ und „Auftragsverarbeiter“ sowie die Definition des Begriffs „Pseudonymisierung“, die in der Verordnung (EU) 2016/679 festgelegt sind, wurden ohne wesentliche Änderungen in die UK GDPR übernommen.[36] Darüber hinaus sind in Artikel 9 Absatz 1 UK GDPR besondere Kategorien von Daten in gleicher Weise definiert wie in der Verordnung (EU) 2016/679 („Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie […] genetische[n] Daten, biometrische[n] Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“). In Paragraf 205 DPA 2018 sind die Ausdrücke „biometrische Daten“ („biometric data“)[37], „Gesundheitsdaten“ („data concerning health“)[38] und „genetische Daten“ („genetic data“)[39] definiert.

2.5. Garantien, Rechte und Pflichten

2.5.1. Rechtmäßigkeit der Verarbeitung und Verarbeitung nach Treu und Glauben

(24) Die Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen.

(25) Die Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben sowie der Transparenz und die Gründe für eine rechtmäßige Verarbeitung werden im Recht des Vereinigten Königreichs durch Artikel 5 Absatz 1 Buchstabe a und Artikel 6 Absatz 1 der UK GDPR gewährleistet, die mit den entsprechenden Bestimmungen der Verordnung (EU) 2016/679 identisch sind.[40] Paragraf 8 DPA 2018 ergänzt Artikel 6

---

36 Artikel 4 Absätze 1, 2, 5, 7 und 8 UK GDPR.

37 Der Begriff „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.

38 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.

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

40 Gemäß Artikel 6 Absatz 1 UK GDPR ist die Verarbeitung nur dann rechtmäßig, wenn: a) die betroffene Person ihre Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat, b) die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen auf Antrag der betroffenen Person erforderlich ist, c) die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt, d) die Verarbeitung für den Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist, e) die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem Verantwortlichen übertragen wurde, oder f) die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

www.parlament.gv.at

Absatz 1 Buchstabe e; darin ist vorgesehen, dass die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe e UK GDPR (die zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt durch den Verantwortlichen erfolgt, erforderlich ist) auch die Verarbeitung personenbezogener Daten umfasst, die erforderlich ist für die Rechtspflege, die Ausübung einer Funktion einer der beiden Kammern des Parlaments, die Ausübung einer Funktion, die einer Person durch einen Rechtsetzungsakt oder eine Rechtsvorschrift übertragen wurde, die Ausübung einer Funktion der Krone, eines Ministers der Krone oder eines Ministeriums oder eine Aktivität, die demokratisches Engagement unterstützt oder fördert.

(26) In Bezug auf die Einwilligung (einer der Gründe für eine rechtmäßige Verarbeitung) behält die UK GDPR ebenfalls die in Artikel 7 der Verordnung (EU) 2016/679 vorgesehenen Bedingungen unverändert bei. Somit gilt Folgendes: Der Verantwortliche muss nachweisen können, dass die betroffene Person eingewilligt hat; ein schriftliches Ersuchen zur Einwilligung muss in einer klaren und einfachen Sprache erfolgen; die betroffene Person muss das Recht haben, ihre Einwilligung jederzeit zu widerrufen; und bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, sollte dem Umstand Rechnung getragen werden, ob die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Darüber hinaus ist gemäß Artikel 8 der UK GDPR im Zusammenhang mit der Bereitstellung von Diensten der Informationsgesellschaft die Einwilligung eines Kindes nur dann rechtmäßig, wenn das Kind mindestens 13 Jahre alt ist. Dieses Alter liegt innerhalb der Altersgrenze, die in Artikel 8 der Verordnung (EU) 2016/679 festgelegt ist.

2.5.2. Verarbeitung besonderer Kategorien von personenbezogenen Daten

(27) Wenn besondere Kategorien („special categories“) von Daten verarbeitet werden, sollten besondere Garantien vorhanden sein.

(28) Die UK GDPR und der DPA 2018 enthalten spezifische Vorschriften für die Verarbeitung besonderer Kategorien personenbezogener Daten; diese sind in Artikel 9 Absatz 1 der UK GDPR auf die gleiche Weise definiert wie in der Verordnung (EU) 2016/679 (siehe Erwägungsgrund 23 oben). Gemäß Artikel 9 UK GDPR ist die Verarbeitung besonderer Datenkategorien grundsätzlich verboten, es sei denn, es gilt eine spezifische Ausnahme.

(29) Diese (in Artikel 9 Absätze 2 und 3 der UK GDPR aufgeführten) Ausnahmen unterscheiden sich inhaltlich nicht von den Ausnahmen gemäß Artikel 9 Absätze 2 und 3 der Verordnung (EU) 2016/679. Sofern die betroffene Person nicht ausdrücklich in die Verarbeitung dieser personenbezogenen Daten eingewilligt hat, ist die Verarbeitung besonderer Kategorien personenbezogener Daten nur unter bestimmten und begrenzten Umständen zulässig. In den meisten Fällen muss die Verarbeitung sensibler Daten für einen bestimmten, in der entsprechenden Bestimmung festgelegten Zweck erforderlich sein (siehe Artikel 9 Absatz 2 Buchstaben b, c, f, g, h, i und j).

(30) Ferner gilt: Wenn eine Ausnahme gemäß Artikel 9 Absatz 2 UK GDPR eine gesetzliche Genehmigung erfordert oder sich auf das öffentliche Interesse bezieht, sind in Paragraf 10 DPA 2018 in Verbindung mit Anhang 1 des DPA 2018 die Bedingungen festgelegt, die erfüllt sein müssen, damit die Ausnahmen geltend gemacht werden können. Beispielsweise ist für den Fall der Verarbeitung sensibler Daten zum Schutz der öffentlichen Gesundheit („public health“) (Artikel 9 Absatz 2 Buchstabe i UK GDPR) in Anhang 1 Teil 1 Nummer 3 Buchstabe b festgelegt, dass

www.parlament.gv.at

zusätzlich zur Erforderlichkeitsprüfung eine solche Verarbeitung „von medizinischem Fachpersonal oder unter dessen Verantwortung“ oder „von einer anderen Person, die aufgrund eines Rechtsetzungsaktes oder einer Rechtsvorschrift [einschließlich gemäß der etablierten gewohnheitsrechtlichen Pflicht zur Vertraulichkeit] zur Vertraulichkeit verpflichtet ist“, durchgeführt werden muss.

(31) Für Fälle, in denen sensible Daten aus Gründen eines erheblichen öffentlichen Interesses verarbeitet werden (Artikel 9 Absatz 2 Buchstabe g UK GDPR), enthält Anhang 1 Teil 2 des DPA 2018 eine erschöpfende Liste von Zwecken, die als erhebliches öffentliches Interesse angesehen werden können, sowie für jeden dieser Zwecke spezifische zusätzliche Bedingungen. So gilt beispielsweise die Förderung der kulturellen und ethnischen Vielfalt in der Führungsebene von Organisationen als erhebliches öffentliches Interesse. Die Verarbeitung sensibler Daten für diesen speziellen Zweck unterliegt genauen Anforderungen; unter anderem muss die Verarbeitung als Teil eines Prozesses zur Ermittlung geeigneter Personen für die Besetzung von Führungspositionen erfolgen sowie zur Förderung der kulturellen und ethnischen Vielfalt erforderlich sein und darf nicht die Gefahr bestehen, dass der betroffenen Person erheblicher Schaden oder erhebliches Leid zugefügt wird.

(32) In Paragraf 11 Absatz 1 DPA 2018 sind die Bedingungen für die Verarbeitung personenbezogener Daten unter den in Artikel 9 Absatz 3 UK GDPR aufgeführten Umständen in Bezug auf die Geheimhaltungspflicht festgelegt. Dazu zählen Umstände, in denen die Verarbeitung von medizinischem oder sozialem Fachpersonal oder unter dessen Verantwortung oder von einer anderen Person, die unter den gegebenen Umständen aufgrund eines Rechtsetzungsakts oder einer Rechtsvorschrift zur Vertraulichkeit verpflichtet ist, durchgeführt wird.

(33) Darüber hinaus erfordern zahlreiche der Ausnahmen, die in Artikel 9 Absatz 2 UK GDPR aufgeführt sind, geeignete und spezifische Garantien, damit sie geltend gemacht werden können. Je nach Art der Verarbeitung und der Höhe des Risikos für die Rechte und Freiheiten der betroffenen Personen umfassen die in Anhang 1 des DPA 2018 vorgesehenen Bedingungen für die Verarbeitung unterschiedliche Garantien. In Anhang 1 wiederum sind die Bedingungen für jede Verarbeitungssituation aufgeführt.

(34) In einigen Fällen regelt und begrenzt der DPA 2018 die Art der sensiblen Daten, die verarbeitet werden dürfen, damit eine bestimmte Rechtsgrundlage erfüllt ist. Gemäß Anhang 1 Nummer 8 beispielsweise ist die Verarbeitung sensibler Daten zum Zweck der Förderung der Chancengleichheit oder der Gleichbehandlung zulässig. Diese Verarbeitungsbedingung kann nur dann geltend gemacht werden, wenn aus den Daten die rassische oder ethnische Herkunft, religiöse oder philosophische Überzeugungen oder die sexuelle Orientierung hervorgehen oder wenn es sich um Gesundheitsdaten handelt.

(35) In einigen Fällen enthält der DPA 2018 eine Einschränkung dahin gehend, welche Art von Verantwortlichen die Verarbeitungsbedingung geltend machen darf. In Anhang 1 Nummer 23 beispielsweise ist die Verarbeitung sensibler Daten im Zusammenhang mit Antworten gewählter Vertreter an die Öffentlichkeit vorgesehen. Diese Verarbeitungsbedingung kann nur dann geltend gemacht werden, wenn der Verantwortliche der gewählte Vertreter ist oder unter dessen Aufsicht handelt.

(36) In einigen anderen Fällen enthält der DPA 2018 Beschränkungen bezüglich der Kategorien von betroffenen Personen, für die eine bestimmte Verarbeitungsbedingung geltend gemacht werden darf. In Anhang 1 Nummer 21 ist beispielsweise die

www.parlament.gv.at

Verarbeitung sensibler Daten für betriebliche Altersversorgungssysteme geregelt. Diese Bedingung kann nur dann geltend gemacht werden, wenn es sich bei der betroffenen Person um ein Geschwister-, Eltern-, Großeltern- oder Urgroßelternteil des Versorgungsanwärters handelt.

(37) Darüber hinaus muss der Verantwortliche, wenn er die Ausnahmen in Artikel 9 Absatz 2 UK GDPR geltend macht, die in Paragraf 10 DPA 2018 in Verbindung mit Anhang 1 des DPA 2018 weiter spezifiziert werden, in den meisten Fällen eine angemessene Dokumentation („appropriate policy document“) vorlegen. Darin sind die Verfahren zu beschreiben, mit denen der Verantwortliche die Einhaltung der Grundsätze nach Artikel 5 UK GDPR gewährleistet. Darüber hinaus müssen die Verfahren zur Speicherung und Löschung dargelegt und die wahrscheinliche Speicherdauer angegeben werden. Die Verantwortlichen müssen diese Dokumentation überprüfen und gegebenenfalls aktualisieren. Der Verantwortliche muss die Dokumentation nach Abschluss der Verarbeitung noch sechs Monate aufbewahren und dem Information Commissioner auf Anfrage zur Verfügung stellen.[41]

(38) Gemäß Anhang 1 Nummer 41 des DPA 2018 muss die Dokumentation stets auch ein erweitertes Verzeichnis der Verarbeitungstätigkeiten umfassen. Darin sind die in der Dokumentation enthaltenen Verpflichtungen darzulegen, d. h., ob Daten in Übereinstimmung mit den Strategien gelöscht oder gespeichert werden. Wenn die Strategien nicht befolgt wurden, müssen in diesem Verzeichnis die Gründe dafür festgehalten werden. Ferner ist darin anzugeben, inwieweit die Verarbeitung Artikel 6 UK GDPR (Rechtmäßigkeit der Verarbeitung) und der spezifischen geltend gemachten Bedingung in Anhang 1 des DPA 2018 entspricht.

(39) Schließlich enthält die UK GDPR ebenso wie die Verordnung (EU) 2016/679 auch allgemeine Garantien für bestimmte Verarbeitungsvorgänge im Zusammenhang mit besonderen Kategorien von Daten. Gemäß Artikel 35 UK GDPR ist eine Datenschutz-Folgenabschätzung vorgeschrieben, wenn besondere Kategorien von Daten in großem Umfang verarbeitet werden. Nach Artikel 37 UK GDPR muss ein Verantwortlicher oder ein Auftragsverarbeiter einen Datenschutzbeauftragten benennen, wenn seine Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten besteht.

(40) In Bezug auf die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten ist Artikel 10 UK GDPR identisch mit Artikel 10 der Verordnung (EU) 2016/679. Demnach darf die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem innerstaatlichen Recht, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist.

(41) Wenn die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten nicht unter behördlicher Aufsicht erfolgt, gilt nach Paragraf 10 Absatz 5 DPA 2018, dass eine solche Verarbeitung nur für die spezifischen Zwecke/in den spezifischen Situationen erfolgen kann, die in Anhang 1 Teile 1, 2 und 3 des DPA 2018 aufgeführt sind, und dass die Verarbeitung den spezifischen Anforderungen unterliegt, die für jeden dieser Zwecke/jede dieser Situationen aufgeführt sind. So können beispielsweise Daten über strafrechtliche Verurteilungen von Organisationen ohne

[41] Anhang 1 Nummern 38 bis 40 des DPA 2018.

www.parlament.gv.at

Gewinnerzielungsabsicht verarbeitet werden, wenn die Verarbeitung a) auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und b) unter der Voraussetzung erfolgt, dass i) sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und ii) die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

(42) Darüber hinaus sind in Anhang 1 Teil 3 des DPA 2018 weitere Umstände aufgeführt, unter denen Daten über strafrechtliche Verurteilungen verwendet werden dürfen; diese Umstände entsprechen den Rechtsgrundlagen für die Verarbeitung sensibler Daten in Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 und der UK GDPR (z. B. Einwilligung der betroffenen Person, lebenswichtige Interessen einer Person, wenn die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben, wenn die Daten von der betroffenen Person bereits offensichtlich öffentlich gemacht wurden, wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist usw.).

2.5.3 Zweckbindung, Richtigkeit, Datenminimierung, Speicherbegrenzung und Datensicherheit

(43) Personenbezogene Daten sollten für einen bestimmten Zweck verarbeitet und anschließend nur verwendet werden, soweit dies mit dem Zweck der Verarbeitung nicht unvereinbar ist.

(44) Dieser Grundsatz ist in Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 festgehalten und wurde unverändert in Artikel 5 Absatz 1 Buchstabe b UK GDPR übernommen. Die Bedingungen für die mit dem ursprünglichen Erhebungszweck vereinbare Weiterverarbeitung gemäß Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 wurden ebenfalls ohne wesentliche Änderungen in Artikel 6 Absatz 4 Buchstaben a bis e UK GDPR übernommen.

(45) Darüber hinaus müssen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Ferner müssen sie dem Zweck angemessen und dafür erheblich sein und dürfen das für die Zwecke der Verarbeitung notwendige Maß nicht überschreiten und sollten grundsätzlich nicht länger gespeichert werden, als dies für den Zweck, zu dem sie verarbeitet werden, erforderlich ist.

(46) Diese Grundsätze der Datenminimierung, Richtigkeit und Speicherbegrenzung sind in Artikel 5 Absatz 1 Buchstaben c bis e der Verordnung (EU) 2016/679 dargelegt und wurden ohne Änderungen in Artikel 5 Absatz 1 Buchstaben c bis e UK GDPR übernommen.

(47) Personenbezogene Daten müssen zudem 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 Unternehmer 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.

www.parlament.gv.at

(48) Die Datensicherheit ist im Recht des Vereinigten Königreichs durch den Grundsatz der Integrität und Vertraulichkeit in Artikel 5 Absatz 1 Buchstabe f UK GDPR sowie in Artikel 32 UK GDPR über die Sicherheit der Verarbeitung verankert. Diese Bestimmungen sind identisch mit den entsprechenden Bestimmungen der Verordnung (EU) 2016/679. Darüber hinaus verlangt die UK GDPR unter den gleichen Bedingungen wie denen in den Artikeln 33 und 34 der Verordnung (EU) 2016/679 die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Artikel 33 UK GDPR) und die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Artikel 34 UK GDPR).

2.5.4 Transparenz

(49) Betroffene Personen müssen über die Hauptmerkmale der Verarbeitung ihrer personenbezogenen Daten unterrichtet werden.

(50) Dies wird durch die Artikel 13 und 14 UK GDPR sichergestellt, die neben einem allgemeinen Grundsatz der Transparenz auch Vorschriften dazu enthalten, welche Informationen der betroffenen Person zur Verfügung gestellt werden müssen.[42] Mit der UK GDPR wurden keine wesentlichen Änderungen dieser Vorschriften gegenüber den entsprechenden Artikeln der Verordnung (EU) 2016/679 eingeführt. Wie in der Verordnung (EU) 2016/679 unterliegen die Transparenzanforderungen dieser Artikel jedoch einer Reihe von Ausnahmen, die im DPA 2018 festgelegt sind (siehe Erwägungsgründe 55 bis 72).

2.5.5 Rechte des Einzelnen

(51) Betroffene Personen sollten bestimmte Rechte besitzen, die gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter durchgesetzt werden können, insbesondere ein Auskunftsrecht, das Recht, der Verarbeitung zu widersprechen, und das Recht auf Berichtigung und Löschung von Daten. Gleichzeitig können diese Rechte Beschränkungen unterliegen, soweit diese Beschränkungen zur Aufrechterhaltung der öffentlichen Sicherheit oder zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses notwendig und verhältnismäßig sind.

2.5.5.1 Die substanziellen Rechte

(52) Die UK GDPR gewährt Einzelpersonen die gleichen durchsetzbaren Rechte wie die Verordnung (EU) 2016/679. Die Bestimmungen zu den Rechten des Einzelnen wurden ohne wesentliche Änderungen in der UK GDPR beibehalten.

---

42 In Artikel 13 Absatz 1 Buchstabe f und Artikel 14 Absatz 1 Buchstabe f wurden die Verweise auf Angemessenheitsbeschlüsse der Kommission durch Verweise auf ein gleichwertiges Instrument des Vereinigten Königreichs, nämlich die Angemessenheitsvorschriften im Sinne des DPA 2018, ersetzt. Darüber hinaus wurden in Artikel 14 Absatz 5 Buchstaben c bis d die Verweise auf das Recht der EU oder der Mitgliedstaaten durch Verweise auf innerstaatliches Recht ersetzt (als Beispiele für derartige innerstaatliche Rechtsvorschriften, die unter Artikel 14 Absatz 5 Buchstabe c fallen können, nennt das Vereinigte Königreich Paragraf 7 des Gesetzes über Altmetallhändler von 2013 (Scrap Metal Dealers Act 2013), der Vorschriften für das Register der Lizenzen für Altmetallhändler enthält, oder Teil 35 des Unternehmensgesetzes (Companies Act) von 2006, der die Vorschriften für den Registrar of Companies enthält. Innerstaatliche Rechtsvorschriften, die unter Artikel 14 Absatz 5 Buchstabe d fallen können, wären wiederum solche, in denen Vorschriften für das Berufsgeheimnis oder Verpflichtungen festgelegt sind, die in Arbeitsverträgen enthalten sein müssen oder der gewohnheitsrechtlichen Pflicht zur Vertraulichkeit entsprechen (z. B. personenbezogene Daten, die von medizinischem Fachpersonal, Personalverantwortlichen, Sozialarbeitern usw. verarbeitet werden).

www.parlament.gv.at

(53) Zu diesen Rechten zählen das Auskunftsrecht der betroffenen Person (Artikel 15 UK GDPR), das Recht auf Berichtigung (Artikel 16 UK GDPR), das Recht auf Löschung (Artikel 17 UK GDPR), das Recht auf Einschränkung der Verarbeitung (Artikel 18 UK GDPR), eine Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Artikel 19 UK GDPR), das Recht auf Datenübertragbarkeit (Artikel 20 UK GDPR) und das Widerspruchsrecht (Artikel 21 UK GDPR).[43] Letzteres umfasst auch das in Artikel 21 Absätze 2 und 3 der Verordnung (EU) 2016/679 vorgesehene Recht einer betroffenen Person, Widerspruch gegen die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung einzulegen. Darüber hinaus muss der Information Commissioner gemäß Paragraf 122 DPA 2018 einen Verhaltenskodex (Code of Practice) für die Durchführung von Direktwerbung entsprechend den Anforderungen der Datenschutzgesetze (und der Datenschutzverordnung sowie der Richtlinie über elektronische Kommunikation von 2003) sowie andere derartige Leitlinien zur Förderung der guten Praxis im Bereich der Direktwerbung erstellen, die er für angemessen hält. Das Büro des Information Commissioner Office arbeitet derzeit einen entsprechenden Kodex für Direktwerbung aus.[44]

(54) Das in Artikel 22 DSGVO vorgesehene Recht der betroffenen Person, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wurde ebenfalls ohne wesentliche Änderungen in der UK GDPR beibehalten. Allerdings wurde ein neuer Absatz 3A eingefügt, in dem darauf hingewiesen wird, dass Paragraf 14 DPA 2018 Garantien für die Rechte, Freiheiten und berechtigten Interessen der betroffenen Personen für Fälle enthält, in denen die Verarbeitung gemäß Artikel 22 Absatz 2 Buchstabe b UK GDPR erfolgt. Diese Bestimmung gilt nur, wenn die Grundlage für eine solche Entscheidung eine Genehmigung oder Anforderung nach britischem Recht ist; sie gilt nicht, wenn die Entscheidung im Rahmen eines Vertrags erforderlich ist oder mit der ausdrücklichen Einwilligung der betroffenen Person getroffen wird. Findet Paragraf 14 DPA 2018 Anwendung, muss der Verantwortliche der betroffenen Person so rasch wie nach vernünftigem Ermessen möglich schriftlich mitteilen, dass eine Entscheidung getroffen wurde, die ausschließlich auf einer automatisierten Verarbeitung beruht. Die betroffene Person hat das Recht zu verlangen, dass der Verantwortliche binnen eines Monats nach Erhalt der Mitteilung die Entscheidung überprüft oder eine neue Entscheidung trifft, die nicht ausschließlich auf einer automatisierten Verarbeitung beruht. Der Secretary of State ist befugt, weitere Garantien in Bezug auf die automatisierte Entscheidungsfindung zu erlassen. Von dieser Befugnis wurde bislang noch kein Gebrauch gemacht.

---

43 In Artikel 17 Absatz 1 Buchstabe e und Artikel 17 Absatz 3 Buchstabe b wurden die Verweise auf das Recht der EU oder der Mitgliedstaaten durch Verweise auf innerstaatliches Recht ersetzt (als Beispiele für derartige innerstaatliche Rechtsvorschriften gemäß Artikel 17 Absatz 1 Buchstabe e nennt das Vereinigte Königreich die Bestimmungen über Bildung (Schülerinformationen) (England) ((Education (Pupil Information) (England) Regulations)) von 2006, demnach die Namen von Schülern nach deren Schulabschluss aus Schulregistern zu löschen sind, oder das Medizingesetz (Medical Act) von 1983, Paragraf 34F, in dem die Vorschriften für die Löschung von Namen aus dem Register für Allgemeinmediziner und dem Register für Fachmediziner festgelegt sind).

44 Der Entwurf dieses Code of Practice ist unter folgendem Link abrufbar: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

www.parlament.gv.at

2.5.5.2 Beschränkungen der Rechte des Einzelnen und andere Bestimmungen

(55) Im DPA 2018 sind mehrere Beschränkungen der Rechte des Einzelnen vorgesehen, die sich in den Rahmen von Artikel 23 der UK GDPR einfügen. Mit diesem Rahmen werden keine Beschränkungen des in Artikel 21 Absätze 2 und 3 UK GDPR vorgesehenen Rechts auf Widerspruch gegen Direktwerbung oder des in Artikel 22 UK GDPR vorgesehenen Rechts, keiner automatisierten Entscheidungsfindung unterworfen zu werden, eingeführt.

(56) Die Beschränkungen sind in den Anhängen 2 bis 4 des DPA 2018 aufgeführt. Nach Angaben der britischen Behörden orientieren sich diese Beschränkungen an zwei Grundsätzen, und zwar dem Grundsatz der Spezifizität (ein detaillierter Ansatz, bei dem allgemeine Beschränkungen in verschiedene spezifischere Bestimmungen aufgeteilt werden) und dem Grundsatz der Konditionalität (jede Bestimmung wird durch Garantien in Form von Einschränkungen oder Bedingungen zur Verhinderung von Missbrauch ergänzt).[45]

(57) Die in Artikel 23 Absatz 1 UK GDPR vorgesehenen Beschränkungen sind dergestalt, dass sie nur unter bestimmten Umständen gelten, wenn sie in einer demokratischen Gesellschaft notwendig sind und in einem angemessenen Verhältnis zu dem mit ihnen verfolgten legitimen Ziel stehen. Darüber hinaus kann in Übereinstimmung mit der ständigen Rechtsprechung zur Auslegung von Beschränkungen eine Ausnahme von den Datenschutzvorschriften in einem bestimmten Fall nur dann angewandt werden, wenn dies erforderlich und verhältnismäßig ist.[46] Bei der Prüfung der Erforderlichkeit muss „streng vorgegangen werden, und jeder Eingriff in die Rechte der betroffenen Person muss in einem angemessenen Verhältnis zur Schwere der Bedrohung des öffentlichen Interesses stehen. Daher umfasst diese Prüfung eine klassische Analyse der Verhältnismäßigkeit.“[47]

(58) Die mit diesen Beschränkungen verfolgten Ziele entsprechen den in Artikel 23 der Verordnung (EU) 2016/679 aufgeführten Zielen, mit Ausnahme der Beschränkungen in Bezug auf die nationale Sicherheit und Verteidigung, die in Paragraf 26 DPA 2018 geregelt sind, jedoch denselben Anforderungen bezüglich Notwendigkeit und Verhältnismäßigkeit unterliegen (siehe Erwägungsgründe 63 bis 66).

(59) Bei einigen der Beschränkungen, z. B. denjenigen, die sich auf die Verhütung oder Aufdeckung von Straftaten, die Ergreifung oder Verfolgung von Straftätern und die Festsetzung oder Erhebung von Steuern oder Abgaben beziehen[48], können sämtliche Rechte des Einzelnen und Transparenzpflichten eingeschränkt werden (mit Ausnahme der Rechte nach Artikel 21 Absatz 2 und Artikel 22). Anderer Beschränkungen beziehen sich ausschließlich auf Transparenzpflichten und Auskunftsrechte, z. B. die Beschränkungen in Bezug auf die Vertraulichkeit der anwaltlichen Korrespondenz[49],

---

45 UK Explanatory Framework for Adequacy Discussions, Section E: Restrictions, S. 1, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

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

47 Guriev/Community Safety Development (United Kingdom) Ltd, [2016] EWHC 643 (QB), Rn. 43. Siehe hierzu auch Lin/Commissioner of Police for the Metropolis, [2015] EWHC 2484 (QB), Rn. 80.

48 Anhang 2 Nummer 2 des DPA 2018.

49 Anhang 2 Nummer 19 des DPA 2018.

www.parlament.gv.at

in Bezug auf das Recht auf Freiheit von der Informationspflicht, wenn man sich dadurch selbst belasten würde[50], und in Bezug auf Unternehmensfinanzierung, insbesondere die Verhinderung von Insiderhandel[51]. Nur wenige Beschränkungen erlauben eine Einschränkung der Pflicht des Verantwortlichen, einer betroffenen Person eine Datenschutzverletzung mitzuteilen, oder eine Einschränkung der Grundsätze der Zweckbindung und der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben sowie der Transparenz der Verarbeitung.[52]

(60) Einige der Beschränkungen gelten automatisch in vollem Umfang („in full") für eine bestimmte Art der Verarbeitung personenbezogener Daten (beispielsweise finden Transparenzpflichten und die Rechte des Einzelnen keine Anwendung, wenn personenbezogene Daten zum Zweck der Beurteilung der Eignung einer Person für ein richterliches Amt verarbeitet werden oder wenn personenbezogene Daten von Gerichten, Tribunalen oder Personen verarbeitet werden, die im Rahmen ihrer justiziellen Tätigkeit handeln).

(61) In den meisten Fällen jedoch besagt die betreffende Nummer in Anhang 2 des DPA 2018, dass die Beschränkung nur dann gilt, wenn (und soweit) durch Anwendung der Bestimmungen das mit dieser Beschränkung verfolgte legitime Ziel „voraussichtlich beeinträchtigt würde" („would be likely to prejudice"): So gelten etwa die in der UK GDPR aufgeführten Bestimmungen nicht für personenbezogene Daten, die zur Verhütung oder Aufdeckung von Straftaten, Ergreifung oder Verfolgung von Straftätern oder Festsetzung oder Erhebung von Steuern oder Abgaben verarbeitet werden, sofern eines dieser Ziele „durch Anwendung dieser Bestimmungen voraussichtlich beeinträchtigt würde".[53]

(62) Die Norm der „voraussichtlichen Beeinträchtigung" wurde von britischen Gerichten stets dahin gehend ausgelegt, dass „eine erhebliche und schwerwiegende Gefahr bestehen muss, dass ein bestimmtes öffentliches Interesse beeinträchtigt wird".[54] Eine der Beeinträchtigungsprüfung unterliegende Beschränkung kann daher nur dann und insoweit in Anspruch genommen werden, als eine erhebliche und schwerwiegende Gefahr besteht, dass die Einräumung eines bestimmten Rechts das betreffende öffentliche Interesse beeinträchtigen würde. Der Verantwortliche muss auf Einzelfallbasis beurteilen, ob diese Bedingungen erfüllt sind.[55]

(63) Zusätzlich zu den in Anhang 2 des DPA 2018 enthaltenen Beschränkungen ist in Paragraf 26 DPA 2018 eine Ausnahme vorgesehen, die auf gewisse Bestimmungen der UK GDPR und des DPA 2018 angewendet werden kann, wenn diese Ausnahme zum Schutz der nationalen Sicherheit oder für Verteidigungszwecke erforderlich ist. Diese Ausnahme gilt für die Datenschutzgrundsätze (mit Ausnahme des Grundsatzes der Rechtmäßigkeit), die Transparenzpflichten, die Rechte der betroffenen Person, die

---

50 Anhang 2 Nummer 20 des DPA 2018.

51 Anhang 2 Nummer 21 des DPA 2018.

52 So sind etwa Beschränkungen des Rechts auf Mitteilung einer Datenschutzverletzung nur dann zulässig, wenn es um Straftaten und Steuern (Anhang 2 Nummer 2 des DPA 2018), die parlamentarischen Vorrechte (Anhang 2 Nummer 13 des DPA 2018) und die Verarbeitung für journalistische, wissenschaftliche, künstlerische und literarische Zwecke (Anhang 2 Nummer 26 des DPA 2018) geht.

53 Anhang 2 Nummer 2 des DPA 2018.

54 R (Lord)/Secretary of State for the Home Department, [2003] EWHC 2073 (Admin), Rn. 100, und Guriev/Community Safety Development (United Kingdom) Ltd, [2016] EWHC 643 (QB), Rn. 43.

55 Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor, Rn. 31.

www.parlament.gv.at

Pflicht zur Mitteilung einer Datenschutzverletzung, die Vorschriften über internationale Übermittlungen, einige der Pflichten und Befugnisse des Information Commissioner sowie die Vorschriften über Rechtsbehelfe, Haftung und Sanktionen, mit Ausnahme der Bestimmung über die allgemeinen Bedingungen für die Verhängung von Geldbußen gemäß Artikel 83 UK GDPR und der Bestimmung über Sanktionen gemäß Artikel 84 UK GDPR. Des Weiteren wird in Paragraf 28 DPA 2018 die Anwendung von Artikel 9 Absatz 1 dahin gehend geändert, dass die Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 Absatz 1 UK GDPR ermöglicht wird, sofern die Verarbeitung zum Schutz der nationalen Sicherheit oder für Verteidigungszwecke und mit geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen durchgeführt wird.[56]

(64) Die Ausnahme kann nur insoweit angewendet werden, als dies zum Schutz der nationalen Sicherheit oder für Verteidigungszwecke erforderlich ist. Wie auch die anderen Ausnahmen, die im DPA 2018 vorgesehen sind, muss diese Ausnahme vom Verantwortlichen auf Einzelfallbasis geprüft und darf nur im Einzelfall geltend gemacht werden. Des Weiteren müssen bei jeder Anwendung der Ausnahme die (durch den Human Rights Act 1998 untermauerten) Menschenrechtsstandards beachtet werden, wonach jeder Eingriff in die Rechte auf Privatsphäre in einer demokratischen Gesellschaft notwendig und verhältnismäßig sein sollte.[57]

(65) Diese Auslegung der Ausnahme wird durch das ICO bestätigt, das ausführliche Leitlinien über die Anwendung der Ausnahme zum Schutz der nationalen Sicherheit oder für Verteidigungszwecke herausgegeben hat, aus denen klar hervorgeht, dass die Ausnahme vom Verantwortlichen auf Einzelfallbasis geprüft werden muss und nur im Einzelfall angewandt werden darf.[58] In den Leitlinien wird insbesondere hervorgehoben, dass es sich nicht um eine pauschale Ausnahme handelt und dass es nicht ausreicht, dass die Daten zu Zwecken der nationalen Sicherheit verarbeitet werden, um die Ausnahme geltend machen zu können. Der Verantwortliche, der sich darauf stützt, muss hingegen belegen, dass eine echte Möglichkeit einer nachteiligen Wirkung auf die nationale Sicherheit besteht, und erforderlichenfalls dem ICO Beweise für die Gründe vorlegen, aus denen er diese Ausnahmeregelung in Anspruch genommen hat. Die Leitlinien enthalten eine Checkliste und eine Reihe von Beispielen, um die Bedingungen für die Inanspruchnahme dieser Ausnahmeregelung zu veranschaulichen.

(66) Die Tatsache, dass die Daten für Zwecke der nationalen Sicherheit oder der Verteidigung verarbeitet werden, reicht somit für sich genommen nicht aus, um die Ausnahme anzuwenden. Ein Verantwortlicher muss die tatsächlichen Folgen für die

---

56 Gemäß den von den britischen Behörden vorgelegten Informationen wenden Verantwortliche bei einer Verarbeitung im Kontext der nationalen Sicherheit in der Regel verstärkte Garantien und Sicherheitsmaßnahmen für die Verarbeitung an, um dem sensiblen Charakter der Verarbeitung Rechnung zu tragen. Welche Garantien jeweils angemessen sind, hängt davon ab, welche Risiken mit der durchgeführten Verarbeitung verbunden sind. Möglich wären etwa Beschränkungen des Zugriffs auf die Daten, sodass nur befugte Personen mit entsprechender Sicherheitsermächtigung darauf zugreifen können, strenge Beschränkungen für den Austausch von Daten und ein hoher Sicherheitsstandard für die Verfahren zur Speicherung von und zum Umgang mit Daten.

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

58 Siehe Leitfaden des ICO über die Ausnahme zum Schutz der nationalen Sicherheit oder für Verteidigungszwecke, abrufbar unter folgendem Link:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

www.parlament.gv.at

nationale Sicherheit berücksichtigen, wenn er die jeweilige Datenschutzbestimmung einhalten müsste. Die Ausnahme darf nur auf die Bestimmungen angewendet werden, von denen das Risiko erwiesenermaßen ausgeht, und muss so restriktiv wie möglich angewendet werden.[59]

(67) Diese Verfahrensweise wurde vom Informationsgericht (Information Tribunal) bestätigt.[60] In der Rechtssache Baker/Secretary of State for the Home Department („Baker/Secretary of State“) stellte das Gericht fest, dass es rechtswidrig war, die Ausnahme zum Schutz der nationalen Sicherheit als pauschale Ausnahme auf die von den Nachrichtendiensten erhaltenen Zugriffsanträge anzuwenden. Stattdessen hätte die Ausnahme auf Einzelfallbasis angewandt werden müssen, indem jeder Antrag für sich und im Hinblick auf das Recht des Einzelnen auf Achtung seines Privatlebens geprüft wird.[61]

2.5.6 Beschränkungen für personenbezogene Daten, die zu journalistischen, künstlerischen, wissenschaftlichen und literarischen Zwecken sowie zu Archiv- und Forschungszwecken verarbeitet werden

(68) Gemäß Artikel 85 Absatz 2 UK GDPR können personenbezogene Daten, die zu journalistischen, künstlerischen, wissenschaftlichen und literarischen Zwecken verarbeitet werden, von mehreren Bestimmungen der UK GDPR ausgenommen werden. In Anhang 2 Teil 5 des DPA 2018 sind die für die Verarbeitung zu diesen Zwecken geltenden Ausnahmen festgelegt. Hierzu zählen Ausnahmen von den Datenschutzgrundsätzen (mit Ausnahme des Grundsatzes der Integrität und Vertraulichkeit), den Rechtsgrundlagen für die Verarbeitung (einschließlich besonderer Datenkategorien und Daten über strafrechtliche Verurteilungen usw.), den Bedingungen für die Einwilligung, den Transparenzpflichten, den Rechten der betroffenen Personen, der Pflicht zur Mitteilung von Datenschutzverletzungen und der Pflicht zur Konsultation des Information Commissioner vor einer risikoreichen Verarbeitung sowie den Vorschriften für internationale Übermittlungen.[62] Diesbezüglich weicht die UK GDPR nicht wesentlich von der Verordnung (EU)

---

59 Die britischen Behörden führen hierzu folgendes Beispiel an: Wenn ein mutmaßlicher Terrorist, gegen den der MI5 aktiv ermittelt, einen Zugriffsantrag beim Innenministerium stellt (z. B. weil er mit dem Innenministerium in einen Streit über Einwanderungsangelegenheiten verwickelt ist), wäre es erforderlich, alle Daten, die der MI5 womöglich mit dem Innenministerium im Zusammenhang mit laufenden Ermittlungen ausgetauscht hat und die sensible Quellen, Methoden oder Techniken beeinträchtigen und/oder zu einer Erhöhung der von der Person ausgehenden Bedrohung führen könnten, vor dem Zugriff durch die betroffene Person zu schützen. Unter derartigen Umständen ist es wahrscheinlich, dass die Schwelle für die Anwendung der Ausnahme gemäß Paragraf 26 erreicht wurde und eine Ausnahme von der Offenlegung der Informationen erforderlich wäre, um die nationale Sicherheit zu schützen. Wenn das Innenministerium jedoch auch personenbezogene Daten über die Person besäße, die sich nicht auf die Ermittlungen des MI5 beziehen, und diese Informationen ohne die Gefahr einer Beeinträchtigung der nationalen Sicherheit zur Verfügung gestellt werden könnten, dann wäre die Ausnahme zum Schutz der nationalen Sicherheit nicht anwendbar, wenn die Weitergabe von Informationen an die Person in Erwägung gezogen wird. Das ICO erstellt derzeit Leitlinien dazu, wie Verantwortliche bei der Anwendung der Ausnahme gemäß Paragraf 26 vorgehen sollten. Die Leitlinien sollten bis Ende März 2021 veröffentlicht werden.

60 Das Information Tribunal wurde eingerichtet, um sich mit Beschwerden im Bereich des Datenschutzes gemäß dem Data Protection Act 1984 zu befassen. Im Jahr 2010 wurde das Information Tribunal im Rahmen der strukturellen Reform des britischen Gerichtssystems Teil der Kammer für allgemeine Regelungen (General Regulatory Chamber) des First-tier Tribunal.

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

62 Siehe Artikel 85 UK GDPR und Anhang 2 Teil 5 Nummer 26 Ziffer 9 des DPA 2018.

www.parlament.gv.at

2016/679 ab, nach deren Artikel 85 ebenfalls die Möglichkeit besteht, Verarbeitungen zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken von einer Reihe von Anforderungen der Verordnung (EU) 2016/679 auszunehmen. Die Bestimmungen des DPA 2018, insbesondere Anhang 2 Teil 5, sind mit der UK GDPR vereinbar.

(69) Die zentrale Abwägung, die nach Artikel 85 UK GDPR zu treffen ist, bezieht sich auf die Frage, ob eine Ausnahme von den Erwägungsgrund 68 genannten Datenschutzvorschriften „erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen“.[63] Um diese Abwägung zu treffen, prüft das Vereinigte Königreich gemäß Anhang 2 Nummer 26 Ziffern 2 und 3 des DPA 2018, ob nach vernünftigem Ermessen von einem bestimmten Sachverhalt ausgegangen werden kann („Reasonable belief“-Prüfung). Damit eine Ausnahme gerechtfertigt ist, muss der Verantwortliche nach vernünftigem Ermessen davon ausgehen, i) dass die Veröffentlichung im öffentlichen Interesse liegt und ii) dass die Anwendung der entsprechenden Bestimmung der GDPR mit journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken unvereinbar wäre. Wie durch die Rechtsprechung bestätigt wurde[64], besitzt die „Reasonable belief“-Prüfung sowohl eine subjektive als auch eine objektive Komponente: Es reicht nicht aus, wenn der Verantwortliche nachweist, dass er selbst davon ausgegangen ist, dass die Einhaltung einer bestimmten Vorschrift unvereinbar war. Seine Einschätzung muss vernünftig sein, d. h., sie könnte von einer vernünftigen Person in Kenntnis der relevanten Fakten geglaubt werden. Der Verantwortliche muss daher bei der Bildung seiner Einschätzung die erforderliche Sorgfalt walten lassen, um die Vernünftigkeit nachweisen zu können. Laut den Erläuterungen der britischen Behörden muss die „Reasonable belief“-Prüfung für jede Ausnahme einzeln durchgeführt werden.[65] Sind

---

63 Gemäß Anhang 2 Teil 5 Nummer 26 Ziffer 2 des DPA 2018 gilt die Ausnahme für die Verarbeitung personenbezogener Daten für besondere Zwecke (journalistische, akademische, künstlerische und literarische Zwecke) dann, wenn die Verarbeitung mit dem Ziel einer Veröffentlichung von journalistischem, akademischem, künstlerischem oder literarischem Material durch eine Person erfolgt und der Verantwortliche nach vernünftigem Ermessen davon ausgeht, dass die Veröffentlichung dieses Materials im öffentlichen Interesse liegt. Bei der Bestimmung dessen, ob eine Veröffentlichung im öffentlichen Interesse liegt, muss der Verantwortliche die besondere Bedeutung des öffentlichen Interesses an der Freiheit der Meinungsäußerung und der Informationsfreiheit berücksichtigen. Darüber hinaus muss der Verantwortliche die für die betreffende Veröffentlichung relevanten Verhaltenskodizes oder Leitlinien berücksichtigen (BBC Editorial Guidelines, Ofcom Broadcasting Code und Editors' Code of Practice). Damit eine Ausnahme zur Anwendung kommt, muss der Verantwortliche ferner nach vernünftigem Ermessen davon ausgehen, dass die Einhaltung der betreffenden Bestimmung mit den besonderen Zwecken unvereinbar wäre (Anhang 2 Nummer 26 Ziffer 3 des DPA 2018).

64 Im Urteil in der Rechtssache NT1/Google, [2018] EWHC 799 (QB), Rn. 102, wurde erörtert, ob der Verantwortliche nach vernünftigem Ermessen davon ausging, dass die Veröffentlichung im öffentlichen Interesse lag und dass die Einhaltung der betreffenden Bestimmungen mit den besonderen Zwecken unvereinbar war. Das Gericht stellte fest, dass Paragraf 32 Absatz 1 Buchstaben b und c des Data Protection Act 1998 ein subjektives und ein objektives Element besitzt: Der Verantwortliche muss nachweisen, dass er der davon ausgegangen ist, dass die Veröffentlichung im öffentlichen Interesse liegt, und dass diese Einschätzung objektiv vernünftig war, und er muss die subjektive Einschätzung nachweisen, dass die Einhaltung der Vorschrift, von der er eine Ausnahme begehrt, mit dem betreffenden besonderen Zweck unvereinbar wäre.

65 Ein Beispiel für die Anwendung der „Reasonable belief“-Prüfung findet sich in der gemäß dem Data Protection Act 1998 erlassenen Entscheidung des ICO, eine Geldstrafe gegen True Visions Productions zu verhängen. Das ICO akzeptierte, dass der Medienverantwortliche subjektiv davon ausging, dass die Einhaltung des ersten Datenschutzgrundsatzes (Verarbeitung nach Treu und Glauben und

www.parlament.gv.at

die Bedingungen erfüllt, gilt die Ausnahme als notwendig und verhältnismäßig nach britischem Recht.

(70) Gemäß Paragraf 124 DPA 2018 soll das ICO einen Verhaltenskodex zu Datenschutz und Journalismus erstellen. Die Arbeiten an diesem Kodex laufen derzeit noch. Im Rahmen des Data Protection Act 1998 wurden Leitlinien zu diesem Thema herausgegeben; darin wird insbesondere betont, dass es für die Inanspruchnahme dieser Ausnahme nicht ausreicht, lediglich festzustellen, dass die Einhaltung einer Bestimmung für Journalisten eine Unannehmlichkeit darstellen würde, sondern dass es ein klares Argument dafür geben muss, dass die betreffende Bestimmung ein Hindernis für einen verantwortungsvollen Journalismus darstellt.[66] Die britische Telekommunikationsaufsicht OFCOM und die BBC (in ihren redaktionellen Leitlinien) haben zudem Anwendungsleitlinien zur Prüfung des öffentlichen Interesses und zur Abwägung zwischen dem öffentlichen Interesse und dem Interesse des Einzelnen an Privatsphäre veröffentlicht.[67] Die Leitlinien enthalten insbesondere Beispiele dafür, welche Informationen als im öffentlichen Interesse liegend angesehen werden können; ferner wird erläutert, dass man in der Lage sein muss, nachzuweisen, dass das öffentliche Interesse unter den besonderen Umständen des Falles die Rechte auf Privatsphäre überwiegt.

(71) Ähnlich wie in Artikel 89 DSGVO vorgesehen, können personenbezogene Daten, die zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden, ebenfalls von einer Reihe gelisteter Bestimmungen der UK GDPR ausgenommen werden[68]. In den Bereichen Forschung und Statistik sind Ausnahmen von den Bestimmungen der UK GDPR in Bezug auf Folgendes möglich: Bestätigung der Verarbeitung und Auskunft über Daten und Garantien für Übermittlungen an Drittländer; Recht auf Berichtigung; Einschränkung der Verarbeitung und Widerspruch gegen die Verarbeitung. In Bezug auf die Archivierung im öffentlichen

---

Rechtmäßigkeit) mit journalistischen Zwecken unvereinbar war. Das ICO akzeptierte jedoch nicht, dass diese Einschätzung objektiv vernünftig war. Die Entscheidung des ICO ist unter folgendem Link abrufbar: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

66 Laut den Leitlinien müssen Organisationen erklären können, weshalb die Einhaltung der jeweiligen Bestimmung des Data Protection Act 1998 mit den Zwecken des Journalismus unvereinbar ist. Insbesondere müssen Verantwortliche eine Abwägung treffen, und zwar zwischen den möglichen nachteiligen Auswirkungen der Einhaltung der Bestimmung auf den Journalismus und den möglichen nachteiligen Auswirkungen der Nichteinhaltung auf die Rechte der betroffenen Person. Wenn ein Journalist seine redaktionellen Ziele nach vernünftigem Ermessen auf eine Weise erreichen kann, die mit den Standardbestimmungen des DPA vereinbar ist, muss er dies tun. Organisationen müssen in der Lage sein, bei jeder Bestimmung, die sie nicht eingehalten haben, zu rechtfertigen, weshalb sie eine Beschränkung angewandt haben. „Data protection and journalism: a guide for the media“, abrufbar unter folgendem Link: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

67 Beispiele für ein öffentliches Interesse wären etwa die Aufdeckung einer Straftat, der Schutz der öffentlichen Gesundheit oder Sicherheit, die Aufdeckung irreführender Behauptungen von Einzelpersonen oder Organisationen oder die Offenlegung von Inkompetenz, die Auswirkungen auf die Öffentlichkeit hat. Siehe die Leitlinien des OFCOM, abrufbar unter folgendem Link: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf, und die redaktionellen Leitlinien der BBC, abrufbar unter folgendem Link: https://www.bbc.com/editorialguidelines/guidelines/privacy.

68 Siehe Artikel 89 UK GDPR und Anhang 2 Teil 6 Nummer 27 Ziffer 2 und Nummer 28 Ziffer 2 des DPA 2018.

www.parlament.gv.at

Interesse sind auch Ausnahmen von der Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung sowie vom Recht auf Datenübertragbarkeit möglich.

(72) Gemäß Anhang 2 Nummer 27 Ziffer 1 und Nummer 28 Ziffer 1 des DPA 2018 sind die Ausnahmen von den Bestimmungen der UK GDPR möglich, wenn die Anwendung der Bestimmungen das Erreichen der betreffenden Zwecke „verhindern oder ernsthaft beeinträchtigen“ würde.[69]

(73) Angesichts ihrer Bedeutung für eine wirksame Ausübung der Rechte des Einzelnen werden alle relevanten Entwicklungen bezüglich der Auslegung der vorgenannten Ausnahmen und ihrer Anwendung in der Praxis (zusätzlich zu der Ausnahme im Zusammenhang mit der Aufrechterhaltung einer wirksamen Einwanderungskontrolle, wie in Erwägungsgrund 6 erläutert), einschließlich aller Weiterentwicklungen in der Rechtsprechung sowie der Leitlinien und Durchsetzungsmaßnahmen des ICO, im Kontext der kontinuierlichen Überwachung dieses Beschlusses gebührend berücksichtigt.[70]

2.5.7 Beschränkungen für Weiterübermittlungen

(74) Das Schutzniveau für personenbezogene Daten, die aus der Europäischen Union an Verantwortliche oder Auftragsverarbeiter 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 des britischen Verantwortlichen oder Auftragsverarbeiters 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. Aus diesem Grund ist die Anwendung der Vorschriften der UK GDPR und des DPA 2018 auf die internationale Übermittlung personenbezogener Daten ein wichtiger Faktor, um die Kontinuität des Schutzes für Fälle zu gewährleisten, in denen personenbezogene Daten im Rahmen dieses Beschlusses aus der Europäischen Union an das Vereinigte Königreich übermittelt werden.

(75) Die Bestimmungen zu internationalen Übermittlungen personenbezogener Daten aus dem Vereinigten Königreich finden sich in den Artikeln 44 bis 49 UK GDPR, ergänzt durch den DPA 2018, und entsprechen inhaltlich den Bestimmungen in Kapitel V der Verordnung (EU) 2016/679.[71] Übermittlungen personenbezogener Daten an ein

---

69 Dies setzt voraus, dass personenbezogene Daten in Übereinstimmung mit Artikel 89 Absatz 1 UK GDPR, ergänzt durch Paragraf 19 DPA 2018, verarbeitet werden.

70 Siehe Erwägungsgründe 281 bis 287.

71 Mit Ausnahme von Artikel 48 der Verordnung (EU) 2016/679, den das Vereinigte Königreich nicht in die UK GDPR übernommen hat. In dieser Hinsicht sei vor allem daran erinnert, dass das Kriterium, anhand dessen bestimmt wird, ob ein angemessenes Schutzniveau gewährleistet ist, nicht „inhaltlich identisch“, sondern „der Sache nach gleichwertig“ lautet, wie der EuGH klargestellt hat (Schrems I, Rn. 73-74) und vom EDPB anerkannt wurde (Referenzgrundlage für Angemessenheit, S. 3). Wie der EDPB in seiner Referenzgrundlage für Angemessenheit erläutert hat, „ist das Ziel also nicht, die europäischen Vorschriften Punkt für Punkt wiederzugeben, sondern vielmehr die wesentlichen Kernanforderungen dieser Vorschriften festzulegen“. Diesbezüglich sei darauf hingewiesen, dass das britische Recht zwar formell keine mit Artikel 48 identische Bestimmung enthält, die gleiche Wirkung aber durch andere rechtliche Bestimmungen und Grundsätze garantiert wird. Das heißt, dass, wenn ein Gericht oder eine Verwaltungsbehörde eines Drittlands einen Antrag auf Übermittlung personenbezogener Daten stellt, personenbezogene Daten nur dann an dieses Drittland übermittelt

www.parlament.gv.at

Drittland oder eine internationale Organisation dürfen nur auf der Grundlage von Angemessenheitsvorschriften („adequacy regulations“ – dem britischen Äquivalent eines Angemessenheitsbeschlusses gemäß der Verordnung (EU) 2016/679) erfolgen; liegen keine Angemessenheitsvorschriften vor, dürfen solche Übermittlungen nur dann erfolgen, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien gemäß Artikel 46 UK GDPR vorgesehen hat. In Ermangelung von Angemessenheitsvorschriften und geeigneten Garantien darf kann eine Übermittlung nur auf der Grundlage von Ausnahmen gemäß Artikel 49 UK GDPR erfolgen.

(76) Die vom Secretary of State erlassenen Angemessenheitsvorschriften können vorsehen, dass ein Drittland (oder ein Gebiet oder ein Sektor in einem Drittland), eine internationale Organisation oder eine Beschreibung[72] eines solchen Landes, Gebiets, Sektors oder einer solchen Organisation ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet. Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus muss der Secretary of State exakt dieselben Elemente berücksichtigen, die die Kommission gemäß Artikel 45 Absatz 2 Buchstaben a bis c der Verordnung (EU) 2016/679 in Verbindung mit dem Erwägungsgrund 104 der Verordnung (EU) 2016/679 und der beibehaltenen Rechtsprechung der EU zu beurteilen hat. Das bedeutet, dass bei der Beurteilung der Angemessenheit des Schutzniveaus eines Drittlandes die Frage maßgeblich sein wird, ob das betreffende Drittland ein Schutzniveau gewährleistet, das dem innerhalb des Vereinigten Königreichs garantierten Schutzniveau „der Sache nach gleichwertig“ ist.

(77) Was das Verfahren betrifft, so gelten für Angemessenheitsvorschriften die „allgemeinen“ („general“) Verfahrensmodalitäten gemäß Paragraf 182 DPA 2018. Nach diesem Verfahren muss der Secretary of State bei einem Vorschlag zum Erlass von Angemessenheitsvorschriften den Information Commissioner konsultieren.[73] Nach ihrer Verabschiedung durch den Secretary of State werden die Vorschriften dem

---

werden dürfen, wenn eine entsprechende internationale Übereinkunft besteht, auf deren Grundlage das Urteil des Drittlandgerichts oder der betreffende Verwaltungsbeschluss im Vereinigten Königreich anerkannt oder vollstreckt wird, oder wenn die Übermittlung auf der Grundlage eines der Übermittlungsmechanismen gemäß Kapitel V der UK GDPR erfolgt. Insbesondere müssen sich die Gerichte im Vereinigten Königreich, um ein ausländisches Urteil zu vollstrecken, auf das Common Law oder ein Gesetz berufen können, das die Vollstreckbarkeit erlaubt. Allerdings lassen weder das Common Law (siehe *Adams and Others* v *Cape Industries Plc.*, [1990] 2 W.L.R. 657) noch andere Gesetze die Vollstreckung ausländischer Urteile zu, die die Übermittlung von Daten ohne eine bestehende internationale Übereinkunft verlangen. Infolgedessen sind Datenanfragen nach britischem Recht nicht durchsetzbar, wenn keine solche internationale Übereinkunft besteht. Zudem unterliegt die Übermittlung personenbezogener Daten an Drittländer – auch auf Antrag eines ausländischen Gerichts oder einer ausländischen Verwaltungsbehörde – weiterhin den in Kapitel V der UK GDPR festgelegten Beschränkungen, die mit den entsprechenden Bestimmungen der Verordnung (EU) 2016/679 identisch sind; sie muss daher auf einem der gemäß Kapitel V zulässigen Gründe für die Übermittlung beruhen und im Einklang mit den gemäß diesem Kapitel geltenden einschlägigen Bedingungen stehen.

72 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).

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

www.parlament.gv.at

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.[74]

(78) Gemäß Paragraf 17B 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. Diese verfahrenstechnischen Aspekte stehen ebenfalls im Einklang mit den entsprechenden Anforderungen der Verordnung (EU) 2016/679.

(79) Liegen keine Angemessenheitsvorschriften vor, können internationale Übermittlungen erfolgen, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien gemäß Artikel 46 UK GDPR vorgesehen hat. Diese Garantien ähneln denen, die in Artikel 46 der Verordnung (EU) 2016/679 festgelegt sind. Sie umfassen rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen, verbindliche interne Datenschutzvorschriften[75], Standarddatenschutzklauseln, genehmigte Verhaltensregeln, genehmigte Zertifizierungsverfahren und – mit Genehmigung des Information Commissioner – Vertragsklauseln für Verträge zwischen Verantwortlichen (oder Auftragsverarbeitern) oder Verwaltungsvereinbarungen zwischen Behörden. Die Bestimmungen wurden jedoch verfahrenstechnisch geändert und an den Rechtsrahmen des Vereinigten Königreichs angepasst; so können gemäß dem DPA 2018 insbesondere die Standarddatenschutzklauseln vom Secretary of State (Paragraf 17C) oder vom Information Commissioner (Paragraf 119A) angenommen werden.

(80) Falls weder ein Angemessenheitsbeschluss noch geeignete Garantien bestehen, kann eine Übermittlung nur auf der Grundlage von Ausnahmen gemäß Artikel 49 der UK GDPR erfolgen.[76] Mit der UK GDPR wurden keine wesentlichen Änderungen der

---

74 Im Falle eines solchen Votums verlieren die Vorschriften endgültig jede Rechtswirkung.

75 Die Bestimmungen von Artikel 47 der Verordnung (EU) 2016/679 wurden in der UK GDPR beibehalten und lediglich geändert, um sie an den innerstaatlichen Kontext anzupassen: So wurden beispielsweise die Verweise auf die zuständige Aufsichtsbehörde durch Verweise auf den Information Commissioner ersetzt, der Verweis auf das Kohärenzverfahren aus Absatz 1 gestrichen und der gesamte Absatz 3 gestrichen.

76 Gemäß Artikel 49 UK GDPR sind Übermittlungen möglich, wenn eine der folgenden Bedingungen erfüllt ist: a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde, b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich, c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich, d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig, e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich, f) die Übermittlung ist zum Schutz lebenswichtiger

www.parlament.gv.at

Ausnahmen gegenüber den entsprechenden Vorschriften der Verordnung (EU) 2016/679 eingeführt. Gemäß der UK GDPR, wie auch gemäß der Verordnung (EU) 2016/679, können bestimmte Ausnahmen nur dann geltend gemacht werden, wenn die Übermittlung gelegentlich erfolgt.[77] Darüber hinaus stellt das ICO in seinen Leitlinien zu internationalen Übermittlungen Folgendes klar: „Diese Regelungen sind nur als echte ‚Ausnahmen' von der allgemeinen Regel anzuwenden, wonach eine eingeschränkte Übertragung nur dann vorgenommen werden sollte, wenn diesbezüglich ein Angemessenheitsbeschluss vorliegt oder geeignete Garantien bestehen."[78] In Bezug auf Übermittlungen, die aus wichtigen Gründen des öffentlichen Interesses notwendig sind (Artikel 49 Absatz 1 Buchstabe d) kann der Secretary of State Verordnungen erlassen, um die Umstände festzulegen, unter denen eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation aus wichtigen Gründen des öffentlichen Interesses erforderlich nicht erforderlich ist. Darüber hinaus kann der Secretary of State im Wege von Verordnungen die Übermittlung einer Kategorie personenbezogener Daten an ein Drittland oder eine internationale Organisation einschränken, wenn die Übermittlung aufgrund von Angemessenheitsvorschriften nicht erfolgen kann und der Secretary of State die Einschränkung aus wichtigen Gründen des öffentlichen Interesses für erforderlich hält. Bislang wurden noch keine derartigen Verordnungen verabschiedet.

(81) Dieser Rahmen für internationale Übermittlungen ist mit Ende des Übergangszeitraums in Kraft getreten.[79] Allerdings sieht Nummer 4 des (durch die DPPEC Regulations eingeführten) Anhangs 21 des DPA 2018 vor, dass bestimmte Übermittlungen personenbezogener Daten ab dem Ende des Übergangszeitraums so behandelt werden, als ob sie auf Angemessenheitsvorschriften beruhten. Hierzu zählen Übermittlungen an einen EWR-Staat, an das Gebiet Gibraltar, an ein Organ, eine Einrichtung, ein Amt oder eine Agentur der Union, das/die durch den EU-Vertrag oder auf der Grundlage des EU-Vertrags errichtet wurde, sowie an Drittländer, für die am Ende des Übergangszeitraums ein Angemessenheitsbeschluss der EU vorlag. Folglich

---

Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben, g) die Übermittlung erfolgt aus einem Register, das gemäß dem innerstaatlichen Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im innerstaatlichen Recht festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind. Ferner gilt: Ist keine der vorgenannten Bedingungen anwendbar, darf eine Übermittlung nur dann erfolgen, wenn sie nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat.

77 Gemäß Erwägungsgrund 111 UK GDPR sind Übermittlungen im Rahmen eines Vertrags oder zur Geltendmachung von Rechtsansprüchen nur dann zulässig, wenn sie gelegentlich erfolgen.

78 ICO guidance on international transfers, abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

79 Während eines Zeitraums von maximal sechs Monaten, der spätestens am 30. Juni 2021 endet, ist die Anwendbarkeit dieses neuen Rahmens 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/DE/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN.

www.parlament.gv.at

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.

(82) Was die künftige Entwicklung der britischen Bestimmungen zu internationalen Übermittlungen – durch die Annahme neuer Angemessenheitsvorschriften, den Abschluss internationaler Übereinkünfte oder die Einführung neuer Übertragungsmechanismen – angeht, so wird die Kommission die Lage genau verfolgen, bewerten, ob die verschiedenen Übertragungsmechanismen in einer Weise angewandt werden, die die Kontinuität des Schutzes gewährleistet, und erforderlichenfalls geeignete Maßnahmen treffen, um gegen etwaige nachteilige Auswirkungen für diese Kontinuität vorzugehen (siehe Erwägungsgründe 278 bis 287). Da die Vorschriften der EU und des Vereinigten Königreichs über internationale Übermittlungen vergleichbar sind, wird davon ausgegangen, dass problematische Unterschiede auch durch Zusammenarbeit, Informations- und Erfahrungsaustausch einschließlich zwischen dem ICO und dem EDPB vermieden werden können.

2.5.8 Rechenschaftspflicht

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

(84) Der in der Verordnung (EU) 2016/679 vorgesehene Grundsatz der Rechenschaftspflicht wurde in Artikel 5 Absatz 2 UK GDPR ohne wesentliche Änderungen beibehalten; dasselbe gilt für Artikel 24 über die Verantwortung des für die Verarbeitung Verantwortlichen, Artikel 25 über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen und Artikel 30 über das Verzeichnis von Verarbeitungstätigkeiten. Artikel 35 über die Datenschutz-Folgenabschätzung und Artikel 36 über die vorherige Konsultation der Aufsichtsbehörde wurden ebenfalls beibehalten. Auch die Artikel 37 bis 39 der Verordnung (EU) 2016/679 über die Benennung und die Aufgaben des Datenschutzbeauftragten wurden ohne wesentliche Änderungen in die UK GDPR übernommen. Des Weiteren wurden die Bestimmungen der Artikel 40 und 42 der Verordnung (EU) 2016/679 über Verhaltensregeln und Zertifizierung in der UK GDPR beibehalten.[80]

2.6 Aufsicht und Durchsetzung

2.6.1 Unabhängige Aufsicht

[80] Soweit erforderlich, wurden diese Verweise durch Verweise auf die britischen Behörden ersetzt. Beispielsweise kann der Information Commissioner oder die nationale Akkreditierungsstelle des Vereinigten Königreichs nach Paragraf 17 DPA 2018 eine Person, die die in Artikel 43 UK GDPR festgelegten Anforderungen erfüllt, zum Zwecke der Überwachung der Einhaltung der Zertifizierung akkreditieren.

www.parlament.gv.at

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

(86) Im Vereinigten Königreich ist der Information Commissioner für die Überwachung und Durchsetzung der Einhaltung der UK GDPR und des DPA 2018 zuständig. 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.[81] Der Information Commissioner wird vom britischen Ministerium für Digitales, Kultur, Medien und Sport gefördert.[82]

(87) Die Unabhängigkeit des Information Commissioner ist in Artikel 52 UK GDPR ausdrücklich verankert, der keine inhaltlichen Änderungen im Vergleich zu Artikel 52 Absätze 1 bis 3 DSGVO umfasst. 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.

(88) Die Bedingungen für die Ernennung und Abberufung des Information Commissioner sind in Anhang 12 des DPA 2018 festgelegt. Der Information Commissioner wird von Ihrer Majestät 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)[83] 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

---

81 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.

82 Die Beziehung zwischen den beiden Institutionen ist in einer Verwaltungsvereinbarung geregelt. Als Fördereinrichtung ist das Ministerium für Digitales, Kultur, Medien und Sports insbesondere dafür zuständig, sicherzustellen, dass der Information Commissioner mit ausreichenden Mitteln und Ressourcen ausgestattet ist, die Interessen des Information Commissioner gegenüber dem Parlament und anderen Regierungsstellen zu vertreten, sicherzustellen, dass ein solider nationaler Datenschutzrahmen vorhanden ist; das Büro des Information Commissioner 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).

83 Governance Code on Public Appointments, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

www.parlament.gv.at

Vorfeld der Ernennung eine Prüfung durchführen. Die entsprechende Stellungnahme des Ausschusses wird veröffentlicht.[84]

(89) Die Amtszeit des Information Commissioner dauert bis zu sieben Jahre. Nach einer Amtszeit kann er nicht wiederernannt werden. Der Information Commissioner kann von Ihrer Majestät nach einer Meinungsäußerung („Address“[85]) beider Kammern des Parlaments seines Amtes enthoben werden. Ein Antrag auf Entlassung des Information Commissioner kann nur dann einer der beiden Kammern des Parlaments vorgelegt werden, wenn ein Minister einen Bericht vorgelegt hat, nach dem er der Auffassung ist, dass der Information Commissioner sich eines schweren Fehlverhaltens schuldig gemacht hat und/oder nicht mehr die Voraussetzungen für die Ausübung seiner Funktionen erfüllt.[86]

(90) Der Information Commissioner bezieht seine finanziellen Mittel aus drei Quellen: i) von den Verantwortlichen entrichtete Datenschutzgebühren, die durch Verordnungen des Secretary of State[87] (Data Protection (Charges and Information) Regulations 2018) festgelegt werden und 85 % bis 90 % des Jahreshaushalts des Büros des Information Commissioner ausmachen[88], ii) Zuschüsse der Regierung an den Information Commissioner, die hauptsächlich der Finanzierung der Betriebskosten des Information Commissioner für nicht datenschutzbezogene Aufgaben dienen[89], und iii) für Dienstleistungen erhobene Gebühren[90]. Derzeit werden keine derartigen Gebühren erhoben.

---

84 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

85 Eine „Address“ ist ein dem Parlament vorgelegter Antrag, mit dem dem Monarchen die Ansichten des Parlaments zu einem bestimmten Thema mitgeteilt werden sollen.

86 Anhang 12 Nummer 3 Ziffer 3 des DPA 2018.

87 Paragraf 137 DPA 2018, siehe Erwägungsgrund 17.

88 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 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.

89 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 82).

90 Siehe Paragraf 134 DPA 2018.

www.parlament.gv.at

(91) Die allgemeinen Aufgaben des Information Commissioner in Bezug auf die Verarbeitung personenbezogener Daten, die im Anwendungsbereich der UK GDPR liegen, sind in Artikel 57 UK GDPR festgelegt, der weitgehend im Einklang mit den entsprechenden Bestimmungen der Verordnung (EU) 2016/679 steht. Seine Aufgaben umfassen die Überwachung und Durchsetzung der UK GDPR, die Sensibilisierung der Öffentlichkeit, die Bearbeitung von Beschwerden betroffener Personen, die Durchführung von Untersuchungen usw. Darüber hinaus sind in Paragraf 115 DPA 2018 weitere allgemeine Aufgaben des Information Commissioner festgelegt, darunter die Pflicht, das Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten des Einzelnen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten, sowie die Befugnis, 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 an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten. 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 oder Tribunal, das im Rahmen seiner justiziellen Tätigkeit handelt, auszuüben. Die Aufsicht über die Justiz wird jedoch durch spezialisierte Stellen gewährleistet (siehe Erwägungsgründe 99 bis 103).

2.6.2 Durchsetzung, einschließlich Sanktionen

(92) Die Befugnisse des Information Commissioner sind in Artikel 58 UK GDPR festgelegt, der keine wesentlichen Änderungen gegenüber dem entsprechenden Artikel der Verordnung (EU) 2016/679 umfasst. Der DPA 2018 enthält ergänzende Vorschriften dazu, wie diese Befugnisse ausgeübt werden können. Der Information Commissioner hat insbesondere die Befugnis, a) im Wege eines Informationsbescheides („information notice“) den Verantwortlichen und den Auftragsverarbeiter (und unter bestimmten Umständen jede andere Person) anzuweisen, erforderliche Informationen bereitzustellen[91], b) Untersuchungen und Überprüfungen durchzuführen, indem er einen Bewertungsbescheid („assessment notice“) 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, Personen zu befragen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten, usw.[92], c) anderweitig Zugriff auf Dokumente usw. von Verantwortlichen und Auftragsverarbeitern zu erhalten und Zugang zu deren Räumlichkeiten gemäß Paragraf 154 DPA 2018 zu erhalten („powers of entry and inspection“), d) 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, einschließlich der Anweisung an den Verantwortlichen oder Auftragsverarbeiter, alle Maßnahmen zu ergreifen, die in Artikel 58 Absatz 2 Buchstaben c bis g und j UK GDPR aufgeführt sind („enforcement notice“)[93], e) im Wege eines Bußgeldbescheides Geldbußen zu

91 Paragraf 142 DPA 2018 (vorbehaltlich der in Paragraf 143 DPA 2018 genannten Einschränkungen).

92 Paragraf 146 DPA 2018 (vorbehaltlich der in Paragraf 147 DPA 2018 genannten Einschränkungen).

93 Paragraf 149 bis 151 DPA 2018 (vorbehaltlich der in Paragraf 152 DPA 2018 genannten Einschränkungen).

www.parlament.gv.at

verhängen („penalty notice“)[94]. Letztere können auch verhängt werden, wenn eine Behörde gegen die Bestimmungen der UK GDPR verstoßen haben.[95]

(93) In den Leitlinien des ICO zu regulatorischen Maßnahmen (Regulatory Action Policy[96]) ist festgelegt, unter welchen Umständen es einen Informations-, Bewertungs- Durchsetzungs- oder Bußgeldbescheid erteilt. Ein Durchsetzungsbescheid, der als Reaktion auf ein Versäumnis eines Verantwortlichen oder Auftragsverarbeiters erteilt wird, darf nur Forderungen enthalten, die der Information Commissioner für die Behebung des Versäumnisses für angemessen hält. Durchsetzungs- und Bußgeldbescheide können einem Verantwortlichen oder einem Auftragsverarbeiter aufgrund von Verstößen gegen Kapitel II der UK GDPR (Grundsätze der Verarbeitung), Artikel 12 bis 22 (Rechte der betroffenen Person), Artikel 25 bis 39 (Pflichten der Verantwortlichen und Auftragsverarbeiter) und Artikel 44 bis 49 (internationale Übermittlungen) der UK GDPR erteilt werden. Ein Durchsetzungsbescheid kann zudem dann erteilt werden, wenn ein Verantwortlicher einer Aufforderung gemäß den Verordnungen nach Paragraf 137 DPA 2018 zur Zahlung einer Gebühr nicht nachgekommen ist. Darüber hinaus kann eine Überwachungsstelle nach Artikel 41 oder einer Zertifizierungsstelle einen Durchsetzungsbescheid erhalten, wenn sie ihren Verpflichtungen im Rahmen der UK GDPR nicht nachkommt. Ferner kann ein Bußgeldbescheid einer Person erteilt werden, die einem Informationsbescheid, einem Bewertungsbescheid oder einem Durchsetzungsbescheid nicht nachgekommen ist.

(94) Ein Bußgeldbescheid verpflichtet eine Person, einen im Bescheid genannten Betrag an den Information Commissioner zu zahlen. Bei der Entscheidung, ob und in welcher Höhe ein Bußgeldbescheid erteilt wird, muss der Information Commissioner die in Artikel 83 Absätze 1 und 2 UK GDPR aufgeführten Punkte berücksichtigen, die mit den entsprechenden Bestimmungen der Verordnung (EU) 2016/679 identisch sind.[97] Gemäß Artikel 83 Absätze 4 und 5 liegen die Höchstbeträge der Geldbußen im Falle der Nichteinhaltung der in diesen Bestimmungen genannten Verpflichtungen bei 8 700 000 GBP bzw. 17 500 000 GBP. Im Falle eines Unternehmens kann der Information Commissioner auch Geldbußen in Form eines Prozentsatzes des weltweiten Jahresumsatzes verhängen, falls dieser höher ist. Wie in den entsprechenden Bestimmungen der Verordnung (EU) 2016/679 liegen diese Beträge

---

94 Paragraf 155 DPA 2018 und Artikel 83 UK GDPR.

95 Dies ergibt sich aus Paragraf 155 Absatz 1 des DPA 2018 in Verbindung mit Paragraf 149 Absätze 2 und 5 des DPA 2018 sowie aus Paragraf 156 Absatz 4 des DPA 2018, die die Verhängung von Bußgeldbescheiden nur bezüglich der Crown Estate Commissioners und Verantwortlichen für den Königlichen Haushalt gemäß Paragraf 209 Absatz 4 des DPA 2018 einschränken.

96 Regulatory Action Policy abrufbar unter folgendem Link: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

97 Darunter die Art und Schwere des Verstoßes (unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens), die Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes, jegliche von dem Verantwortlichen getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens, der Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters (unter Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen), etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters, der Umfang der Zusammenarbeit mit dem Information Commissioner, die Kategorien personenbezogener Daten, die von dem Versäumnis betroffen sind, jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

www.parlament.gv.at

gemäß Artikel 83 Absätze 4 und 5 bei 2 % bzw. 4 %. Wird einem Informationsbescheid, Bewertungsbescheid oder Durchsetzungsbescheid nicht nachgekommen, liegt der Höchstbetrag der Geldbuße, die durch einen Bußgeldbescheid verhängt werden kann, bei 17 500 000 GBP oder im Falle eines Unternehmens bei 4 % des weltweiten Jahresumsatzes, je nachdem, welcher der Beträge höher ist.

(95) Die Befugnisse des Information Commissioner wurden durch die UK GDPR in Verbindung mit dem DPA 2018 auch gestärkt. So hat er beispielsweise nun die Möglichkeit, im Rahmen von Bewertungsbescheiden obligatorische Überprüfungen bei sämtlichen Verantwortlichen und Auftragsverarbeitern durchzuführen, während er diese Befugnis nach der vorherigen Rechtsvorschrift, dem Data Protection Act 1998, nur in Bezug auf die Zentralregierung und Gesundheitsorganisationen ausüben konnte und andere der Überprüfung zustimmen mussten.

(96) Seit der Einführung der Verordnung (EU) 2016/679 bearbeitet das ICO rund 40 000 Beschwerden von betroffenen Personen pro Jahr[98] und führt darüber hinaus etwa 2000 Untersuchungen von Amts wegen durch.[99] Ein Großteil der Beschwerden betrifft das Recht auf Auskunft und auf Offenlegung von Daten. Im Anschluss an seine Untersuchungen ergreift der Information Commissioner Durchsetzungsmaßnahmen in einer Vielzahl unterschiedlicher Bereiche. Konkret hat er laut seinem letzten Jahresbericht (2019–2020)[100] während des Berichtszeitraums 54 Informationsbescheide, acht Bewertungsbescheide und sieben Durchsetzungsbescheide erteilt, vier Verwarnungen ausgesprochen, in acht Fällen eine Strafverfolgung eingeleitet und in 15 Fällen Geldbußen verhängt.[101]

---

98 Laut den Angaben der britischen Behörden ergab sich im Berichtszeitraum des Jahresberichts 2019–2020 des Information Commissioner folgendes Bild: In etwa 25 % der Fälle wurde kein Verstoß festgestellt; in etwa 29 % der Fälle wurde die betroffene Person aufgefordert, das Anliegen entweder zum ersten Mal gegenüber dem Verantwortlichen vorzubringen, die Antwort des Verantwortlichen abzuwarten oder einen laufenden Dialog mit dem Verantwortlichen fortzusetzen; in etwa 17 % der Fälle wurde zwar kein Verstoß festgestellt, aber dem Verantwortlichen wurden Ratschläge erteilt; in etwa 25 % der Fälle stellte der Information Commissioner einen Verstoß fest und dem Verantwortlichen wurden entweder Ratschläge erteilt oder er wurde aufgefordert, bestimmte Maßnahmen zu ergreifen; in etwa 3 % der Fälle wurde festgestellt, dass die Beschwerde nicht Gegenstand der Verordnung (EU) 2016/679 ist; und etwa 1 % der Fälle wurde im Rahmen des Europäischen Datenschutzausschusses an eine andere Datenschutzbehörde verwiesen.

99 Das ICO kann diese Untersuchungen auf der Grundlage von Informationen aus verschiedenen Quellen einleiten, darunter Meldungen von Verletzungen des Schutzes personenbezogener Daten, Verweise von anderen britischen Behörden oder ausländischen Datenschutzbehörden sowie Beschwerden von Einzelpersonen oder Organisationen der Zivilgesellschaft.

100 Jahresbericht und Jahresabschluss 2019–2020 des Information Commissioner (siehe Fußnote 81).

101 Laut dem vorherigen Jahresbericht für den Zeitraum 2018–2019 hat der Information Commissioner im Berichtszeitraum 22 Bußgeldbescheide gemäß dem DPA 1998 ausgestellt; die Geldbußen beliefen sich auf einen Gesamtbetrag von 3 010 610 GBP und lagen in zwei Fällen bei 500 000 GBP (dem nach dem DPA 1998 zulässigen Höchstbetrag). Im Jahr 2018 führte der Information Commissioner nach den Enthüllungen von Cambridge Analytica insbesondere eine Untersuchung zur Nutzung von Datenanalysen für politische Zwecke durch. Die Untersuchung führte zu einem Strategiebericht, einer Reihe von Empfehlungen, einer Geldbuße in Höhe von 500 000 GBP gegen Facebook und einem Durchsetzungsbescheid an Aggregate IQ, einen kanadischen Datenvermittler, mit dem das Unternehmen angewiesen wurde, in seinem Besitz befindliche personenbezogene Daten über Bürger und Einwohner des Vereinigten Königreichs zu löschen (siehe 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).

www.parlament.gv.at

(97) Hierzu zählten mehrere beträchtliche Geldbußen, die im Rahmen der Verordnung (EU) 2016/679 und des DPA 2018 verhängt wurden. So verhängte der Information Commissioner im Oktober 2020 eine Geldstrafe in Höhe von 20 Mio. GBP gegen eine britische Fluggesellschaft wegen einer Datenschutzverletzung, von der mehr als 400 000 Kunden betroffen waren. Ende Oktober 2020 wurde gegen eine internationale Hotelkette eine Geldbuße von 18,4 Mio. GBP verhängt, weil sie die personenbezogenen Daten von Millionen von Kunden nicht sicher aufbewahrt hatte, und im November 2020 wurde ein britischer Dienstleister, der Veranstaltungstickets im Internet verkauft, mit einer Geldbuße von 1,25 Mio. GBP belegt, weil er die Zahlungsdaten seiner Kunden nicht geschützt hatte.[102]

(98) Zusätzlich zu den in Erwägungsgrund 92 beschriebenen Durchsetzungsbefugnissen des Information Commissioner stellen bestimmte Verstöße gegen die Datenschutzvorschriften Straftaten dar und können daher strafrechtlich geahndet werden (Paragraf 196 DPA 2018). Hierzu zählen beispielsweise die wissentliche oder leichtfertige Erlangung oder Offenlegung personenbezogener Daten ohne Zustimmung des Verantwortlichen, die Veranlassung der Offenlegung personenbezogener Daten gegenüber einer anderen Person ohne Zustimmung des Verantwortlichen[103], die Re-Identifizierung von anonymisiert vorliegenden personenbezogenen Daten ohne Zustimmung des für die Anonymisierung der personenbezogenen Daten zuständigen Verantwortlichen[104], die vorsätzliche Behinderung des Information Commissioner bei der Ausübung seiner Befugnisse in Bezug auf die Einsichtnahme in personenbezogene Daten gemäß internationalen Verpflichtungen[105], die Abgabe falscher Erklärungen bei der Erwiderung auf einen Informationsbescheid oder die Vernichtung von Informationen im Zusammenhang mit Informations- und Bewertungsbescheiden[106].

2.6.3 Aufsicht über die Justiz

(99) 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 das ICO wahrgenommen. Wenn der Verantwortliche im Rahmen einer justiziellen Tätigkeit handelt, kann das ICO seine Aufsichtsfunktionen nicht wahrnehmen[107] und die Aufsicht erfolgt durch spezielle Stellen. Dies entspricht dem Ansatz gemäß Artikel 55 Absatz 3 der Verordnung (EU) 2016/679.

(100) 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) wahrgenommen.[108] Darüber hinaus haben der Lordoberrichter (Lord

---

102 Eine Zusammenfassung der ergriffenen Durchsetzungsmaßnahmen findet sich auf der Website des ICO unter folgendem Link: https://ico.org.uk/action-weve-taken/enforcement/.

103 Paragraf 170 DPA 2018.

104 Paragraf 171 DPA 2018.

105 Paragraf 119 DPA 2018.

106 Paragrafen 144 und 148 DPA 2018.

107 Paragraf 117 DPA 2018.

108 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

www.parlament.gv.at

Chief Justice) und der Leitende Präsident der Tribunale (Senior President of Tribunals) eine Datenschutzerklärung herausgegeben[109], in der dargelegt ist, wie die Gerichte in England und Wales personenbezogene Daten für eine richterliche Funktion verarbeiten. Die Justizbehörden in Nordirland[110] und Schottland[111] haben ähnliche Erklärungen herausgegeben.

(101) In Nordirland hat der Lord Chief Justice of Northern Ireland zudem einen Richter des High Court zum Richter für Datenaufsicht (Data Supervisory Judge – DSJ) ernannt[112]. 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.[113]

(102) In Schottland hat der Lord President einen Data Supervisory Judge ernannt, der sämtliche Beschwerden aus Gründen des Datenschutzes untersucht. Dies ist in den

---

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.

109 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

110 Die Datenschutzerklärung des Lord Chief Justice von Nordirland ist unter folgendem Link abrufbar: https://judiciaryni.uk/data-privacy.

111 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

112 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.

113 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 Rats, 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.

www.parlament.gv.at

Vorschriften für gerichtliche Beschwerden geregelt, die denen für England und Wales entsprechen.[114]

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

2.6.4 Rechtsmittel

(104) 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.

(105) 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 die UK GDPR vorliegt.[115] Die diesbezüglichen Vorschriften von Artikel 77 der Verordnung (EU) 2016/679 wurden in der UK GDPR ohne wesentliche Änderungen beibehalten. Das Gleiche gilt für Artikel 57 Absatz 1 Buchstabe f und Absatz 2, in denen die Aufgaben des Information Commissioner in Bezug auf die Bearbeitung von Beschwerden festgelegt sind. Wie in den Erwägungsgründen 92 bis 98 oben beschrieben, hat der Information Commissioner die Befugnis, die Einhaltung der UK GDPR und des DPA 2018 durch den Verantwortlichen und den Auftragsverarbeiter zu bewerten, sie im Falle der Nichteinhaltung aufzufordern, notwendige Maßnahmen zu ergreifen oder zu unterlassen, und Geldbußen zu verhängen.

(106) Zweitens besteht gemäß der UK GDPR und dem DPA 2018 das Recht auf einen Rechtsbehelf gegen den Information Commissioner. Nach Artikel 78 Absatz 1 UK GDPR hat eine Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss des Information Commissioner. Im Rahmen der gerichtlichen Überprüfung untersucht der Richter den Beschluss, der in der Klage angefochten wird, und prüft, ob der Information Commissioner rechtmäßig gehandelt hat. Darüber hinaus hat der Beschwerdeführer gemäß Artikel 78 Absatz 2 UK GDPR Zugang zu einem gerichtlichen Rechtsbehelf, wenn der Information Commissioner eine Beschwerde der betroffenen Person nicht angemessen bearbeitet.[116] Er kann bei einem First-tier Tribunal 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.[117] Darüber hinaus kann jede Person, die

---

114 Jede begründete Beschwerde wird vom Data Supervisory Judge untersucht und an den Lord President weitergeleitet; dieser hat die Befugnis, einen Rat, 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).

115 Artikel 77 UK GDPR.

116 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.

117 Artikel 78 Absatz 2 UK GDPR und Paragraf 166 DPA 2018.

www.parlament.gv.at

vom Information Commissioner einen der oben genannten Bescheide (Informations-, Bewertungs-, Durchsetzungs- oder Bußgeldbescheid) erhält, beim First-tier Tribunal Widerspruch einlegen.[118] Ist das Gericht der Ansicht, dass der Beschluss des Information Commissioner rechtswidrig ist oder dieser seinen Ermessensspielraum anders hätte nutzen sollen, muss es dem Widerspruch stattgeben oder den beanstandeten Beschluss durch einen anderen Bescheid oder Beschluss ersetzen, den der Information Commissioner hätte erlassen können.

(107) Drittens können natürliche Personen gemäß Artikel 79 UK GDPR und 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.

(108) Darüber hinaus hat jede Person, der wegen eines Verstoßes gegen die UK GDPR ein materieller oder immaterieller Schaden entstanden ist, nach Artikel 82 UK GDPR und Paragraf 168 DPA 2018 Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Die Vorschriften zu Schadenersatz und Haftung in Artikel 82 Absätze 1 bis 5 UK GDPR sind identisch mit den entsprechenden Vorschriften der Verordnung (EU) 2016/679. Gemäß Paragraf 168 DPA 2018 umfassen immaterielle Schäden auch seelisches Leid. Gemäß Artikel 80 UK GDPR hat die betroffene Person zudem das Recht, ein Vertretungsorgan oder eine Organisation zu beauftragen, die Beschwerde in ihrem Namen (gemäß Artikel 77 UK GDPR) beim Commissioner einzureichen und die Rechte nach Artikel 78 (Recht auf wirksamen gerichtlichen Rechtsbehelf gegen den Commissioner), Artikel 79 (Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter) und Artikel 82 (Haftung und Recht auf Schadenersatz) der UK GDPR in ihrem Namen auszuüben.

(109) Viertens kann jede Person zusätzlich zu den vorgenannten Rechtsbehelfen auf der Grundlage des Human Rights Act 1998 einen Rechtsbehelf vor den Gerichten des Vereinigten Königreichs einlegen, wenn sie der Ansicht ist, dass ihre Rechte, einschließlich der Rechte auf Privatsphäre und Datenschutz, von Behörden verletzt wurden.[119] 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).

(110) Befindet das Gericht eine Handlung einer Behörde für rechtswidrig, so kann es im Rahmen seiner Befugnisse den Rechtsbehelf oder die Abhilfe gewähren oder die

---

118 Artikel 78 Absatz 1 UK GDPR und Paragraf 162 DPA 2018.

119 Paragraf 7 Absatz 1 des Human Rights Act 1998. Nach Paragraf 7 Absatz 7 ist eine Person nur dann Opfer einer rechtswidrigen Handlung, wenn sie Opfer im Sinne von Artikel 34 der Europäischen Menschenrechtskonvention wäre, wenn wegen dieser Handlung ein Verfahren vor dem Europäischen Gerichtshof für Menschenrechte eingeleitet würde.

www.parlament.gv.at

Anordnung treffen, die es für gerecht und angemessen hält.[120] Des Weiteren kann das Gericht eine Bestimmung des Primärrechts für unvereinbar mit einem Konventionsrecht befinden.

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

3. ZUGANG ZU UND VERWENDUNG VON AUS DER EUROPÄISCHEN UNION ÜBERMITTELTEN PERSONENBEZOGENEN DATEN DURCH BEHÖRDEN IM VEREINIGTEN KÖNIGREICH

(112) Die Kommission bewertete auch den Rechtsrahmen des Vereinigten Königreichs für die Erhebung und anschließende Verwendung personenbezogener Daten, die britische Behörden im öffentlichen Interesse, insbesondere zu Zwecken der Strafverfolgung und der nationalen Sicherheit, an Unternehmer im Vereinigten Königreich übermitteln („government access“) (im Folgenden als „staatlicher Zugriff“ bezeichnet). Bei der Beurteilung der Frage, ob die Bedingungen für den staatlichen Zugriff auf Daten, die gemäß diesem Beschluss an das Vereinigte Königreich übermittelt werden, das Kriterium der „wesentlichen Gleichwertigkeit“ nach Artikel 45 Absatz 1 der Verordnung (EU) 2016/679 in der Auslegung des Gerichtshofs der Europäischen Union im Lichte der Charta der Grundrechte erfüllen würden, hat die Kommission insbesondere die folgenden Kriterien berücksichtigt.

(113) Erstens muss jede Einschränkung des Rechts auf den Schutz personenbezogener Daten gesetzlich vorgesehen sein, und die gesetzliche Grundlage für den Eingriff in dieses Recht muss selbst den Umfang der Einschränkung der Ausübung des betreffenden Rechts festlegen.[121]

(114) Zweitens: Um dem Erfordernis der Verhältnismäßigkeit zu genügen, wonach Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten nur insoweit gelten dürfen, als dies in einer demokratischen Gesellschaft zur Verwirklichung spezifischer Ziele von allgemeinem Interesse, die den von der Union anerkannten Zielen gleichwertig sind, unbedingt erforderlich ist, muss die Rechtsvorschrift des betreffenden Drittlands, nach der der Eingriff zulässig ist, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, sodass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen.[122] In der Rechtsvorschrift muss insbesondere angegeben sein, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten

---

120 Paragraf 8 Absatz 1 des Human Rights Act 1998.

121 Siehe Schrems II, Rn. 174 und 175, und die darin aufgeführte Rechtsprechung. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch Rechtssache C-623/17 Privacy International ECLI:EU:C:2020:790, Rn. 65, sowie die verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18 La Quadrature du Net u. a. ECLI:EU:C:2020:791, Rn. 175.

122 Siehe Schrems II, Rn. 176 und 181, und die darin aufgeführte Rechtsprechung. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch die Rechtssachen Privacy International, Rn. 68, und La Quadrature du Net u. a., Rn. 132.

www.parlament.gv.at

vorsieht, getroffen werden darf[123]; ferner muss die Erfüllung dieser Anforderungen einer unabhängigen Aufsicht unterliegen[124].

(115) Drittens muss diese Rechtsvorschrift nach innerstaatlichem Recht rechtsverbindlich sein, und diese rechtlichen Anforderungen müssen für die Behörden nicht nur verbindlich sein, sondern gegenüber den Behörden auch gerichtlich durchsetzbar sein.[125] Insbesondere müssen betroffene Personen die Möglichkeit haben, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung solcher Daten zu erwirken.[126]

3.1 Allgemeiner Rechtsrahmen

(116) Als eine Ausübung einer Befugnis durch eine Behörde muss der staatliche Zugriff im Vereinigten Königreich unter uneingeschränkter Einhaltung des Gesetzes erfolgen. Das Vereinigte Königreich hat die Europäische Menschenrechtskonvention ratifiziert (siehe Erwägungsgrund 9), und alle Behörden im Vereinigten Königreich sind verpflichtet, in Übereinstimmung mit der Konvention zu handeln.[127] Nach Artikel 8 der Konvention muss jeder Eingriff in die Privatsphäre im Einklang mit dem Gesetz und im Interesse eines der in Artikel 8 Absatz 2 genannten Ziele erfolgen und im Hinblick auf dieses Ziel verhältnismäßig sein. Darüber hinaus wird in Artikel 8 verlangt, dass der Eingriff „vorhersehbar“ („foreseeable“) ist, d. h., eine klare, zugängliche gesetzliche Grundlage hat, und dass das Gesetz geeignete Garantien umfasst, um Missbrauch zu verhindern.

(117) Des Weiteren hat der Europäische Gerichtshof für Menschenrechte in seiner Rechtsprechung klargestellt, dass jeder Eingriff in die Rechte auf Schutz der Privatsphäre und Datenschutz der wirksamen, unabhängigen und unparteiischen Aufsicht durch einen Richter oder eine andere unabhängige Stelle (z. B. eine Verwaltungsbehörde oder ein parlamentarisches Gremium) unterliegen muss.[128]

(118) Darüber hinaus muss dem Einzelnen ein wirksamer Rechtsbehelf zur Verfügung stehen, und der Europäische Gerichtshof für Menschenrechte hat klargestellt, dass der Rechtsbehelf von einer unabhängigen und unparteiischen Stelle bereitgestellt werden muss, die sich eine eigene Geschäftsordnung gegeben hat und die aus Mitgliedern besteht, die ein hohes richterliches Amt bekleiden oder bekleidet haben oder erfahrene Juristen sind, und dass keine Beweisführungslast gelten darf, um einen Antrag bei dieser Stelle einzureichen. Bei der Untersuchung von Beschwerden natürlicher Personen sollte die unabhängige und unparteiische Stelle außerdem Zugriff auf alle

---

123 Siehe Schrems II, Rn. 176. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch die Rechtssachen Privacy International, Rn. 68, und La Quadrature du Net u. a., Rn. 132.

124 Siehe Schrems II, Rn. 179.

125 Siehe Schrems II, Rn. 181 und 182.

126 Siehe Schrems I, Rn. 95, und Schrems II, Rn. 194. In diesem Zusammenhang hat der EuGH insbesondere betont, dass die Einhaltung von Artikel 47 der Charta der Grundrechte, der das Recht auf einen wirksamen Rechtsbehelf vor einem unabhängigen und unparteiischen Gericht garantiert, „für das in der Union erforderliche Schutzniveau maßgebend ist und [von der] Kommission [festgestellt werden] muss, bevor sie einen Angemessenheitsbeschluss im Sinne von Art. 45 Abs. 1 der [Verordnung (EU) 2016/679] erlässt“ (Schrems II, Rn. 186).

127 Paragraf 6 des Human Rights Act 1998.

128 Europäischer Gerichtshof für Menschenrechte, Klass u. a./Deutschland, Antrag Nr. 5029/71, Rn. 17 bis 51.

www.parlament.gv.at

relevanten Informationen, einschließlich geheim gehaltener Materialien, haben. Und schließlich sollte sie befugt sein, bei Rechtsverletzungen Abhilfe zu schaffen.[129]

(119) Das Vereinigte Königreich hat zudem das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten („Übereinkommen Nr. 108“) und 2018 auch das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (bekannt als „Übereinkommen Nr. 108+“) unterzeichnet.[130] Nach Artikel 9 des Übereinkommens Nr. 108 sind Ausnahmen von den allgemeinen Datenschutzgrundsätzen (Artikel 5 – Datenqualität), den Vorschriften über besondere Kategorien von Daten (Artikel 6 – Besondere Kategorien von Daten) und den Rechten der betroffenen Person (Artikel 8 – Zusätzliche Garantien für die betroffene Person) nur dann zulässig, wenn eine solche Ausnahme im Recht der Vertragspartei vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft im Interesse des Schutzes der staatlichen Sicherheit, der öffentlichen Sicherheit, der finanziellen Interessen des Staates oder der Bekämpfung von Straftaten oder zum Schutz der betroffenen Person oder der Rechte und Freiheiten anderer notwendig ist.[131]

(120) Daher unterliegt das Vereinigte Königreich durch die Mitgliedschaft im Europarat, den Beitritt zur Europäischen Menschenrechtskonvention und die Anerkennung der Gerichtsbarkeit des Europäischen Gerichtshofs für Menschenrechte einer Reihe von völkerrechtlich verankerten Verpflichtungen, die den Rahmen für sein System des staatlichen Zugriffs bilden, und zwar auf der Grundlage von Grundsätzen, Garantien und individuellen Rechten, die denen ähnlich sind, die im EU-Recht garantiert sind und für die Mitgliedstaaten gelten. Wie in Erwägungsgrund 19 hervorgehoben, ist die kontinuierliche Einhaltung dieser Instrumente daher ein besonders wichtiges Element der Bewertung, auf die sich dieser Beschluss stützt.

(121) Darüber hinaus werden durch den DPA 2018 besondere Datenschutzgarantien und -rechte für Fälle gewährleistet, in denen Daten durch Behörden, einschließlich Strafverfolgungsbehörden und nationaler Sicherheitsorgane, verarbeitet werden.

(122) So ist insbesondere die Regelung für die Verarbeitung personenbezogener Daten im Rahmen der Strafverfolgung in Teil 3 des DPA 2018 festgelegt, der zur Umsetzung der Richtlinie (EU) 2016/680 erlassen wurde. Teil 3 des DPA 2018 gilt für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der

---

129 Europäischer Gerichtshof für Menschenrechte, Kennedy/Vereinigtes Königreich, Antrag Nr. 26839/05, („Kennedy“), Rn. 167 und 190.

130 Für weitere Informationen über die Europäische Menschenrechtskonvention und ihre Umsetzung in das Recht des Vereinigten Königreichs durch den Human Rights Act 1998 sowie über das Übereinkommen Nr. 108 siehe Erwägungsgrund 9.

131 Ebenso sind nach Artikel 11 des Übereinkommens Nr. 108+ Beschränkungen bestimmter spezifischer Rechte und Pflichten des Übereinkommens für Zwecke der nationalen Sicherheit oder der Verhütung, Ermittlung und Verfolgung von Straftaten und der Strafvollstreckung nur dann zulässig, wenn eine solche Beschränkung gesetzlich vorgesehen ist, den Wesensgehalt der Grundrechte und -freiheiten wahrt und eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellt. Verarbeitungstätigkeiten zu Zwecken der nationalen Sicherheit und Verteidigung müssen zudem einer unabhängigen und wirksamen Überprüfung und Aufsicht nach dem innerstaatlichen Recht der jeweiligen Vertragspartei des Übereinkommens unterliegen.

www.parlament.gv.at

Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.[132]

(123) 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.[133] Wie nachstehend erläutert (siehe Erwägungsgrund 139) können bestimmte zuständige Behörden (z. B. die National Crime Agency) unter bestimmten Voraussetzungen von den im Gesetz über Ermittlungsbefugnisse von 2016 (Investigatory Powers Act, IPA 2016) vorgesehenen Befugnissen Gebrauch machen. In diesem Fall gelten die im IPA 2016 vorgesehenen Garantien zusätzlich zu den in Teil 3 des DPA 2018 vorgesehenen. Die Nachrichtendienste (Secret Intelligence Service, Security Service und die Government Communications Headquarters) gelten nicht als „zuständige Behörden“ („competent authorities“)[134], die unter Teil 3 des DPA 2018 fallen, und die dort festgelegten Regeln finden daher auf deren Tätigkeiten keine Anwendung. Ein besonderer Teil des DPA 2018 (Teil 4) behandelt die Verarbeitung personenbezogener Daten durch Nachrichtendienste (siehe Erwägungsgrund 125 für weitere Einzelheiten).

(124) Analog zur Richtlinie (EU) 2016/680 sind in Teil 3 des DPA 2018 die Grundsätze der Rechtmäßigkeit und der Verarbeitung nach Treu und Glauben[135], der Zweckbindung[136], der Datenminimierung[137], der Richtigkeit[138], der Speicherbegrenzung[139] und der Sicherheit[140] festgelegt. Gemäß dem DPA 2018 gelten bestimmte Transparenzpflichten[141] und für Einzelpersonen das Recht auf Auskunft[142], Berichtigung und Löschung[143] sowie das Recht, keiner automatisierten Entscheidungsfindung unterworfen zu werden[144]. Zudem sind die zuständigen Behörden verpflichtet, den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen umzusetzen, ein Verzeichnis von Verarbeitungstätigkeiten zu führen sowie für bestimmte Verarbeitungen Datenschutz-Folgenabschätzungen durchzuführen und den Information Commissioner vorab zu

---

132 Paragraf 31 DPA 2018.

133 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 National Crime Agency, die Welsh Revenue Authority, die Competition and Markets Authority und Her Majesty’s Land Register), Staatsanwaltschaften, sonstige Strafjustizbehörden und andere mit Strafverfolgungsaufgaben betraute Träger oder Organisationen (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).

134 Paragraf 30 Absatz 2 DPA 2018.

135 Paragraf 35 DPA 2018.

136 Paragraf 36 DPA 2018.

137 Paragraf 37 DPA 2018.

138 Paragraf 38 DPA 2018.

139 Paragraf 39 DPA 2018.

140 Paragraf 40 DPA 2018.

141 Paragraf 44 DPA 2018.

142 Paragraf 45 DPA 2018.

143 Paragrafen 46 und 47 DPA 2018.

144 Paragrafen 49 und 50 DPA 2018.

www.parlament.gv.at

konsultieren.[145] Nach Paragraf 56 DPA 2018 müssen die zuständigen Behörden, die Einhaltung dieser Bestimmungen nachweisen. Darüber hinaus sind sie verpflichtet, geeignete Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu ergreifen[146], und unterliegen im Falle einer Datenschutzverletzung besonderen Pflichten, wie der Meldung solcher Verletzungen an den Information Commissioner und die betroffenen Personen.[147] Wie im Rahmen der Richtlinie (EU) 2016/680 ist ebenfalls vorgesehen, dass der Verantwortliche (sofern es sich nicht um ein Gericht oder eine andere Justizbehörde handelt, die im Rahmen einer justiziellen Tätigkeit handelt) einen Datenschutzbeauftragten benennen muss[148], der den Verantwortlichen bei der Einhaltung seiner Pflichten unterstützt und diese Einhaltung überwacht[149]. Ferner gelten besondere Anforderungen bezüglich internationaler Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen zu Strafverfolgungszwecken, um die Kontinuität des Schutzes zu gewährleisten.[150] Am Tag der Annahme dieses Beschlusses hat die Kommission einen weiteren Angemessenheitsbeschluss auf der Grundlage von Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 angenommen, nach dem die für die Verarbeitung durch britische Strafverfolgungsbehörden geltende Datenschutzregelung ein Schutzniveau gewährleistet, das der Sache nach dem durch die Richtlinie (EU) 2016/680 garantierten Schutzniveau gleichwertig ist.

(125) Teil 4 des DPA 2018 gilt für jede Verarbeitung durch Nachrichtendienste oder in deren Namen. Konkret ist darin Folgendes geregelt: die wesentlichen Datenschutzgrundsätze (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben sowie Transparenz[151], Zweckbindung[152], Datenminimierung[153], Richtigkeit[154], Speicherbegrenzung[155] und Sicherheit[156]), die Bedingungen für die Verarbeitung

145 Paragrafen 56 bis 65 DPA 2018.

146 Paragraf 66 DPA 2018.

147 Paragrafen 67 und 68 DPA 2018.

148 Paragrafen 69 bis 71 DPA 2018.

149 Paragrafen 67 und 68 DPA 2018.

150 Teil 3 Kapitel 5 des DPA 2018.

151 Gemäß 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 erlangt 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.

152 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 DPA 2018 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).

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

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

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

www.parlament.gv.at

besonderer Kategorien von Daten[157], die Rechte der betroffenen Person[158], die Verpflichtung zum Datenschutz durch Technikgestaltung[159] und internationale Übermittlungen personenbezogener Daten[160]. Das ICO hat kürzlich detaillierte Leitlinien zu der Verarbeitung durch Nachrichtendienste gemäß Teil 4 des IPA 2018 veröffentlicht.[161]

(126) Gleichzeitig ist in Paragraf 110 DPA 2018 eine Ausnahme von bestimmten Bestimmungen von Teil 4 des DPA 2018 vorgesehen[162], wenn eine solche Ausnahme zum Schutz der nationalen Sicherheit erforderlich ist. Diese Ausnahme kann auf der Grundlage einer Einzelfallprüfung in Anspruch genommen werden.[163] 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

---

156 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 1) jeder Verantwortliche geeignete Sicherheitsmaßnahmen ergreifen muss, die den mit der Verarbeitung personenbezogener Daten verbundenen Risiken angemessen sind, und dass 2) im Falle einer automatisierten Verarbeitung jeder Verantwortliche und jeder Auftragsverarbeiter vorbeugende oder schadensbegrenzende Maßnahmen auf der Grundlage einer Risikobewertung ergreifen muss.

157 Paragraf 86 Absatz 2 Buchstabe b und Anhang 10 des DPA 2018.

158 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. Wie in den Leitlinien des ICO zu der Verarbeitung durch Nachrichtendienste ausgeführt, kann der Einzelne alle seine Rechte (einschließlich Antrag auf Berichtigung) wahrnehmen, indem er Beschwerde beim ICO einlegt oder die Angelegenheit vor Gericht bringt (siehe ICO Guidance to intelligence services processing, abrufbar unter folgendem Link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

159 Paragraf 103 DPA 2018.

160 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.

161 ICO Guidance, siehe Fußnote 158.

Paragraf 30 DPA 2018 und Anhang 7 des DPA 2018.

162 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.

163 Siehe Baker/Secretary of State, siehe Fußnote 61.

www.parlament.gv.at

Verteidigung zu beeinträchtigen“.[164] Das ICO beurteilt im Rahmen seiner Aufsichtsfunktion, ob die Ausnahmeregelung ordnungsgemäß angewandt wurde.[165]

(127) Darüber hinaus kann ein Verantwortlicher im Hinblick auf die Möglichkeit, die Anwendung der vorstehend genannten Bestimmungen gemäß Paragraf 111 des DPA 2018 zum Schutz der „nationalen Sicherheit“ („national security“) einzuschränken, eine von einem Kabinettsminister oder dem Generalstaatsanwalt unterzeichnete Bescheinigung beantragen, in der bestätigt wird, dass eine Einschränkung dieser Rechte eine notwendige und verhältnismäßige Maßnahme zum Schutz der nationalen Sicherheit darstellt.[166]

(128) Die britische Regierung hat Leitlinien für Verantwortliche herausgegeben, die erwägen, eine nationale Sicherheitsbescheinigung gemäß dem DPA 2018 zu beantragen. Darin wird insbesondere hervorgehoben, dass jede Einschränkung der Rechte der betroffenen Personen aus Gründen des Schutzes der nationalen Sicherheit verhältnismäßig und notwendig sein muss.[167] Alle nationalen Sicherheitsbescheinigungen müssen auf der Webseite des ICO veröffentlicht werden.[168]

---

164 UK Explanatory Framework for Adequacy Discussions, Section H: National Security Data Protection and Investigatory Powers Framework, S. 15 und 16 (siehe Fußnote 31). Siehe auch die Rechtssache Baker/Secretary of State (siehe Fußnote 61); darin hob das Gericht 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 hinausging, was zum Schutz der nationalen Sicherheit erforderlich und verhältnismäßig war.

165 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 (UKIC), Nummer 16, abrufbar unter folgendem Link: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

166 Mit dem DPA 2018 wurde die Möglichkeit aufgehoben, Bescheinigungen nach Paragraf 28 Absatz 2 des Data Protection Act 1998 auszustellen. Die Möglichkeit, „alte Bescheinigungen“ („old certificates“) auszustellen, besteht jedoch weiterhin sofern es Anfechtungen im Rahmen des Gesetzes von 1998 gibt (siehe Anhang 20 Teil 5 Nummer 17 des DPA 2018). Diese Möglichkeit scheint jedoch sehr selten zu sein und nur für wenige Fälle zu gelten, so beispielsweise wenn eine betroffene Person die Anwendung der Ausnahme zum Schutz der nationalen Sicherheit im Zusammenhang mit einer von einer Behörde gemäß dem Gesetz von 1998 vorgenommenen Verarbeitung anficht. Es sei darauf hingewiesen, dass in diesen Fällen Paragraf 28 des DPA 1998 in seiner Gesamtheit anwendbar ist, was auch die Möglichkeit einschließt, dass die betroffene Person die Bescheinigung vor Gericht anfechten kann.

167 UK 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. Gemäß der Erläuterung der britischen Behörden ist eine Bescheinigung zwar ein schlüssiger Beweis dafür, dass die Ausnahme in Bezug auf die in der Bescheinigung beschriebenen Daten oder Verarbeitungen anwendbar ist, sie entbindet den Verantwortlichen jedoch nicht von der Pflicht, im Einzelfall zu prüfen, ob die Inanspruchnahme der Ausnahme notwendig ist.

168 Gemäß Paragraf 130 des DPA 2018 kann das ICO entscheiden, den Wortlaut oder einen Teil des Wortlauts der Bescheinigung nicht zu veröffentlichen, wenn dies dem Interesse der nationalen Sicherheit oder dem öffentlichen Interesse zuwiderlaufen oder die Sicherheit einer Person gefährden würde. In diesen Fällen wird das ICO jedoch veröffentlichen, dass die Bescheinigung ausgestellt wurde.

www.parlament.gv.at

(129) Die Bescheinigung sollte für einen festen Zeitraum von höchstens fünf Jahren gültig sein und regelmäßig von der Exekutive überprüft werden.[169] 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.[170]

(130) Es sei darauf hingewiesen, dass die nationalen Sicherheitsbescheinigungen keinen zusätzlichen Grund für eine Einschränkung der Datenschutzrechte aus Gründen der nationalen Sicherheit vorsehen. Das heißt, 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, wie oben erläutert, auf Einzelfallbasis anzuwenden ist.[171] 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.[172]

(131) Jede Person, die von der Ausstellung der Bescheinigung unmittelbar betroffen ist, kann beim Upper Tribunal[173] Rechtsmittel gegen die Bescheinigung einlegen[174] oder, wenn in der Bescheinigung bestimmte Daten in Form einer allgemeinen Beschreibung ausgewiesen werden, die Anwendung der Bescheinigung auf diese Daten anfechten[175]. Das Gericht überprüft daraufhin die Entscheidung zur Ausstellung einer Bescheinigung und entscheidet, ob berechtigte Gründe für die Ausstellung der Bescheinigung vorlagen.[176] 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.[177]

---

169 UK Government Guidance on National Security Certificates, Nummer 15, siehe Fußnote **Error! Bookmark not defined.**.

170 UK Government Guidance on National Security Certificates, Nummer 5, siehe Fußnote **Error! Bookmark not defined.**.

171 Siehe Fußnote 164.

172 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/.

173 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.

174 Paragraf 111 Absatz 3 DPA 2018.

175 Paragraf 111 Absatz 5 DPA 2018.

176 In der Rechtssache Baker/Secretary of State (siehe Fußnote 61) 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.

177 UK Government Guidance on National Security Certificates, Nummer 25, siehe Fußnote **Error! Bookmark not defined.**.

www.parlament.gv.at

(132) Weitere mögliche Einschränkungen betreffen diejenigen, die nach Anhang 11 des DPA 2018 für gewisse Bestimmungen von Teil 4 des DPA 2018[178] gelten, um den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses oder geschützter Interessen zu gewährleisten, wie zum Beispiel die parlamentarischen Vorrechte, die Vertraulichkeit des Schriftverkehrs zwischen Rechtsanwalt und Mandant, die Durchführung von Gerichtsverfahren oder die Schlagkraft der Streitkräfte.[179] 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").[180] 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.

(133) Aus den vorstehenden Ausführungen ergibt sich, dass in den geltenden Rechtsvorschriften des Vereinigten Königreichs Einschränkungen und Bedingungen

---

178 Hierzu zählen folgende Bestimmungen: 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, iii) die Pflichten im Zusammenhang mit der Meldung von Verletzungen des Schutzes personenbezogener Daten an das ICO.

179 Teil 4 des DPA 2018 bildet den rechtlichen Rahmen für alle Arten der Verarbeitung personenbezogener Daten durch Nachrichtendienste (und nicht nur für die Wahrnehmung ihrer Aufgaben im Bereich der nationalen Sicherheit). Daher gilt Teil 4 auch dann, wenn Nachrichtendienste Daten beispielsweise für die Zwecke der Personalverwaltung, im Rahmen von Rechtsstreitigkeiten oder im Zusammenhang mit der Vergabe öffentlicher Aufträge verarbeiten. Die in Anhang 11 aufgeführten Beschränkungen sollen in erster Linie in diesen anderen Zusammenhängen gelten. So kann beispielsweise im Rahmen eines Rechtsstreits mit einem Beschäftigten die Einschränkung für die Zwecke eines „Gerichtsverfahrens" („legal proceedings") geltend gemacht werden, oder im Zusammenhang mit der Vergabe öffentlicher Aufträge kann die Einschränkung für „Verhandlungszwecke" („negotiation") geltend gemacht werden usw. Dies spiegelt sich in den Leitlinien des ICO zu der Verarbeitung durch Nachrichtendienste wider, in denen die Aushandlung eines Vergleichs zwischen einem Nachrichtendienst und einem ehemaligen Beschäftigten, der einen Anspruch aus dem Arbeitsverhältnis geltend macht, als Beispiel für die Anwendung von Einschränkungen nach Anhang 11 genannt wird (siehe Fußnote 161). Es sei auch darauf hingewiesen, dass anderen Behörden gemäß Anhang 2 Teil 2 des DPA 2018 die gleichen Beschränkungen zur Verfügung stehen.

180 Dem UK Explanatory Framework zufolge gelten folgende Ausnahmen als „class based": i) Informationen über die Verleihung königlicher Ehren und Würden, ii) die Vertraulichkeit des Schriftverkehrs zwischen Rechtsanwalt und Mandant, iii) vertrauliche Beschäftigungs- oder Aus- und Weiterbildungszeugnisse, 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. UK Explanatory Framework for Adequacy Discussions, Section H: National security, S. 13, siehe Fußnote 31.

www.parlament.gv.at

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.

3.2 Zugriff und Verwendung durch Behörden des Vereinigten Königreichs für Strafverfolgungszwecke

(134) Das Recht des Vereinigten Königreichs umfasst eine Reihe von Beschränkungen für den Zugang zu und die Verwendung von personenbezogenen Daten für Zwecke der Strafverfolgung; ferner sieht es für diesen Bereich Aufsichtsmechanismen und Rechtsbehelfe vor, die den in den Erwägungsgründen 113 bis 115 des vorliegenden Beschlusses genannten Anforderungen entsprechen. Die folgenden Abschnitte enthalten eine detaillierte Bewertung der Bedingungen, unter denen ein solcher Zugriff erfolgen kann, sowie der Garantien, die für die Nutzung dieser Befugnisse gelten.

3.2.1 Rechtsgrundlagen und anwendbare Beschränkungen/Garantien

(135) Gemäß dem in Paragraf 35 DPA 2018 garantierten Grundsatz der Rechtmäßigkeit ist die Verarbeitung personenbezogener Daten für einen der Strafverfolgungszwecke nur dann rechtmäßig, wenn sie auf einer gesetzlichen Grundlage beruht und entweder die betroffene Person ihre Einwilligung für die Verarbeitung zu dem betreffenden Zweck erteilt hat[181] oder die Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde für den betreffenden Zweck wahrgenommen wird.

3.2.1.1 Durchsuchungsanordnungen und Herausgabeanordnungen

(136) Gemäß dem Rechtsrahmen des Vereinigten Königreichs ist die Erhebung personenbezogener Daten von Unternehmern – einschließlich Unternehmern, die im Rahmen des vorliegenden Angemessenheitsbeschlusses aus der Union übermittelte Daten verarbeiten würden – für Zwecke der Strafverfolgung auf der Grundlage von Durchsuchungsanordnungen („search warrants“)[182] und Herausgabeanordnungen („production orders“)[183] zulässig.

---

181 Die Einwilligung scheint bei der Bewertung der Angemessenheit nicht relevant zu sein, da eine britische Strafverfolgungsbehörde bei einer Übermittlung die Daten nicht direkt bei einer betroffenen Person in der EU auf der Grundlage einer Einwilligung erhebt.

182 Die einschlägigen Rechtsgrundlagen finden sich für England und Wales in den Paragrafen 8 ff. des Gesetzes über polizeiliche und strafrechtliche Beweismittel (Police and Criminal Evidence Act) von 1984 (im Folgenden „PACE 1984“), für Nordirland in den Paragrafen 10 ff. der Verordnung Nordirlands über polizeiliche und strafrechtliche Beweismittel (Police and Criminal Evidence Order (Northern Ireland)) von 1989 und für Schottland im Common Law (siehe Paragraf 46 des Strafjustizgesetzes Schottlands (Criminal Justice (Scotland) Act) von 2016 und Paragraf 23B des Strafrechtsgesetzes (Konsolidierung) Schottlands (Criminal Law (Consolidation) (Scotland) Act)). Für nach der Festnahme ausgestellte Durchsuchungsanordnungen findet sich die Rechtsgrundlage für England und Wales in Paragraf 18 PACE 1984, für Nordirland in den Paragrafen 20 ff. der Police and Criminal Evidence Order (Northern Ireland) 1989 und für Schottland im Common Law (siehe Paragraf 46 des Criminal Justice (Scotland) Act 2016). Die britischen Behörden haben klargestellt, dass Durchsuchungsanordnungen auf Antrag des Ermittlungsbeamten von einem Gericht ausgestellt werden. Sie erlauben es einem Beamten, Räumlichkeiten zu betreten, um nach Material oder Personen zu suchen, die für seine Ermittlungen relevant sind; die Vollstreckung der Anordnung erfordert oftmals die Unterstützung eines Polizeibeamten.

183 Beziehen sich die Ermittlungen auf den Bereich der Geldwäsche (einschließlich Beschlagnahmeverfahren und zivilrechtlicher Wiedereinziehungsverfahren), sind die einschlägigen Rechtsgrundlagen für die Beantragung einer Herausgabeanordnung die Paragrafen 345 ff. für England, Wales und Nordirland und die Paragrafen 380 ff. des Proceeds of Crime Act 2002 für Schottland.

www.parlament.gv.at

(137) Durchsuchungsanordnungen werden – in der Regel auf Antrag des Ermittlungsbeamten – von einem Gericht ausgestellt. Sie erlauben es einem Beamten, Räumlichkeiten zu betreten, um nach Material oder Personen zu suchen, die für seine Ermittlungen relevant sind, und sämtliches Material, für das eine Durchsuchung genehmigt wurde, einzubehalten, einschließlich aller relevanten Dokumente oder Materialien, die personenbezogene Daten enthalten.[184] Eine Herausgabeanordnung, die ebenfalls von einem Gericht ausgestellt werden muss, verpflichtet die darin genannte Person, Material, das sich in ihrem Besitz oder unter ihrer Kontrolle befindet, herauszugeben oder Zugang dazu zu gewähren. Der Antragsteller muss gegenüber dem Gericht begründen, warum die Durchsuchungsanordnung oder Herausgabeanordnung notwendig ist und warum sie im öffentlichen Interesse liegt. Es gibt eine Reihe gesetzlicher Befugnisse, nach denen der Erlass von Durchsuchungsanordnungen oder Herausgabeanordnungen möglich ist. Für jede Bestimmung gelten eigene gesetzliche Voraussetzungen, die erfüllt sein müssen, damit eine Durchsuchungsanordnung[185] oder Herausgabeanordnungen[186] erlassen werden kann.

Betreffen die Ermittlungen andere Bereiche als Geldwäsche, kann ein Antrag auf eine Herausgabeanordnung in England und Wales gemäß Paragraf 9 und Anhang 1 des PACE 1984 und in Nordirland gemäß Paragraf 10 ff. der Police and Criminal Evidence Order (Northern Ireland) 1989 gestellt werden. In Schottland findet sich die einschlägige Rechtsgrundlage im Common Law (siehe Paragraf 46 des Criminal Justice (Scotland) Act 2016) und Paragraf 23B des Criminal Law (Consolidation) (Scotland)). Die britischen Behörden haben klargestellt, dass eine Herausgabeanordnung die darin genannte Person verpflichtet, das Material, das sich in ihrem Besitz oder unter ihrer Kontrolle befindet, herauszugeben oder Zugang dazu zu gewähren (siehe Anhang 1 Nummer 4 des PACE 1984).

184 So enthalten beispielsweise die Paragrafen 8 und 18 PACE 1984 Befugnisse, nach denen sämtliches Material, für das eine Durchsuchung genehmigt wurde, beschlagnahmt und einbehalten werden kann.

185 So regeln beispielsweise die Paragrafen 8 und 18 PACE die Befugnis eines Friedensrichters, eine Durchsuchungsanordnung zu genehmigen, bzw. die Befugnis eines Polizeibeamten, eine Immobilie zu durchsuchen. Im ersten Fall (Paragraf 8) muss sich ein Friedensrichter vor dem Erlass einer Durchsuchungsanordnung zunächst davon überzeugen, dass hinreichende Gründe für die Annahme bestehen, dass: i) eine schwere Straftat begangen wurde. ii) sich in den Räumlichkeiten Material befindet, das (entweder für sich genommen oder zusammen mit anderem Material) wahrscheinlich von erheblichem Wert für die Untersuchung der Straftat ist, iii) es sich bei dem Material wahrscheinlich um relevantes Beweismaterial handelt, iv) das Material nicht aus Gegenständen besteht oder Gegenstände enthält, die einem Rechtsprivileg unterliegen, und nicht aus ausgeschlossenem Material oder besonderem Verfahrensmaterial besteht oder dieses enthält, und v) es ohne eine Durchsuchungsanordnung nicht möglich wäre, sich Zutritt zu verschaffen. Im zweiten Fall ist ein Polizeibeamter gemäß Paragraf 18 befugt, die Räumlichkeiten einer Person, die wegen einer schweren Straftat festgenommen wurde, nach Material, das nicht einem Rechtsprivileg unterliegendes Material ist, zu durchsuchen, wenn er den begründeten Verdacht hat, dass sich in den Räumlichkeiten Beweismittel befinden, die sich auf diese Straftat oder eine andere ähnliche oder damit verbundene schwere Straftat beziehen. Eine solche Durchsuchung muss auf das Auffinden dieses Materials beschränkt sein und von einem Polizeibeamten, der mindestens den Rang eines Inspektors hat, schriftlich genehmigt werden, es sei denn, dies ist für die Untersuchung der Straftat erforderlich. In diesem Fall muss ein Polizeibeamter, der mindestens den Rang eines Inspektors hat, so bald wie möglich nach der Durchführung der Durchsuchung unterrichtet werden. Die Gründe für die Durchsuchung und die Art der gesuchten Beweismittel sind festzuhalten. Darüber hinaus sind in den Paragrafen 15 und 16 PACE 1984 gesetzliche Garantien vorgesehen, die bei der Beantragung einer Durchsuchungsanordnung beachtet werden müssen. Paragraf 15 umfasst die Anforderungen für das Erwirken einer Durchsuchungsanordnung (darunter Angaben zum Inhalt des vom Polizeibeamten zu stellenden Antrags und das Erfordernis, dass in der Anordnung unter anderem anzugeben ist, gemäß welchem Rechtsetzungsakt sie ergeht, welche Gegenstände und Personen gesucht werden und welche Räumlichkeiten durchsucht werden). In Paragraf 16 ist geregelt, wie eine Durchsuchung aufgrund einer

www.parlament.gv.at

(138) Herausgabeanordnungen und Durchsuchungsanordnungen können im Wege der gerichtlichen Überprüfung angefochten werden.[187] Was Garantien anbelangt, so dürfen

---

Durchsuchungsanordnung durchzuführen ist (Beispiele: nach Paragraf 16 Absatz 5 muss der Beamte, der die Durchsuchungsanordnung vollstreckt, der Person, deren Räumlichkeiten durchsucht werden, eine Kopie der Durchsuchungsanordnung aushändigen; gemäß Paragraf 16 Absatz 11 muss die Durchsuchungsanordnung nach ihrer Vollstreckung für einen Zeitraum von 12 Monaten aufbewahrt werden; nach Paragraf 16 Absatz 12 hat die Person, deren Räumlichkeiten durchsucht wurden, das Recht, die Durchsuchungsanordnung während dieses Zeitraums einzusehen, wenn sie dies wünscht). Durch diese Paragrafen wird unter anderem sichergestellt, dass Artikel 8 EMRK eingehalten wird (siehe z. B. Kent Pharmaceuticals/Director of the Serious Fraud Office, [2002] EWHC 3023 (QB) unter [30] von Lord Woolf CJ). Werden diese Garantien nicht eingehalten, kann die Durchsuchung für rechtswidrig erklärt werden (Beispiele hierfür sind R (Brook)/Preston Crown Court, [2018] EWHC 2024 (Admin), [2018] ACD 95; R (Superior Import / Export Ltd)/Revenue and Customs Commissioners, [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; und R (F)/Blackfriars Crown Court, [2014] EWHC 1541 (Admin)). Die Paragrafen 15 und 16 PACE 1984 werden durch den Code B des PACE ergänzt, einen Verhaltenskodex, in dem die Ausübung polizeilicher Befugnisse zur Durchsuchung von Räumlichkeiten geregelt ist.

186 Wenn beispielsweise eine Herausgabeanordnung gemäß dem Proceeds of Crime Act 2002 erlassen wird, müssen zusätzlich zu den hinreichenden Gründen zur Erfüllung der Bedingungen nach Paragraf 346 Absatz 2 dieses Rechtsakts auch hinreichende Gründe für die Annahme vorliegen, dass die Person im Besitz des spezifizierten Materials ist oder dieses kontrolliert und dass das Material wahrscheinlich von erheblichem Wert ist. Ein weiteres Erfordernis für den Erlass einer Herausgabeanordnung besteht darin, dass hinreichende Gründe für die Annahme vorliegen müssen, dass die Herausgabe des Materials oder die Gewährung des Zugangs dazu im öffentlichen Interesse liegt, und zwar unter Berücksichtigung a) des voraussichtlichen Nutzens der Erlangung des Materials für die Untersuchung und b) der Umstände, unter denen die im Antrag genannte Person im Besitz des Materials zu sein scheint oder dieses zu kontrollieren scheint. In ähnlicher Weise muss ein Gericht, das einen Antrag auf eine Herausgabeanordnung gemäß Anhang 1 des PACE 1984 prüft, davon überzeugt sein, dass bestimmte Bedingungen erfüllt sind. So enthält Anhang 1 des PACE insbesondere zwei unterschiedliche alternative Gruppen von Bedingungen, von denen eine erfüllt sein muss, bevor ein Richter eine Herausgabeanordnung erlassen kann. Gemäß der ersten Gruppe von Bedingungen müssen dem Richter hinreichende Gründe für die Annahme vorliegen, dass i) eine schwere Straftat begangen wurde, ii) das in den Räumlichkeiten gesuchte Material aus speziellem Verfahrensmaterial, jedoch nicht aus ausgeschlossenem Material besteht oder dieses enthält, iii) das Material entweder für sich genommen oder zusammen mit anderem Material wahrscheinlich von erheblichem Wert für die Untersuchung ist, iv) es sich wahrscheinlich um relevantes Beweismaterial handelt, v) andere Methoden zur Beschaffung des Materials entweder versucht wurden oder nicht versucht wurden, weil sie zwangsläufig fehlschlagen würden, und vi) es unter Berücksichtigung des Nutzens für die Untersuchung und der Umstände, unter denen die Person über das Material verfügt, im öffentlichen Interesse liegt, dass das Material herausgegeben oder der Zugang dazu gewährt wird. Gemäß der zweiten Gruppe müssen folgende Bedingungen erfüllt sein: i) in den Räumlichkeiten befindet sich Material, das aus besonderem Verfahrensmaterial oder ausgeschlossenem Material besteht, ii) wenn das Verbot der Durchsuchung auf der Grundlage von vor dem Erlass des PACE erlassenen Rechtsvorschriften für besonderes Verfahrensmaterial, ausgeschlossenes Material oder einem Rechtsprivileg unterliegendes Material nicht bestünde, hätte eine Durchsuchungsanordnung für das Material erlassen werden können, und iii) dies wäre angemessen gewesen.

187 Die gerichtliche Überprüfung ist das Rechtsverfahren, mit dem die Entscheidungen einer öffentlichen Stelle vor dem High Court angefochten werden können. Die Gerichte „überprüfen" („review") die angefochtene Entscheidung und entscheiden unter Berücksichtigung von Konzepten und Grundsätzen des öffentlichen Rechts, ob Gründe für die Annahme bestehen, dass die Entscheidung rechtlich fehlerhaft ist. Die wichtigsten Gründe für eine gerichtliche Überprüfung sind Rechtswidrigkeit, Irrationalität, Verfahrensfehler, Vertrauensschutz und Menschenrechte. Nach einer erfolgreichen gerichtlichen Überprüfung kann ein Gericht eine Reihe verschiedener Abhilfemaßnahmen anordnen; die häufigste Maßnahme ist der Aufhebungsbeschluss („quashing order") (durch den die ursprüngliche

www.parlament.gv.at

alle in den Anwendungsbereich des Teils 3 des DPA 2018 fallende Strafverfolgungsbehörden nur dann auf personenbezogene Daten zugreifen – was eine Form der Verarbeitung darstellt –, wenn sie die Grundsätze und Anforderungen nach dem DPA 2018 erfüllen (siehe Erwägungsgründe 122 und 124 oben). Demnach sollte ein von einer Strafverfolgungsbehörde gestellter Antrag dem Grundsatz entsprechen, wonach die Zwecke der Verarbeitung genau festgelegt, eindeutig und rechtmäßig sein müssen[188] und die von einer zuständigen Behörde verarbeiteten personenbezogenen Daten für diese Zwecke angemessen sein müssen und nicht darüber hinausgehen dürfen[189].

3.2.1.2 Ermittlungsbefugnisse zu Strafverfolgungszwecken

(139) Zum Zwecke der Verhütung oder Aufdeckung von ausschließlich schweren Straftaten[190] verfügen bestimmte Strafverfolgungsbehörden, z. B. die National Crime Agency oder der Chief of Police[191], über gezielte Ermittlungsbefugnisse gemäß dem IPA 2016. In diesem Fall gelten die im IPA 2016 vorgesehenen Garantien zusätzlich zu den in Teil 3 des DPA 2018 vorgesehenen. Bei den spezifischen Ermittlungsbefugnissen, auf die diese Strafverfolgungsbehörden zurückgreifen können, handelt es sich um folgende: gezieltes Abfangen von Informationen („interception“) (Teil 2 des IPA 2016), Beschaffung von Kommunikationsdaten („acquisition of communications data“) (Teil 3 des IPA 2016), Speicherung von Kommunikationsdaten („retention of communications data“) (Teil 4 des IPA 2016) und gezielter Gerätezugriff („equipment interference“) (Teil 5 des IPA 2016). Das Abfangen umfasst die Erfassung des Inhalts eines Kommunikationsvorgangs[192]; bei der Beschaffung und Speicherung von Kommunikationsdaten hingegen geht es weniger darum, den Inhalt, als vielmehr das „Wer“, „Wann“, „Wo“ und „Wie“ eines Kommunikationsvorgangs zu ermitteln. Dies umfasst beispielsweise den Zeitpunkt

---

Entscheidung – d. h. die Entscheidung zum Erlass einer Durchsuchungsanordnung – aufgehoben oder annuliert wird), wobei unter bestimmten Umständen auch eine finanzielle Entschädigung gewährt werden kann. Weitere Einzelheiten zur gerichtlichen Überprüfung im Vereinigten Königreich enthält die Veröffentlichung „Judge Over Your Shoulder – a guide to good decision-making“ des Government Legal Department, die unter folgendem Link abrufbar ist: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

188 Paragraf 36 Absatz 1 DPA 2018.

189 Paragraf 37 DPA 2018.

190 Gemäß Paragraf 263 Absatz 1 IPA 2016 handelt es sich bei einer „schweren Straftat“ („serious crime“) um ein Delikt, für das ein Erwachsener, der nicht vorbestraft ist, nach vernünftigem Ermessen zu einer Freiheitsstrafe von mindestens drei Jahren verurteilt werden könnte, bzw. ein Delikt, bei dem Gewalt angewendet wurde oder ein erheblicher finanzieller Gewinn entstanden ist oder das von einer großen Anzahl von Personen begangen wurde. Für die Zwecke der Beschaffung von Kommunikationsdaten gemäß Teil 4 des IPA 2016 besagt Paragraf 87 Absatz 10B zudem, dass eine „schwere Straftat“ ein Delikt ist, für das eine Freiheitsstrafe von mindestens 12 Monaten verhängt werden kann oder das von einer Person begangen wird, die keine natürliche Person ist, oder dessen wesentlicher Bestandteil eine Nachrichtenübermittlung oder eine Verletzung der Privatsphäre einer Person ist.

191 Insbesondere die folgenden Strafverfolgungsbehörden können eine Anordnung für gezieltes Abfangen beantragen: der Generaldirektor der National Crime Agency, der Commissioner of Police of the Metropolis, der Chief Constable of the Police Service of Northern Ireland, der Chief Constable of the Police Service of Scotland, der Commissioner for Her Majesty's Revenue and Customs, der Chief of Defence Intelligence und eine Person, die eine zuständige Behörde eines Landes oder Gebiets außerhalb des Vereinigten Königreichs für die Zwecke eines EU-Amtshilfeinstruments oder eines internationalen Amtshilfeabkommens ist (Paragraf 18 Absatz 1 IPA 2016).

192 Siehe Paragraf 4 IPA 2016.

www.parlament.gv.at

und die Dauer eines Kommunikationsvorgangs, die Telefonnummer oder E-Mail-Adresse des Urhebers und des Empfängers des Kommunikationsvorgangs und mitunter auch den Standort der Geräte, von denen aus die Kommunikation erfolgte, den Teilnehmer eines Telefondienstes oder einen Einzelverbindungsnachweis.[193] Der Gerätezugriff umfasst eine Reihe von Techniken, mit denen eine Vielzahl unterschiedlicher Daten von Geräten gesammelt wird, unter anderem von Computern, Tablets und Smartphones sowie Kabeln, Drähten und Speichergeräten.[194]

(140) Ferner können Befugnisse zum gezielten Abfangen dann in Anspruch genommen werden, wenn dies „zur Umsetzung der Bestimmungen eines EU-Amtshilfeinstruments oder eines internationalen Amtshilfeabkommens erforderlich ist“ („mutual assistance warrant“ (Amtshilfeanordnung[195])). Amtshilfeanordnungen sind nur in Bezug auf das Abfangen, nicht aber auf die Beschaffung von Kommunikationsdaten oder den Zugriff auf Geräte vorgesehen. Diese gezielten Befugnisse sind im Investigatory Powers Act 2016 (IPA 2016)[196] geregelt, der zusammen mit dem Regulation of Investigatory Powers Act 2000 (RIPA) für England, Wales und Nordirland sowie dem Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) für Schottland die Rechtsgrundlage für die Ausübung dieser Befugnisse bildet und die diesbezüglich geltenden Beschränkungen und Garantien festlegt. Des Weiteren ist im IPA 2016 auch die Ausübung von Massenermittlungsbefugnissen geregelt, wenngleich diese Befugnisse Strafverfolgungsbehörden nicht zur Verfügung stehen (nur Nachrichtendienste können davon Gebrauch machen).[197]

(141) Für die Ausübung dieser Befugnisse benötigen die Behörden eine von einer zuständigen Behörde[198] ausgestellte und von einem unabhängigen Justizbeauftragten

---

193 Siehe Paragraf 261 Absatz 5 IPA 2016 und den Verhaltenskodex für die massenhafte Beschaffung von Kommunikationsdaten (Code of Practice on Bulk Acquisition of Communications Data), abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, Nummer 2.9.

194 Code of Practice on Equipment Interference, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, Nummer 2.2.

195 Durch eine Amtshilfeanordnung erhält eine britische Behörde die Befugnis, einer Behörde außerhalb des britischen Hoheitsgebiets im Rahmen eines internationalen Amtshilfeinstruments Unterstützung beim Abfangen und bei der Weitergabe des abgefangenen Materials an diese Behörde zu leisten (Paragraf 15 Absatz 4 IPA 2016).

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

197 Paragraf 138 Absatz 1, Paragraf 158 Absatz 1, Paragraf 178 Absatz 1 und Paragraf 199 Absatz 1 IPA 2016.

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

www.parlament.gv.at

(Judicial Commissioner)[199] genehmigte Anordnung[200] (das sogenannte „Double-Lock"-Verfahren). Die Ausstellung einer solchen Anordnung unterliegt einer Erforderlichkeits- und Verhältnismäßigkeitsprüfung.[201] Da diese gezielten Ermittlungsbefugnisse gemäß dem IPA 2016 denen entsprechen, die den nationalen Sicherheitsbehörden zur Verfügung stehen, werden die für diese Befugnisse geltenden Bedingungen, Einschränkungen und Garantien ausführlich im Abschnitt über den Zugang zu und die Verwendung von personenbezogenen Daten durch Behörden des Vereinigten Königreichs für Zwecke der nationalen Sicherheit behandelt (siehe Erwägungsgründe 177 und folgende).

3.2.2 Weitere Verwendung der erhobenen Daten

(142) Für die Weitergabe von Daten durch eine Strafverfolgungsbehörde an eine andere Behörde zu anderen Zwecken als denen, für die sie ursprünglich erhoben wurden, (die sogenannte Weitergabe – „onward sharing") gelten bestimmten Bedingungen.

(143) In Anlehnung an Artikel 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.[202] In diesem Fall gelten für die Verarbeitung durch die empfangende Behörde alle in Teil 3 des DPA 2018 aufgeführten Garantien, auf die in den Erwägungsgründen 122 und 124 verwiesen wird.

(144) Die britische Rechtsordnung umfasst eine Reihe von Gesetzen, nach denen eine solche 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 Behörden einhergehen würde,[203] oder im Falle einer Schuld gegenüber einer Behörde oder der Krone[204], ii) das Straf- und Gerichtsgesetz (Crime and Courts Act) von 2013, gemäß dem der Austausch von Informationen mit der National Crime Agency (NCA)[205] zur Bekämpfung, Ermittlung und Verfolgung von

---

199 Judicial Commissioners unterstützen den Beauftragten für Ermittlungsbefugnisse (Investigatory Powers Commissioner – IPC), ein unabhängiges Gremium, das die Nutzung von Ermittlungsbefugnissen durch Nachrichtendienste beaufsichtigt (für weitere Einzelheiten siehe Erwägungsgrund 162 und folgende).

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

201 Siehe insbesondere Paragrafen 19 und 23 IPA 2016.

202 Paragraf 36 Absatz 3 DPA 2018.

203 Paragraf 56 des Digital Economy Act 2017, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2017/30/section/56.

204 Paragraf 48 des Digital Economy Act 2017.

205 Paragraf 7 des Crime and Courts Act 2013, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2013/22/section/7.

www.parlament.gv.at

schwerer und organisierter Kriminalität gestattet ist, iii) das Gesetz über schwere Straftaten (Serious Crime Act) von 2007, nach dem Behörden zum Zwecke der Betrugsverhinderung Informationen an Betrugsbekämpfungsstellen weitergeben dürfen[206].

(145) In diesen Gesetzen ist ausdrücklich festgehalten, dass die Weitergabe von Informationen in Übereinstimmung mit den im DPA 2018 festgelegten Grundsätzen erfolgen muss. Darüber hinaus hat das College of Policing Leitlinien über zugelassene dienstliche Vorgehensweisen beim Austausch von Informationen (Authorised Professional Practice on Information Sharing)[207] 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, unterliegt selbstverständlich der gerichtlichen Überprüfung.[208]

(146) 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.[209]

(147) Diese Art der Weitergabe 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 Steuerbehörde, eine Wettbewerbsbehörde, ein Jugendamt usw.); 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. In den Erwägungsgründen 12 bis 111 hat die Kommission die in der UK GDPR und in Teil 2 des DPA 2018 vorgesehenen Garantien bewertet und ist zu dem Schluss gelangt, dass das Vereinigte Königreich ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die im Rahmen der Verordnung (EU) 2016/679 aus der Europäischen Union an das Vereinigte Königreich übermittelt werden.

(148) Im zweiten Szenario, das die Weitergabe von durch eine Strafverfolgungsbehörde erhobenen Daten an einen Nachrichtendienst für Zwecke der nationalen Sicherheit

---

206 Paragraf 68 des Serious Crime Act 2007, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2007/27/contents.

207 Authorised Professional Practice on Information Sharing, abrufbar unter folgendem Link: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

208 Siehe beispielsweise die Rechtssache M, R/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 Business Crime Reduction Partnership. 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.

209 Paragraf 36 Absatz 4 DPA 2018.

www.parlament.gv.at

betrifft, bildet Paragraf 19 des Gesetzes zur Terrorismusbekämpfung (Counter Terrorism Act) von 2008 die Rechtsgrundlage für eine solche Weitergabe.[210] Nach diesem Gesetz kann jede Person Informationen an einen der Nachrichtendienste zum Zwecke der Erfüllung einer der Aufgaben dieses Dienstes weitergeben, einschließlich für Zwecke der „nationalen Sicherheit".

(149) 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)[211] und dem Gesetz über Sicherheitsdienste (Security Service Act)[212] auf das zur Erfüllung ihrer gesetzlichen Aufgaben erforderliche Maß beschränkt. Strafverfolgungsbehörden, die Daten mit den Nachrichtendiensten austauschen möchten, müssen zusätzlich zu den gesetzlichen Aufgaben der Behörden, die im Intelligence Services Act und im Security Service Act festgelegt sind, eine Reihe von Faktoren/Einschränkungen berücksichtigen.[213] In Paragraf 20 des Counter Terrorism Act 2008 ist klar geregelt, dass jeglicher Datenaustausch gemäß Paragraf 19 in jedem Falle den Datenschutzvorschriften entsprechen muss, was bedeutet, dass sämtliche Einschränkungen und Anforderungen von Teil 3 des DPA 2018 Anwendung finden. Da zuständige Behörden überdies staatliche Stellen im Sinne des Human Rights Act 1998 darstellen, müssen sie sicherstellen, dass sie in Übereinstimmung mit den Konventionsrechten, einschließlich Artikel 8 EMRK, handeln. Durch diese Einschränkungen wird sichergestellt, dass die Datenweitergabe zwischen Strafverfolgungsbehörden und Nachrichtendiensten grundsätzlich den Datenschutzvorschriften sowie der EMRK entspricht.

(150) Wenn eine zuständige Behörde beabsichtigt, personenbezogene Daten, die gemäß Teil 3 des DPA 2018 verarbeitet wurden, an Strafverfolgungsbehörden eines Drittlandes weiterzugeben, gelten besondere Anforderungen.[214] Insbesondere dürfen

---

210 Counter Terrorism Act 2008, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

211 Intelligence Services Act 1994, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/1994/13/contents.

212 Security Service Act 1989, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/1989/5/contents.

213 In Paragraf 2 Absatz 2 des Intelligence Services Act 1994 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, mit denen sichergestellt wird, 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; 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 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, b) dass der Dienst keine Maßnahmen zur Förderung der Interessen einer politischen Partei des Vereinigten Königreichs ergreift, 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."

214 Siehe Teil 3 Kapitel 5 des DPA 2018.

www.parlament.gv.at

derartige Übermittlungen nur dann erfolgen, wenn sie auf Angemessenheitsvorschriften des Secretary of State beruhen; falls keine derartigen Vorschriften vorliegen, müssen geeignete Garantien vorgesehen werden. Nach Paragraf 75 DPA 2018 liegen geeignete Garantien dann vor, wenn sie durch ein für den vorgesehenen Empfänger verbindliches Rechtsinstrument festgelegt wurden oder wenn der Verantwortliche nach Beurteilung aller Umstände der Übermittlung dieser Art von personenbezogenen Daten an das Drittland oder die internationale Organisation zu dem Schluss gelangt, dass geeignete Garantien zum Schutz der Daten bestehen.

(151) Beruht eine Übermittlung nicht auf einer Angemessenheitsvorschrift oder geeigneten Garantien, kann sie nur unter bestimmten, festgelegten Umständen – „besonderen Umständen" („special circumstances") – erfolgen.[215] 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, ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder 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). 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. Diese Umstände entsprechen den bestimmten Fällen und Bedingungen, die nach Artikel 38 der Richtlinie (EU) 2016/680 als „Ausnahmen" gelten.

(152) Darüber hinaus sind im IPA 2016 zusätzliche Garantien für den Fall vorgesehen, dass das Material, das Strafverfolgungsbehörden im Rahmen einer Anordnung für Abfangmaßnahmen oder Gerätezugriff beschafft haben, an ein Drittland weitergegeben wird. So ist eine solche Offenlegung gegenüber dem Ausland („overseas disclosure") nur dann zulässig, wenn die anordnende Behörde der Ansicht ist, dass geeignete Vorkehrungen getroffen wurden, um die Anzahl der Personen, an die die Daten weitergegeben werden, den Umfang, in dem Material offengelegt oder zugänglich gemacht wird, sowie den Umfang, in dem Material kopiert wird, und die Anzahl der angefertigten Kopien zu begrenzen. Darüber hinaus kann die anordnende Behörde geeignete Vorkehrungen für notwendig erachten, mit denen sichergestellt wird, dass jede Kopie, die von einem Teil dieses Materials angefertigt wurde, vernichtet wird, sobald es keine maßgeblichen Gründe mehr deren Aufbewahrung gibt (sofern sie nicht früher vernichtet wird).[216]

(153) Schließlich könnten bestimmte Formen der Weiterübermittlung aus dem Vereinigten Königreich in die Vereinigten Staaten künftig auf der Grundlage des im Oktober 2019 abgeschlossenen „Abkommens zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika über den Zugang zu elektronischen Daten zur Bekämpfung von schwerer Kriminalität" (im Folgenden das „Abkommen zwischen dem Vereinigten Königreich

215 Paragraf 76 DPA 2018.

216 Paragraf 54 und Paragraf 130 IPA 2016. Die anordnenden Behörden müssen prüfen, ob für das an ausländische Behörden weitergegebene Material besondere Garantien vorgesehen werden müssen, um sicherzustellen, dass die Daten im Hinblick auf ihre Speicherung, Vernichtung und Offenlegung ähnlichen Garantien unterliegen wie denen, die laut Paragraf 53 und Paragraf 129 IPA 2016 vorgeschrieben sind.

www.parlament.gv.at

und den USA“ oder „das Abkommen“)[217] erfolgen.[218] Dieses Abkommen ist zwar zum Zeitpunkt des Erlasses dieses Beschlusses noch nicht in Kraft, sein absehbares Inkrafttreten kann sich jedoch auf die Weiterübermittlung von Daten in die USA auswirken, die zuvor auf der Grundlage des Beschlusses an das Vereinigte Königreich übermittelt wurden. Konkret könnten Daten, die aus der EU an Dienstleister im Vereinigten Königreich übermittelt werden, Gegenstand von Anordnungen zur Herausgabe elektronischer Beweismittel sein, die von den zuständigen US-amerikanischen Strafverfolgungsbehörden erlassen wurden und nach Inkrafttreten dieses Abkommens im Vereinigten Königreich anwendbar sind. Daher ist die Beurteilung der Bedingungen und Garantien, unter denen derartige Anordnungen erlassen und ausgeführt werden können, für diesen Beschluss relevant.

(154) In diesem Zusammenhang sind folgende Punkte zu beachten: Erstens erstreckt sich der sachliche Anwendungsbereich des Abkommens nur auf Straftaten, die mit einer Freiheitsstrafe von mindestens drei Jahren geahndet werden (definiert als „schwere Straftaten“ („serious crime“))[219], wozu auch „terroristische Aktivitäten“ („terrorist activity“) zählen. Zweitens können Daten, die in der jeweils anderen Rechtsordnung verarbeitet werden, im Rahmen dieses Abkommens nur nach einer Anordnung erlangt werden, „die gemäß dem innerstaatlichen Recht der anordnenden Vertragspartei vor oder in einem Verfahren zur Vollstreckung der Anordnung einer Überprüfung oder Aufsicht durch ein Gericht, einen Richter, einen Friedensrichter oder eine anderen unabhängige Behörde unterliegt“.[220] Drittens muss jede Anordnung „auf den Erfordernissen einer stichhaltigen Rechtfertigung auf der Grundlage artikulierbarer und glaubwürdiger Fakten sowie der Besonderheit, Rechtmäßigkeit und Schwere im Hinblick auf das untersuchte Verhalten beruhen“[221] und sie muss „auf bestimmte Konten abzielen und eine bestimmte Person, ein bestimmtes Konto, eine bestimmte Adresse oder ein bestimmtes persönliches Gerät oder eine andere spezifische Kennung identifizieren“[222]. Viertens genießen Daten, die im Rahmen dieses Abkommens

---

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

218 Es handelt sich dabei um das erste Abkommen, das im Rahmen des Gesetzes über die Klarstellung der Nutzung von Daten im Ausland (US Clarifying Lawful Overseas Use of Data (CLOUD) Act – im Folgenden „CLOUD Act“) geschlossen wurde. Der United States CLOUD Act ist ein US-Bundesgesetz, das am 23. März 2018 verabschiedet wurde. Darin wird durch eine Änderung des Gesetzes über gespeicherte Kommunikationsvorgänge (Stored Communications Act) von 1986 präzisiert, dass US-amerikanische Diensteanbieter verpflichtet sind, US-amerikanische Anordnungen zur Offenlegung von Inhalts- und Nichtinhaltsdaten unabhängig davon zu befolgen, wo die Daten gespeichert sind. Der CLOUD Act erlaubt auch den Abschluss von Durchführungsabkommen mit ausländischen Regierungen, auf deren Grundlage US-amerikanische Diensteanbieter diesen ausländischen Regierungen Inhaltsdaten direkt zur Verfügung stellen könnten (der Text des CLOUD Act ist unter folgendem Link abrufbar: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

219 Artikel 1 Absatz 14 des Abkommens.

220 Artikel 5 Absatz 2 des Abkommens.

221 Artikel 5 Absatz 1 des Abkommens.

222 Artikel 4 Absatz 5 des Abkommens. Ein zusätzlicher und strengerer Standard gilt in Bezug auf das Abfangen in Echtzeit: Demnach müssen Anordnungen für einen begrenzten Zeitraum gelten, der nicht länger sein darf, als es zur Erfüllung der Zwecke der Anordnung vernünftigerweise erforderlich ist;

www.parlament.gv.at

erlangt werden, ein gleichwertiges Schutzniveau wie durch die spezifischen Garantien des sogenannten „EU-US-Rahmenabkommens“[223] – ein im Dezember 2016 zwischen der EU und den Vereinigten Staaten geschlossenes umfassendes Datenschutzabkommen, in dem die für Datenübermittlungen im Rahmen der Zusammenarbeit bei der Strafverfolgung geltenden Garantien und Rechte festgelegt sind –, die allesamt durch Verweis sinngemäß in dieses Abkommen aufgenommen wurden, um insbesondere den Besonderheiten der Übermittlungen Rechnung zu tragen (d. h. Übermittlungen von privaten Anbietern an eine Strafverfolgungsbehörde und nicht Übermittlungen zwischen Strafverfolgungsbehörden).[224] Das Abkommen zwischen dem Vereinigten Königreich und den USA sieht ausdrücklich vor, dass „alle personenbezogenen Informationen, die bei der Ausführung von im Rahmen des Abkommens ergangenen Anordnungen zur Gewährleistung eines gleichwertigen Schutzniveaus erstellt werden“, ein gleichwertiges Schutzniveau genießen wie durch das EU-US-Rahmenabkommen.[225]

(155) Daten, die im Rahmen des Abkommens zwischen dem Vereinigten Königreich und den USA an US-Behörden übermittelt werden, sollten daher ein Schutzniveau genießen, das durch ein Rechtsinstrument der EU gewährleistet wird, wobei die erforderlichen Anpassungen vorzunehmen sind, um der Art der betreffenden Übermittlungen Rechnung zu tragen. Die britischen Behörden haben ferner bestätigt, dass das durch das Rahmenabkommen gewährleistete Schutzniveau für alle personenbezogenen Daten gilt, die im Rahmen des Abkommens erstellt oder aufbewahrt werden, unabhängig von der Art oder dem Typ der beantragenden Stelle (z. B. in den USA Strafverfolgungsbehörden sowohl auf Bundes- als auch auf Staatenebene), sodass in allen Fällen ein gleichwertiges Schutzniveau gewährleistet werden muss. Die britischen Behörden haben jedoch auch erklärt, dass die Einzelheiten der konkreten Umsetzung der Datenschutzgarantien noch Gegenstand von Gesprächen zwischen dem Vereinigten Königreich und den USA sind. Bei den Gesprächen mit den Dienststellen der Europäischen Kommission über diesen Beschluss haben die britischen Behörden bestätigt, dass sie das Abkommen erst dann in Kraft treten lassen werden, wenn sie sich davon überzeugt haben, dass bei seiner Umsetzung die in ihm enthaltenen rechtlichen Verpflichtungen eingehalten werden; unter anderem soll Klarheit darüber herrschen, dass in Bezug auf alle im Rahmen dieses Abkommens angeforderten Daten die einschlägigen Datenschutzstandards eingehalten werden. Da ein mögliches Inkrafttreten des Abkommens Auswirkungen auf das in diesem Beschluss bewertete Schutzniveau haben kann, sollte das Vereinigte Königreich der Europäischen Kommission jede Information und künftige Klarstellung hinsichtlich der Art und Weise, wie die USA ihren Verpflichtungen im Rahmen des Abkommens nachkommen werden, so bald wie möglich und in jedem Fall vor Inkrafttreten des Abkommens mitteilen, damit eine ordnungsgemäße Überwachung dieses Beschlusses in Übereinstimmung mit Artikel 45 Absatz 4 der Verordnung (EU) 2016/679 gewährleistet werden kann. Besonderes Augenmerk wird dabei darauf

---

ferner dürfen sie nur dann erteilt werden, wenn die gleichen Informationen nicht durch eine weniger einschneidende Methode erlangt werden können (Artikel 5 Absatz 3 des Abkommens).

223 Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten (ABl. L 336 vom 10.12.2016, S. 3), abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN

224 Artikel 9 Absatz 1 des Abkommens.

225 Artikel 9 Absatz 1 des Abkommens.

www.parlament.gv.at

gelegt, wie das Schutzniveau des Rahmenabkommens auf die besondere Art von Übermittlungen, die unter das Abkommen zwischen dem Vereinigten Königreich und den USA fallen, angewandt wird bzw. wie dieses Schutzniveau an diese Art von Übermittlungen angepasst wird.

(156) Generell werden alle relevanten Entwicklungen in Bezug auf das Inkrafttreten und die Anwendung des Abkommens im Rahmen der kontinuierlichen Überwachung dieses Beschlusses gebührend berücksichtigt, auch mit Blick auf mögliche Konsequenzen, die zu ziehen sind, wenn es Anzeichen dafür gibt, dass ein der Sache nach gleichwertiges Schutzniveau nicht länger gewährleistet ist.

3.2.3 Aufsicht

(157) Je nachdem, welche Befugnisse die zuständigen Behörden bei der Verarbeitung personenbezogener Daten zu Strafverfolgungszwecken ausüben (ob nach dem DPA 2018 oder dem IPA 2016), sind unterschiedliche Stellen für die Aufsicht über die Ausübung dieser Befugnisse zuständig. Der Information Commissioner beaufsichtigt die Verarbeitung personenbezogener Daten, wenn diese in den Anwendungsbereich von Teil 3 des DPA 2018 fallen.[226] Für die unabhängige und gerichtliche Aufsicht über die Ausübung von Ermittlungsbefugnissen im Rahmen des IPA 2016 ist hingegen das Büro des Beauftragten für Ermittlungsbefugnisse (Investigatory Powers Commissioner's Office – im Folgenden „IPCO") zuständig[227] (dieser Teil wird in den Erwägungsgründen 250 bis 255 behandelt). Zusätzliche Aufsichtsfunktionen werden vom Parlament und anderen Stellen wahrgenommen.

3.2.3.1 Aufsicht über die Umsetzung von Teil 3 des DPA 2018

(158) Die allgemeinen Aufgaben des Information Commissioner – dessen Unabhängigkeit und Organisation in Erwägungsgrund 87 erläutert werden – 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. Die Hauptaufgabe des ICO besteht darin, Teil 3 des DPA 2018 zu überwachen und durchzusetzen, die Öffentlichkeit zu sensibilisieren und das Parlament, die Regierung sowie andere Einrichtungen und Gremien zu beraten. 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. In diesen Fällen nehmen andere Stellen die Aufsichtsfunktionen wahr, wie in den Erwägungsgründen 99 bis 103 erläutert.

(159) Der Information Commissioner besitzt allgemeine Ermittlungs-, Berichtigungs-, Genehmigungs- und Beratungsbefugnisse im Hinblick auf die Verarbeitung personenbezogener Daten, die Gegenstand von Teil 3 sind. Insbesondere ist er befugt, den Verantwortlichen oder den Auftragsverarbeiter auf einen mutmaßlichen Verstoß gegen Teil 3 des DPA 2018 hinzuweisen, Warnungen oder Verwarnungen gegenüber einem Verantwortlichen oder Auftragsverarbeiter auszusprechen, der gegen Bestimmungen von Teil 3 des Gesetzes verstoßen hat, und zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder

226 Paragraf 116 DPA 2018.

227 Siehe IPA 2016, insbesondere Teil 8 Kapitel 1.

www.parlament.gv.at

auf Anfrage Stellungnahmen an das Parlament, die Regierung oder an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten.[228]

(160) Darüber hinaus besitzt der Information Commissioner die Befugnis, Informationsbescheide[229], Bewertungsbescheide[230] und Durchsetzungsbescheide[231] zu erlassen, sowie die Befugnis, Dokumente von Verantwortlichen und Auftragsverarbeitern einzusehen, Zugang deren Räumlichkeiten zu erlangen[232] und im Wege von Bußgeldbescheiden Geldbußen zu verhängen[233]. In den Leitlinien des ICO zu regulatorischen Maßnahmen (Regulatory Action Policy) ist festgelegt, unter welchen Umständen es einen Informations-, Bewertungs- Durchsetzungs- oder Bußgeldbescheid erteilt[234] (siehe auch Erwägungsgrund 93 und den Angemessenheitsbeschluss gemäß der Richtlinie (EU) 2016/680, Erwägungsgründe 101 und 102).

(161) Laut seinen letzten Jahresberichten (für die Zeiträume 2018–2019[235] und 2019–2020[236]) hat der Information Commissioner im Zusammenhang mit der Verarbeitung von Daten durch Strafverfolgungsbehörden eine Reihe von Untersuchungen durchgeführt und Durchsetzungsmaßnahmen ergriffen. 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). Bei einer anderen Untersuchung des Information Commissioner zur „Gangs-Matrix“[237] des Metropolitan Police Service stellte er eine Reihe von schwerwiegenden Verstößen gegen das Datenschutzrecht fest, die geeignet waren, das Vertrauen der Öffentlichkeit in die Matrix und die Verwendung der Daten zu untergraben. 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. In einem weiteren Fall verhängte der Information Commissioner im Mai 2018 im Rahmen einer Durchsetzungsmaßnahme eine Geldbuße in Höhe von

---

228 Anhang 13 Nummer 2 DPA 2018.

229 Mit diesem Bescheid werden der Verantwortliche und der Auftragsverarbeiter (und unter bestimmten Umständen jede andere Person) angewiesen, erforderliche Informationen bereitzustellen (Paragraf 142 DPA 2018).

230 Mit diesem Bescheid darf der Information Commissioner Untersuchungen und Überprüfungen durchführen, wobei 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 und Personen zu befragen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten (Paragraf 146 DPA 2018).

231 Mit diesem Bescheid kann der Information Commissioner Abhilfebefugnisse ausüben, um Verantwortliche bzw. Auftragsverarbeiter aufzufordern, bestimmte Maßnahmen zu ergreifen oder zu unterlassen (Paragraf 149 DPA 2018).

232 Paragraf 154 DPA 2018.

233 Paragraf 155 DPA 2018.

234 Regulatory Action Policy, siehe Fußnote 96.

235 Jahresbericht und Jahresabschluss 2018–19 des Information Commissioner, siehe Fußnote 101.

236 Jahresbericht und Jahresabschluss 2019-20 des Information Commissioner, siehe Fußnote 82.

237 Eine Datenbank, in der Erkenntnisse über mutmaßliche Bandenmitglieder und Opfer von Bandenkriminalität erfasst wurden.

www.parlament.gv.at

325 000 GBP gegen den Crown Prosecution Service wegen des Verlusts unverschlüsselter DVDs mit abgespeicherten Vernehmungsprotokollen. Der Information Commissioner führte auch 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. Des Weiteren ermittelt der Information Commissioner derzeit in einem Fall, bei dem es um den Zugriff auf Daten, die sich im Besitz eines privatwirtschaftlichen Unternehmens (Clearview AI Inc.) befinden, durch Strafverfolgungsbehörden geht.[238]

(162) Neben den in den Erwägungsgründen 160 und 161 beschriebenen Durchsetzungsbefugnissen des Information Commissioner stellen bestimmte Verstöße gegen die Datenschutzvorschriften Straftaten dar und können daher strafrechtlich geahndet werden (Paragraf 196 DPA 2018). Dies gilt beispielsweise für die Erlangung, Offenlegung oder Speicherung personenbezogener Daten ohne die Zustimmung des Verantwortlichen sowie die Veranlassung der Offenlegung personenbezogener Daten gegenüber einer anderen Person ohne die Zustimmung des Verantwortlichen[239], die Re-Identifizierung von anonymisiert vorliegenden personenbezogen Daten ohne die Zustimmung des für die Anonymisierung der personenbezogenen Daten zuständigen Verantwortlichen[240], die vorsätzliche Behinderung des Information Commissioner bei der Ausübung seiner Befugnisse in Bezug auf die Einsichtnahme in personenbezogene Daten gemäß internationalen Verpflichtungen[241], die Abgabe falscher Erklärungen bei der Erwiderung auf einen Informationsbescheid oder die Vernichtung von Informationen im Zusammenhang mit Informations- und Bewertungsbescheiden[242].

3.2.3.3 Andere Aufsichtsgremien im Bereich der Strafverfolgung

(163) Neben dem Information Commissioner gibt es eine Reihe weiterer Aufsichtsgremien im Bereich der Strafverfolgung mit spezifischen Mandaten, die für Fragen des Datenschutzes relevant sind. Hierzu zählen beispielsweise der Beauftragte für die Aufbewahrung und Verwendung von biometrischem Material (Commissioner for the Retention and Use of Biometric Material – „Biometrics Commissioner“)[243] und der Beauftragte für Überwachungskameras (Surveillance Camera Commissioner)[244].

---

238 Siehe Erklärung des ICO, abrufbar unter folgendem Link: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

239 Paragraf 170 DPA 2018.

240 Paragraf 171 DPA 2018.

241 Paragraf 119 Absatz 6 DPA 2018.

242 Während des Geschäftsjahres vom 1. April 2019 bis zum 31. März 2020 hat das ICO im Rahmen seiner Untersuchungen vier Verwarnungen ausgesprochen und in acht Fällen eine Strafverfolgung eingeleitet. Die Strafverfolgung erfolgte in diesen Fällen auf der Grundlage von Paragraf 55 des Datenschutzgesetzes (Data Protection Act) von 1998, Paragraf 77 des Gesetzes über die Informationsfreiheit (Freedom of Information Act) von 2000 und Paragraf 170 des Datenschutzgesetzes (Data Protection Act) von 2018. In 75 % der Fälle bekannten sich die Angeklagten schuldig, weshalb keine langwierigen und kostspieligen Prozesse notwendig waren. (Jahresbericht und Jahresabschluss 2019–2020 des Information Commissioner, siehe Fußnote 87, S. 40).

243 Das Amt des Biometrics Commissioner wurde mit dem Gesetz zum Schutz der Freiheiten (Protection of Freedoms Act, PoFA) von 2012 (siehe: https://www.legislation.gov.uk/ukpga/2012/9/contents). 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

www.parlament.gv.at

3.2.3.4 Parlamentarische Aufsicht im Bereich der Strafverfolgung

(164) Für die parlamentarische Aufsicht im Bereich der Strafverfolgung ist der Sonderausschuss für innere Angelegenheiten (Home Affairs Select Committee – HASC) zuständig. Er besteht aus elf Mitgliedern des Parlaments, die den drei stärksten politischen Parteien angehören. Die Aufgabe des Ausschusses besteht darin, die Ausgaben, die Verwaltung und die Verfahrensweisen des Innenministeriums und der mit ihm verbundenen öffentlichen Einrichtungen zu prüfen; er kann also auch ausdrücklich die Arbeit der Polizei und der NCA prüfen.[245]

(165) Der Ausschuss kann im Rahmen seiner Zuständigkeit den Untersuchungsgegenstand selbst wählen; dabei kann es sich auch um einzelne Fälle handeln, solange die Sache nicht anhängig ist. Zudem kann der Ausschuss schriftliches und mündliches Beweismaterial von einer Vielzahl von relevanten Gruppen und Einzelpersonen einholen. Er erstellt Berichte über seine Ergebnisse und gibt Empfehlungen an die Regierung ab.[246] Von der Regierung wird erwartet, dass sie auf jede der Empfehlungen des Berichts antwortet, und sie muss sich innerhalb von 60 Tagen äußern.[247]

(166) Im Bereich der Überwachung erstellte der Ausschuss auch einen Bericht über den Regulation of Investigatory Powers Act 2000 (im Folgenden „RIPA 2000“)[248]; darin

---

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 Biometrics Commissioner wird gemäß dem Code for Public Appointments (abrufbar unter folgendem Link: https://www.gov.uk/government/publications/governance-code-for-public-appointments) ernannt und aus seinem Mandat wird deutlich, dass er vom Innenminister nur unter eng gefassten Umständen seines Amtes enthoben werden darf; dazu gehören die Nichterfüllung seines Amtes für einen Zeitraum von drei Monaten, die Verurteilung wegen einer Straftat oder der Verstoß gegen sein Mandat.

244 Das Amt des Surveillance Camera Commissioner wurde mit dem Gesetz zum Schutz der Freiheiten (Protection of Freedoms Act) von 2012 eingerichtet; seine Aufgaben bestehen darin, die Förderung der Einhaltung des Verhaltenskodex für Überwachungskameras zu fördern, die Anwendung dieses Kodex zu überprüfen und Minister dahin gehend zu beraten, ob der Kodex geändert werden muss. Der Commissioner wird nach denselben Regeln wie der Biometrics Commissioner ernannt und verfügt über ähnliche Befugnisse, Ressourcen und Schutz vor Amtsenthebung

245 Siehe https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/.

246 Die Sonderausschüsse, einschließlich des Sonderausschusses für innere Angelegenheiten, unterliegen der Geschäftsordnung (Standing Orders) des britischen Unterhauses. Die Standing Orders sind die vom Unterhaus beschlossenen Vorschriften, die die Arbeitsweise des Parlaments regeln. Der Aufgabenbereich der Sonderausschüsse ist breit gefächert; in Standing Order 152 Absatz 1 heißt es hierzu, dass „Sonderausschüsse ernannt werden, um die Ausgaben, die Verwaltung und die Verfahrensweisen der wichtigsten Ministerien im Sinne von Absatz 2 dieser Order und der mit ihnen verbundenen öffentlichen Einrichtungen zu überprüfen“. Somit hat der Sonderausschuss für innere Angelegenheiten die Möglichkeit, jede politische Maßnahme des Innenministeriums zu prüfen, auch Maßnahmen (und die dazugehörigen Rechtsvorschriften) im Zusammenhang mit Ermittlungsbefugnissen. Darüber hinaus besagt Standing Order 152 Absatz 4, dass Ausschüsse verschiedene Befugnisse besitzen, unter anderem die Befugnis, Personen aufzufordern, Beweise oder Dokumente zu einem bestimmten Thema vorzulegen, und Berichte zu erstellen. Eine Übersicht über die aktuellen und früheren Untersuchungen des Ausschusses ist unter folgendem Link abrufbar: https://committees.parliament.uk/committee/83/home-affairs-committee/.

247 Die Befugnisse des Sonderausschusses für innere Angelegenheiten in England und Wales sind in den Standing Orders des Unterhauses dargelegt, die unter folgendem Link abrufbar sind: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

248 Abrufbar unter folgendem Link: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

wurde festgestellt, dass der RIPA 2000 nicht zweckmäßig sei. Die Ergebnisse dieses Berichts wurden berücksichtigt, als wesentliche Teile des RIPA 2000 durch den IPA 2016 ersetzt wurden. Eine vollständige Liste der Untersuchungen findet sich auf der Website des Ausschusses.[249]

(167) Die Aufgaben des Home Affairs Select Committee werden in Schottland vom Justiz-Unterausschuss für Polizeiarbeit (Justice Subcommittee on Policing) und in Nordirland vom Justizausschuss (Committee for Justice) wahrgenommen.[250]

3.2.4 Rechtsbehelfe

(168) In Bezug auf die Verarbeitung von Daten durch Strafverfolgungsbehörden stehen gemäß Teil 3 des DPA 2018 und gemäß dem IPA 2016 sowie gemäß dem Human Rights Act 1998 Rechtsbehelfe zur Verfügung.

(169) Durch diese Mechanismen stehen betroffenen Personen wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung, die es ihnen insbesondere ermöglichen, ihre Rechte durchzusetzen, unter anderem das Auskunftsrecht hinsichtlich ihrer personenbezogenen Daten oder das Recht auf Berichtigung oder Löschung dieser Daten.

(170) Erstens hat eine betroffene Person nach Paragraf 165 DPA 2018 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 vorliegt.[251] Der Information Commissioner hat 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, und Geldbußen zu verhängen.

(171) Zweitens besteht gemäß dem DPA 2018 das Recht auf einen Rechtsbehelf gegen den Information Commissioner, wenn dieser eine Beschwerde der betroffenen Person nicht angemessen bearbeitet. Konkret heißt dies: Wenn der Information Commissioner es versäumt, eine von der betroffenen Person eingereichte Beschwerde angemessen weiterzuverfolgen („progress“)[252], so hat der Beschwerdeführer Zugang zu einem

---

249 Abrufbar unter folgendem Link: https://committees.parliament.uk/committee/83/home-affairs-committee

250 Die Geschäftsordnung des Justice Subcommittee on Policing in Schottland ist unter folgendem Link abrufbar: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx. Die Geschäftsordnung des Committee for Justice in Nordirland ist unter folgendem Link abrufbar: http://www.niassembly.gov.uk/assembly-business/standing-orders/.

251 Der letzte Jahresbericht des ICO enthält eine nach Themenbereichen aufgeschlüsselte Übersicht über die eingegangenen und abgeschlossenen Beschwerden. So machen insbesondere die eingegangenen Beschwerden zum Thema „Polizeiarbeit und Strafregister“ („policing and criminal records“) 6 % aller insgesamt eingegangenen Beschwerden aus (ein Anstieg um 1 % im Vergleich zum vorherigen Geschäftsjahr). Aus dem Jahresbericht geht außerdem hervor, dass Beschwerden im Zusammenhang mit Auskunftsersuchen betroffener Personen am häufigsten sind (46 % aller Beschwerden, wobei im Vergleich zum vorherigen Geschäftsjahr ein Anstieg von 8 % zu verzeichnen war) (Jahresbericht 2019–2020 des ICO, S. 55; siehe Fußnote 88).

252 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

www.parlament.gv.at

gerichtlichen Rechtsbehelf; er kann sich bei einem First-tier Tribunal[253] beantragen, den Commissioner anzuweisen, geeignete Schritte zur Beantwortung der Beschwerde zu unternehmen oder den Beschwerdeführer über den Stand der Bearbeitung der Beschwerde zu informieren.[254] Darüber hinaus kann jede Person, die vom Commissioner einen der genannten Bescheide (Informations-, Bewertungs-, Durchsetzungs- oder Bußgeldbescheid) erhält, beim First-tier Tribunal Berufung 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.[255]

(172) Drittens können Einzelpersonen direkt vor Gericht Rechtsbehelfe gegen Verantwortliche und Auftragsverarbeiter einlegen. Insbesondere kann eine betroffene Person gemäß Paragraf 167 DPA 2018 vor Gericht Beschwerde wegen Verletzung ihrer durch das Datenschutzrecht zugesicherten Rechte einlegen, und das Gericht kann mittels Anordnung den Verantwortlichen auffordern, Maßnahmen bezüglich der Verarbeitung zu ergreifen (oder zu unterlassen), um den Bestimmungen des DPA 2018 nachzukommen. Darüber hinaus hat nach 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 oder der Auftragsverarbeiter weist nach, dass er in keiner Weise für den Vorfall verantwortlich ist, das den Schaden verursacht hat. Als Schaden gilt sowohl ein finanzieller als auch ein nichtfinanzieller Schaden, wie z. B. seelisches Leid.

(173) Viertens kann jede Person, die der Ansicht ist, dass ihre Rechte, einschließlich der Rechte auf Privatsphäre und Datenschutz, von einer Behörde verletzt wurden, vor den Gerichten des Vereinigten Königreichs gemäß dem Human Rights Act 1998 einen Rechtsbehelf einlegen[256]; und schließlich kann eine Person, eine nichtstaatliche

---

Beschwerde nicht innerhalb dieses Zeitraums ab und versäumt es, den Beschwerdeführer hierüber innerhalb eines weiteren Zeitraums von drei Monaten zu unterrichten.

253 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.

254 Paragraf 166 DPA 2018. Ein Beispiel für eine erfolgreiche Klage gegen das ICO vor dem Tribunal ist ein Fall, in dem das ICO den Eingang einer Beschwerde einer betroffenen Person zwar bestätigte, aber nicht angab, welche Maßnahmen es zu ergreifen beabsichtigte; es wurde daher angewiesen, innerhalb von 21 Kalendertagen zu bestätigen, ob es die Beschwerden untersuchen würde, und, falls ja, den Beschwerdeführer mindestens alle 21 Kalendertage über den Stand der Untersuchung zu informieren (das Urteil wurde noch nicht veröffentlicht). Ein weiteres Beispiel ist ein Fall, in dem nach Ansicht des First-tier Tribunal nicht ausreichend klar war, ob die Antwort des ICO an einen Beschwerdeführer tatsächlich das „Ergebnis“ der Beschwerde darstellte (siehe Susan Milne/The Information Commissioner [2020], das Urteil ist unter folgendem Link abrufbar: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

255 Paragrafen 162 und 163 DPA 2018.

256 Siehe z. B. die Rechtssache Brown/Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724, in der gemäß dem DPA 1998 und dem Human Rights Act 1998 Schadensersatz in Höhe von 9000 GBP für die unrechtmäßige Erlangung und den Missbrauch von personenbezogenen Daten zugesprochen wurde, sowie die Rechtssache R (on the application of Bridges)/Chief Constable of South Wales [2020] EWCA Civ 1058, in der der Court of Appeal den Einsatz eines

www.parlament.gv.at

Organisation oder Personengruppe, wenn alle nationalen Rechtsmittel ausgeschöpft wurden, vor dem Europäischen Gerichtshof für Menschenrechte aufgrund der Verletzung ihrer nach der Europäischen Menschenrechtskonvention garantierten Rechte Rechtsbehelfe einlegen (siehe Erwägungsgrund 111).[257]

3.2.4.1 Rechtsbehelfsverfahren gemäß dem IPA 2016

(174) Natürliche Personen können bei Verstößen gegen den IPA 2016 vor dem Gericht für Ermittlungsbefugnisse (Investigatory Powers Tribunal) Rechtsbehelfe einlegen. Die gemäß dem IPA 2016 verfügbaren Rechtsbehelfsverfahren sind in den Erwägungsgründen 263 bis 269 unten beschrieben.

3.3 Zugriff und Verwendung durch Behörden des Vereinigten Königreichs für Zwecke der nationalen Sicherheit

(175) Gemäß der Rechtsordnung des Vereinigten Königreichs sind folgende Nachrichtendienste in Situationen, die für die Bewertung der Angemessenheit relevant sind, befugt, aus Gründen der nationalen Sicherheit, elektronische Informationen zu sammeln, die sich im Besitz von Verantwortlichen oder Auftragsverarbeitern befinden: der Security Service[258] (im Folgenden „MI5“), der Secret Intelligence Service[259] (im Folgenden „SIS“) und die Government Communications Headquarters[260] (im Folgenden „GCHQ“).[261]

Gesichtserkennungssystems durch die Polizei von Wales für rechtswidrig erklärte, da dies einen Verstoß gegen Artikel 8 EMRK darstellte und die vom Verantwortlichen erstellte Datenschutz-Folgenabschätzung nicht dem DPA 2018 entsprach.

257 In Artikel 34 der Europäischen Menschenrechtskonvention heißt es hierzu: „Der Gerichtshof kann von jeder natürlichen Person, nichtstaatlichen Organisation oder Personengruppe, die behauptet, durch eine der Hohen Vertragsparteien in einem der in dieser Konvention oder den Protokollen dazu anerkannten Rechte verletzt zu sein, mit einer Beschwerde befasst werden. Die Hohen Vertragsparteien verpflichten sich, die wirksame Ausübung dieses Rechts nicht zu behindern.“

258 Der MI5 ist dem Innenminister unterstellt. Nach dem Security Service Act 1989 hat der MI5 folgende Aufgaben: Schutz der nationalen Sicherheit (einschließlich des Schutzes vor Bedrohungen durch Spionage, Terrorismus und Sabotage, vor Aktivitäten von Agenten ausländischer Mächte und vor Handlungen, die darauf abzielen, die parlamentarische Demokratie durch politische, industrielle oder gewaltsame Mittel zu stürzen oder zu untergraben), Schutz des wirtschaftlichen Wohls des Vereinigten Königreichs vor Bedrohungen von außen und Unterstützung der Tätigkeiten der Polizeikräfte und anderen Strafverfolgungsbehörden zur Verhütung und Aufdeckung von schweren Straftaten.

259 Der SIS ist dem Außenminister unterstellt und seine Aufgaben sind im Intelligence Services Act 1994 festgelegt. Seine Aufgaben sind die Beschaffung und Bereitstellung von Informationen über die Handlungen oder Absichten von Personen außerhalb der Britischen Inseln sowie weitere Aufgaben im Zusammenhang mit den Handlungen oder Absichten dieser Personen. Diese Aufgaben dürfen ausschließlich im Interesse der nationalen Sicherheit, im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs oder zur Unterstützung der Verhütung oder Aufdeckung von schweren Straftaten wahrgenommen werden.

260 Die GCHQ sind dem Außenminister unterstellt und ihre Aufgaben sind im Intelligence Services Act 1994 festgelegt. Dabei handelt es sich um folgende Aufgaben: a) Überwachung, Nutzung und Störung elektromagnetischer und anderer Emissionen und Geräte, die solche Emissionen erzeugen, Beschaffung und Bereitstellung von Informationen, die aus solchen Emissionen oder mit solchen Geräten sowie aus verschlüsseltem Material gewonnen wurden oder sich darauf beziehen, b) Beratung und Unterstützung der Streitkräfte, der Regierung oder anderer Organisationen oder Personen, die als geeignet erachtet werden, in Bezug auf Sprachen, einschließlich der für technische Angelegenheiten verwendeten Terminologie, sowie Kryptografie und andere Angelegenheiten bezüglich des Schutzes von Informationen. Diese Aufgaben dürfen ausschließlich im Interesse der nationalen Sicherheit, im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs in Bezug auf die Handlungen oder

www.parlament.gv.at

3.3.1 Rechtliche Grundlagen, Beschränkungen und Garantien

(176) Die Befugnisse der Nachrichtendienste des Vereinigten Königreichs sind im IPA 2016 und im RIPA 2000 festgelegt; zusammen mit dem DPA 2018 legen diese Rechtsakte den sachlichen und persönlichen Anwendungsbereich dieser Befugnisse sowie die Beschränkungen und Garantien für deren Ausübung fest. Die Befugnisse sowie die für sie geltenden Beschränkungen und Garantien werden in den folgenden Abschnitten im Detail bewertet.

3.3.1.1 Im Kontext der nationalen Sicherheit ausgeübte Ermittlungsbefugnisse

(177) Der IPA 2016 bildet den rechtlichen Rahmen für die Nutzung von Ermittlungsbefugnissen, d. h. die Befugnis, Kommunikationsdaten abzufangen und auf sie zuzugreifen sowie auf Geräte zuzugreifen. Gemäß dem IPA 2016 ist es allgemein verboten und eine Straftat, Techniken zu nutzen, die den Zugriff auf Kommunikationsinhalte, den Zugriff auf Kommunikationsdaten oder den Zugriff auf Geräte ohne gesetzliche Befugnis ermöglichen.[262] Dies zeigt sich darin, dass der Einsatz dieser Ermittlungsbefugnisse nur dann rechtmäßig ist, wenn er auf der Grundlage einer entsprechenden Anordnung oder einer Genehmigung erfolgt.[263]

(178) Der IPA 2016 enthält detaillierte Vorschriften über den Anwendungsbereich und die Anwendung der einzelnen Ermittlungsbefugnisse sowie die diesbezüglichen spezifischen Beschränkungen und Garantien. Je nach Art der Ermittlungsbefugnis (Abfangen von Kommunikation, Beschaffung und Speicherung von Kommunikationsdaten und Gerätezugriff)[264] sowie je nachdem, ob die Befugnis auf ein bestimmtes Ziel ausgerichtet oder massenhaft ausgeübt wird, gelten unterschiedliche Vorschriften. Der Anwendungsbereich, die Garantien und die Beschränkungen der einzelnen im Rahmen des IPA 2016 vorgesehenen Maßnahmen werden im folgenden Abschnitt näher erläutert.

Absichten von Personen außerhalb der Britischen Inseln oder zur Unterstützung der Verhütung oder Aufdeckung von schweren Straftaten wahrgenommen werden.

261 Andere öffentliche Einrichtungen, die für die nationale Sicherheit maßgebliche Funktionen ausüben, sind die Defence Intelligence (DI), der National Security Council und dessen Sekretariat, die Joint Intelligence Organisation (JIO) und das Joint Intelligence Committee (JIC). Allerdings sind weder das JIC noch die JIO in der Lage, von den Ermittlungsbefugnissen gemäß dem IPA 2016 Gebrauch zu machen, während die DI nur begrenzte Möglichkeiten zur Ausübung dieser Befugnisse hat.

262 Das Verbot gilt sowohl für öffentliche und private Kommunikationsnetze als auch für den öffentlichen Postdienstleister, wenn die Abfangaktion im Vereinigten Königreich erfolgt. Es gilt nicht für den Verantwortlichen des privaten Netzes, wenn der Verantwortliche eine ausdrückliche oder stillschweigende Einwilligung zur Durchführung der Abfangaktion erteilt hat (Paragraf 3 IPA 2016).

263 In bestimmten begrenzten Fällen ist eine Abfangmaßnahme auch ohne eine entsprechende Anordnung rechtmäßig, nämlich dann, wenn eine Einwilligung des Absenders oder Empfängers vorliegt (Paragraf 44 IPA 2016), bei begrenzten Verwaltungs- oder Vollstreckungszwecken (Paragrafen 45 bis 48 IPA 2016), in bestimmten Einrichtungen (Paragrafen 49 bis 51 IPA 2016) und nach entsprechenden Ersuchen aus dem Ausland (Paragraf 52 IPA 2016).

264 Was beispielsweise den Anwendungsbereich solcher Maßnahmen betrifft, ist im Rahmen von Teil 3 und Teil 4 (Speicherung und Beschaffung von Kommunikationsdaten) der Anwendungsbereich der Maßnahme eng verknüpft mit der Definition von „Telekommunikationsbetreibern“ („telecommunication operators“), deren Nutzerdaten der Maßnahme unterliegen. Ein weiteres Beispiel kann im Zusammenhang mit der Nutzung von Massenbefugnissen („bulk“ powers) angeführt werden. In diesem Fall beschränkt sich der Anwendungsbereich dieser Befugnisse auf „Kommunikationsvorgänge, die von Einzelpersonen außerhalb der Britischen Inseln gesendet oder empfangen werden“.

www.parlament.gv.at

(179) Außerdem wird der IPA 2016 durch eine Reihe von gesetzlichen Verhaltenskodizes („Codes of Practice“) ergänzt, die vom Secretary of State herausgegeben und von beiden Kammern des Parlaments gebilligt wurden;[265] diese Kodizes gelten landesweit und enthalten weitere Leitlinien für die Nutzung dieser Befugnisse.[266] Während sich betroffene Personen unmittelbar auf die Bestimmungen des IPA 2016 berufen können, um ihre Rechte geltend zu machen, ist in Anhang 7 Nummer 5 IPA 2016 festgelegt, dass die Codes of Practice als Beweismittel in Zivil- und Strafverfahren zulässig sind und das Gericht, Tribunal oder die Aufsichtsbehörde eine Nichteinhaltung dieser Kodizes bei einschlägigen Entscheidungen in Gerichtsverfahren berücksichtigen kann.[267] Als sie die „Qualität des Gesetzes“ der früheren Gesetzgebung des Vereinigten Königreichs im Bereich Überwachung, den RIPA 2000, bewertete, hat die Große Kammer des Europäischen Gerichtshofs für Menschenrechte die Relevanz der britischen Verhaltenskodizes ausdrücklich anerkannt und akzeptiert, dass die in ihm enthaltenen Bestimmungen bei der Beurteilung der Vorhersehbarkeit der Gesetzgebung, die eine Überwachung erlaubt, berücksichtigt werden können.[268]

(180) Ferner sei darauf verwiesen, dass gezielte Befugnisse (gezieltes Abfangen[269], gezielte Beschaffung von Kommunikationsdaten[270], gezielte Speicherung von Kommunikationsdaten[271] und gezielter Gerätezugriff[272]) den nationalen

---

265 In Anhang 7 des IPA 2016 sind der Anwendungsbereich der Kodizes, das bei ihrem Erlass zu befolgende Verfahren, die Vorschriften für ihre Überarbeitung und die Wirkung der Kodizes festgelegt.

266 Die Verhaltenskodizes nach Maßgabe des IPA 2016 sind unter folgendem Link abrufbar: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

267 Gerichte und Tribunale bewerten anhand der Verhaltenskodizes die Rechtmäßigkeit des Verhaltens der Behörden. Siehe zum Beispiel die Rechtssache Dias/Cleveland Police, [2017] UKIPTrib15_586-CH, in der das Investigatory Powers Tribunal Bezug auf bestimmte Passagen des Verhaltenskodex zu Kommunikationsdaten (Code of Practice on Communication Data) nahm, um die Definition des Grundes der „Verhütung oder Aufdeckung von Straftaten oder Aufrechterhaltung der Ordnung“ zu verstehen, aufgrund dessen die Beschaffung von Kommunikationsdaten beantragt wurde. Der Kodex wurde in die Erwägungen einbezogen, um festzustellen, ob dieser Grund unsachgemäß angeführt worden war. Das Gericht gelangte zu dem Schluss, dass das angefochtene Verhalten rechtswidrig war. Des Weiteren haben Gerichte den Umfang der in den Kodizes enthaltenen Garantien bewertet; siehe z. B. die Rechtssache Just for Law Kids/Secretary of State for the Home Department, [2019] EWHC 1772 (Admin), in der der High Court feststellte, dass das Primär- und Sekundärrecht in Verbindung mit den internen Leitlinien ausreichende Garantien boten; oder die Rechtssache R (National Council for Civil Liberties)/Secretary of State for the Home Department & Others, [2019] EWHC 2057 (Admin), in dem der High Court feststellte, dass sowohl der IPA 2016 als auch der Verhaltenskodex für den Gerätezugriff ausreichende Bestimmungen hinsichtlich der Notwendigkeit der Spezifizität von Anordnungen enthielten.

268 In der Rechtssache Big Brother Watch stellte die Große Kammer des Europäischen Gerichtshofs für Menschenrechte Folgendes fest: „Der Kodex für das Abfangen von Kommunikationsvorgängen ist ein von beiden Kammern des Parlaments gebilligtes öffentliches Dokument, das von der Regierung online und in gedruckter Form veröffentlicht wird und das sowohl von Personen, die Abfangpflichten ausüben, als auch von den Gerichten zu berücksichtigen ist (siehe Rn. 93-94). Daher hat dieser Gerichtshof anerkannt, dass die in ihm enthaltenen Bestimmungen bei der Beurteilung der Vorhersehbarkeit des RIPA berücksichtigt werden können (siehe Kennedy, a.a.O., § 157). Dementsprechend würde der Gerichtshof bejahen, dass das innerstaatliche Recht angemessen ‚zugänglich‘ war.“ (siehe Europäischer Gerichtshof für Menschenrechte (Große Kammer), Big Brother Watch u. a./Vereinigtes Königreich, Beschwerden Nr. 58170/13, 62322/14 und 24960/15, vom 25. Mai 2021, Rn. 366).

269 Teil 2 des IPA 2016.

270 Teil 3 des IPA 2016.

271 Teil 4 des IPA 2016.

272 Teil 5 des IPA 2016.

www.parlament.gv.at

Sicherheitsbehörden sowie bestimmten Strafverfolgungsbehörden[273] zur Verfügung stehen, während Massenbefugnisse (d. h. massenhaftes Abfangen[274], massenhafte Beschaffung von Kommunikationsdaten[275], massenhafter Gerätezugriff[276] und Erfassung in personenbezogenen Massendatensätzen[277]) nur von Nachrichtendiensten ausgeübt werden dürfen.

(181) Bei der Entscheidung darüber, welche Ermittlungsbefugnis ausgeübt werden soll, muss der Nachrichtendienst den in Paragraf 2 Absatz 2 Buchstabe a IPA 2016 aufgeführten „allgemeinen Pflichten in Bezug auf den Schutz der Privatsphäre" („general duties in relation to privacy") nachkommen, die eine Prüfung der Notwendigkeit und Verhältnismäßigkeit umfassen. So muss eine Behörde, die die Absicht hat, eine Ermittlungsbefugnis zu nutzen, gemäß dieser Bestimmung Folgendes prüfen: i) ob das mit der Anordnung, der Genehmigung oder dem Bescheid angestrebte Ziel nach vernünftigem Ermessen auch mit anderen, weniger stark eingreifenden Mitteln erreicht werden könnte, ii) ob das Schutzniveau, das in Bezug auf die Beschaffung von Informationen aufgrund der Anordnung, der Genehmigung oder des Bescheids zugrunde zu legen ist, aufgrund der besonderen Sensibilität dieser Informationen höher ist, iii) das öffentliche Interesse an der Integrität und Sicherheit von Telekommunikationssystemen und Postdiensten sowie iv) alle anderen Aspekte des öffentlichen Interesses am Schutz der Privatsphäre[278].

(182) Die Art und Weise, wie diese Kriterien anzuwenden sind – und wie ihre Einhaltung im Rahmen der Genehmigung der Nutzung derartiger Befugnisse durch den Secretary of State und die unabhängigen Judicial Commissioners bewertet wird –, wird in den entsprechenden Verhaltenskodizes näher erläutert. Insbesondere muss die Ausübung einer dieser Ermittlungsbefugnisse stets „in einem angemessenen Verhältnis zu dem angestrebten Ziel stehen, wofür die Schwere des Eingriffs in die Privatsphäre (sowie weitere Erwägungen gemäß Paragraf 2 Absatz 2) gegen die Notwendigkeit der Aktivität im Hinblick auf Ermittlungen, Einsatzzwecke oder Kapazitäten abgewogen werden muss". Dies bedeutet insbesondere, dass „die Ausübung der Befugnis eine realistische Aussicht bieten sollte, dass sich der erwartete Nutzen einstellt, und nicht unverhältnismäßig oder willkürlich sein sollte"; ferner „sollte ein Eingriff in die Privatsphäre nicht als verhältnismäßig angesehen werden, wenn die benötigten

---

273 Eine Auflistung der einschlägigen Strafverfolgungsbehörden, die gezielte Ermittlungsbefugnisse gemäß dem IPA 2016 ausüben dürfen, enthält Fußnote (139).

274 Paragraf 136 IPA 2016.

275 Paragraf 158 IPA 2016.

276 Paragraf 176 IPA 2016.

277 Paragraf 199 IPA 2016.

278 Gemäß dem Verhaltenskodex für das Abfangen von Kommunikationsvorgängen werden im Rahmen der Verhältnismäßigkeitsprüfung folgende weitere Elemente geprüft: „i) das Ausmaß des vorgeschlagenen Eingriffs in die Privatsphäre im Vergleich zum angestrebten Ziel, ii) wie und warum die anzuwendenden Methoden die geringstmögliche Beeinträchtigung für die Person und für andere verursachen werden, iii) ob die Aktivität eine angemessene Anwendung des Gesetzes und – unter Berücksichtigung aller vernünftigen Alternativen – einen vernünftigen Weg darstellt, um das angestrebte Ziel zu erreichen, iv) welche anderen Methoden gegebenenfalls entweder nicht angewandt wurden oder zwar angewandt wurden, aber als unzureichend erachtet werden, um die operativen Ziele ohne den Einsatz der vorgeschlagenen Ermittlungsbefugnis zu erreichen." Code of Practice on Interception of Communications, Nummer 4.16, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

www.parlament.gv.at

Informationen nach vernünftigem Ermessen auch mit anderen, weniger stark eingreifenden Mitteln erlangt werden könnten“.[279] Im Einzelnen ist die Einhaltung des Grundsatzes der Verhältnismäßigkeit anhand folgender Kriterien zu beurteilen: „i) dem Ausmaß des vorgeschlagenen Eingriffs in die Privatsphäre im Vergleich zum angestrebten Ziel, ii) wie und warum die anzuwendenden Methoden die geringstmögliche Beeinträchtigung für die Person und für andere verursachen werden, iii) ob die Aktivität eine angemessene Anwendung des Gesetzes und – unter Berücksichtigung aller vernünftigen Alternativen – einen vernünftigen Weg darstellt, um das angestrebte Ziel zu erreichen, iv) welche anderen Methoden gegebenenfalls entweder nicht angewandt wurden oder zwar angewandt wurden, aber als unzureichend erachtet werden, um die operativen Ziele ohne den Einsatz der vorgeschlagenen Ermittlungsbefugnis zu erreichen.“[280]

(183) Gemäß den Erläuterungen der britischen Behörden wird dadurch in der Praxis sichergestellt, dass ein Nachrichtendienst zunächst das operative Ziel festlegt (und damit die Erhebung eingrenzt, z. B. einen Zweck der internationalen Terrorismusbekämpfung in einem bestimmten geografischen Gebiet) und danach auf der Grundlage dieses operativen Ziels prüfen muss, welche technische Option (z. B. gezieltes oder massenhaftes Abfangen, gezielter oder massenhafter Gerätezugriff, gezielte oder massenhafte Beschaffung von Kommunikationsdaten) im Hinblick auf das angestrebte Ziel am verhältnismäßigsten ist (d. h. am wenigsten in die Privatsphäre eingreift, vgl. Paragraf 2 Absatz 2 IPA) und daher auf einer der verfügbaren gesetzlichen Grundlagen genehmigt werden kann.

(184) Es ist auch anzumerken, dass diese Anwendung der Grundsätze der Notwendigkeit und Verhältnismäßigkeit auch vom UN-Sonderberichterstatter über das Recht auf Privatheit, Joseph Cannataci, zur Kenntnis genommen und begrüßt wurde; dieser stellte im Hinblick auf das durch den IPA 2016 geschaffene System fest, dass „die sowohl innerhalb der Nachrichtendienste als auch innerhalb der Strafverfolgungsbehörden bestehenden Verfahren es offenbar systematisch erforderlich machen, die Notwendigkeit und Verhältnismäßigkeit einer Überwachungsmaßnahme oder -aktion zu bewerten, bevor sie zur Genehmigung empfohlen wird, und sie aus denselben Gründen zu überprüfen“.[281] Des Weiteren stellte er fest, dass bei seinem Treffen mit Vertretern von Strafverfolgungsbehörden und nationalen Sicherheitsbehörden „die übereinstimmende Meinung herrschte, dass das Recht auf Privatsphäre bei jeder Entscheidung über Überwachungsmaßnahmen eine vorrangige Erwägung sein muss. Alle Vertreter haben die Grundsätze der Notwendigkeit und Verhältnismäßigkeit als die wesentlichen Prinzipien verstanden und geschätzt, die es zu berücksichtigen gilt.“

(185) Die spezifischen Kriterien für den Erlass der verschiedenen Anordnungen sowie die gemäß dem IPA 2016 für die einzelnen Ermittlungsbefugnisse geltenden

---

279 Siehe Code of Practice on Interception of Communications, Nummern 4.12 und 4.15, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

280 Siehe Code of Practice on Interception of Communications, Nummer 4.16.

281 Erklärung des Sonderberichterstatters über das Recht auf Privatheit zum Abschluss seiner Mission im Vereinigten Königreich von Großbritannien und Nordirland, abrufbar unter folgendem Link: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, Nummer 1 Buchstabe a.

www.parlament.gv.at

Beschränkungen und Garantien sind in den Erwägungsgründen 186 bis 243 aufgeführt.

3.3.1.1.1 Gezieltes Abfangen und gezielte Überprüfung

(186) Es gibt drei Arten von Anordnungen für gezieltes Abfangen: die Anordnung zum gezielten Abfangen[282], die Anordnung zur gezielten Überprüfung und eine Amtshilfeanordnung[283]. Die Bedingungen für den Erhalt solcher Anordnungen und die entsprechenden Garantien sind in Teil 2 Kapitel 1 des IPA 2016 aufgeführt.

(187) Eine Anordnung zum gezielten Abfangen gestattet das Abfangen der in der Anordnung beschriebenen Kommunikationsvorgänge während ihrer Übertragung sowie die Erlangung anderer für diese Kommunikationsvorgänge relevanter Daten[284], einschließlich Sekundärdaten[285]. Eine Anordnung zur gezielten Überprüfung gestattet einer Person, abgefangene Inhalte, die aufgrund einer Anordnung zum massenhaften Abfangen erlangt wurden, für eine Überprüfung auszuwählen.[286]

(188) Eine Anordnung nach Maßgabe von Teil 2 des IPA 2016 kann vom Secretary of State ausgestellt[287] und von einem Judicial Commissioner genehmigt werden.[288] In allen Fällen ist die Dauer einer Anordnung gleich welcher Art auf sechs Monate begrenzt[289]; zudem gelten besondere Vorschriften für ihre Änderung[290] und Verlängerung[291].

(189) Vor dem Erlass einer Anordnung muss der Secretary of State eine Prüfung der Notwendigkeit und Verhältnismäßigkeit durchführen.[292] Insbesondere bei einer Anordnung zum gezielten Abfangen und einer Anordnung zur gezielten Überprüfung

---

282 Paragraf 15 Absatz 2 IPA 2016.

283 Paragraf 15 Absatz 4 IPA 2016.

284 Paragraf 15 Absatz 2 IPA 2016.

285 Sekundärdaten sind Daten, die mit dem abgefangenen Kommunikationsvorgang verknüpft oder logisch verbunden sind, die logisch von dem Kommunikationsvorgang getrennt werden können und die, wenn sie getrennt würden, nichts von dem preisgeben würden, was nach vernünftigem Ermessen als der Inhalt (sofern vorhanden) des Kommunikationsvorgangs angesehen werden könnte. Beispiele für Sekundärdaten sind Router-Konfigurationen oder Firewalls oder die Zeitspanne, in der ein Router in einem Netzwerk aktiv war, wenn diese Daten Teil des abgefangenen Kommunikationsvorgangs sind, mit ihm verknüpft sind oder logisch mit ihm verbunden sind. Für weitere Einzelheiten siehe die Definition in Paragraf 16 IPA 2016 sowie den Code of Practice on Interception of Communications, Nummer 2.19, siehe Fußnote 278.

286 Die Durchführung einer solchen Überprüfung stellt eine Ausnahme von Paragraf 152 Absatz 4 IPA 2016 dar, wonach es verboten ist, Kommunikationsvorgänge von Personen zu erfassen, die sich auf den Britischen Inseln befinden. Siehe Erwägungsgrund 229.

287 Der schottische Minister genehmigt die Anordnung, wenn sie sich auf schwerwiegende kriminelle Aktivitäten in Schottland bezieht (siehe Paragrafen 21 und 22 IPA 2016); ein hoher Beamter kann vom Secretary of State dazu bestimmt werden, eine Amtshilfeanordnung zu erlassen, wenn eine Abfangmaßnahme eine Person oder Räumlichkeiten betrifft, die sich außerhalb des Vereinigten Königreichs befinden (Paragraf 40 IPA 2016).

288 Paragrafen 19 und 23 IPA 2016.

289 Paragraf 32 IPA 2016.

290 Paragraf 39 IPA 2016. Begrenzte Änderungen an einer Anordnung können von bestimmten Personen unter den im IPA 2016 festgelegten Bedingungen vorgenommen werden. Die Person, die eine Anordnung ausgestellt hat, kann diese jederzeit aufheben. Sie ist dazu verpflichtet, wenn die Anordnung aus einem maßgeblichen Grund nicht mehr erforderlich ist oder wenn die durch die Anordnung genehmigte Verfahrensweise im Hinblick auf das angestrebte Ziel nicht mehr verhältnismäßig ist.

291 Paragraf 33 IPA 2016. Die Entscheidung zur Verlängerung einer Anordnung muss von einem Judicial Commissioner genehmigt werden.

292 Paragraf 19 IPA 2016.

www.parlament.gv.at

sollte der Secretary of State prüfen, ob die Maßnahme aus einem der folgenden Gründe notwendig ist: im Interesse der nationalen Sicherheit, zur Verhütung oder Aufdeckung von schweren Straftaten oder im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs[293], sofern diese Interessen auch für die Interessen der nationalen Sicherheit relevant sind[294]. Hingegen kann eine Amtshilfeanordnung (siehe Erwägungsgrund 139 oben) nur dann ausgestellt werden, wenn nach Ansicht des Secretary of State Umstände vorliegen, die mit den Umständen vergleichbar sind, unter denen er eine Anordnung zum Zweck der Verhütung und/oder Aufdeckung schwerer Straftaten erlassen würde.[295]

(190) Darüber hinaus sollte der Secretary of State beurteilen, ob die Maßnahme im Hinblick auf das angestrebte Ziel verhältnismäßig ist.[296] Bei der Beurteilung der Verhältnismäßigkeit der beantragten Maßnahmen sind die allgemeinen Pflichten in Bezug auf den Schutz der Privatsphäre gemäß Paragraf 2 Absatz 2 IPA 2016 zu berücksichtigen; insbesondere ist zu beurteilen, ob das mit der Anordnung, der Genehmigung oder dem Bescheid angestrebte Ziel nach vernünftigem Ermessen auch mit anderen, weniger stark eingreifenden Mitteln erreicht werden könnte und ob das Schutzniveau, das in Bezug auf die Erlangung von Informationen aufgrund der Anordnung, der Genehmigung oder des Bescheids zugrunde zu legen ist, aufgrund der besonderen Sensibilität dieser Informationen höher ist (siehe Erwägungsgrund 181 oben).

(191) Zu diesem Zweck muss der Secretary of State alle im Antrag der beantragenden Behörde dargelegten Elemente berücksichtigten, insbesondere diejenigen, die sich auf die zu überwachenden Personen und die Relevanz der Maßnahme für die Ermittlungen beziehen. Diese Elemente sind im Verhaltenskodex für das Abfangen von Kommunikationsvorgängen (Code of Practice on Interception of Communications) festgelegt und müssen hinreichend spezifisch beschrieben werden.[297] Darüber hinaus ist in Paragraf 17 des IPA 2016 vorgesehen, dass in jeder gemäß Kapitel 2 des IPA 2016 ausgestellten Anordnung die jeweilige Person oder eine Personengruppe, Organisation oder Räumlichkeit, die überwacht werden sollen (das „Ziel“ („target“)), benannt oder beschrieben werden muss. Im Falle einer Anordnung zum gezielten Abfangen oder einer Anordnung zur gezielten Überprüfung können damit auch eine

---

293 Zum Begriff „Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs, sofern diese Interessen auch für die Interessen der nationalen Sicherheit relevant sind“ („interests of the economic well-being of the United Kingdom, so far as those interests are also relevant for national security“) hat die Große Kammer des Europäischen Gerichtshofs für Menschenrechte in der Rechtssache Big Brother Watch u. a./Vereinigtes Königreich (siehe Fußnote 268 oben), Rn. 371, festgestellt, dass dieser Begriff hinreichend auf die nationale Sicherheit ausgerichtet war. Zwar bezog sich die Feststellung des Hofes in diesem Fall auf die Verwendung dieses Begriffs im RIPA 2000, jedoch wird derselbe Begriff auch im IPA 2016 verwendet.

294 Paragraf 20 Absatz 2 IPA 2016.

295 Paragraf 20 Absatz 3 IPA 2016.

296 Paragraf 19 Absatz 1 Buchstabe b, Paragraf 19 Absatz 2 Buchstabe b und Paragraf 19 Absatz 3 Buchstabe b IPA 2016.

297 Die angeforderten Informationen umfassen Einzelheiten über den Hintergrund (Beschreibung der zu überwachenden Personen/Organisationen/Räumlichkeiten, des abzufangenden Kommunikationsvorgangs) und darüber, wie die Erlangung dieser Informationen den Ermittlungen zugute kommt, sowie eine Beschreibung der zu genehmigenden Handlung. Ist eine Beschreibung der Personen/Organisationen/Räumlichkeiten nicht möglich, muss eine Erklärung dazu beigefügt werden, warum dies nicht möglich war oder warum nur eine allgemeine Beschreibung vorgenommen wurde (Code of Practice on Interception of Communications, Nummern 5.32 und 5.34, siehe Fußnote 278).

www.parlament.gv.at

Personengruppe, mehrere Personen oder Organisationen oder mehrere Räumlichkeiten gemeint sein (auch genannt „thematische Anordnung“ („thematic warrant“)).[298] In diesen Fällen sollten in der Anordnung der gemeinsame Zweck oder die gemeinsame Tätigkeit der Personengruppe oder des Einsatzes/der Untersuchung beschrieben und so viele dieser Personen/Organisationen oder Räumlichkeiten benannt oder beschrieben werden, wie es nach vernünftigem Ermessen möglich ist.[299] Schließlich sind in allen nach Teil 2 des IPA 2016 ausgestellten Anordnungen die Adressen, Nummern, Vorrichtungen, Faktoren oder Kombinationen von Faktoren anzugeben, die zur Identifizierung der Kommunikationsvorgänge verwendet werden sollen.[300] Diesbezüglich heißt es im Code of Practice on Interception of Communications, dass im Falle einer Anordnung zum gezielten Abfangen und einer Anordnung zur gezielten Überprüfung „die Faktoren oder die Kombination von Faktoren anzugeben (oder zu beschreiben) sind, die zur Identifizierung der Kommunikationsvorgänge verwendet werden sollen. Sollten die Kommunikationsvorgänge beispielsweise anhand einer Telefonnummer identifiziert werden, muss diese Nummer vollständig angegeben werden. Sollen jedoch sehr komplexe oder sich laufend ändernde Internet-Selektoren zur Identifizierung der Kommunikationsvorgänge verwendet werden, sollten diese Selektoren so weit wie möglich beschrieben werden.“[301]

(192) Eine wichtige Garantie in diesem Zusammenhang besteht darin, dass die vom Secretary of State vorgenommene Bewertung zur Ausstellung einer Anordnung von einem unabhängigen Judicial Commissioner genehmigt werden muss[302], wobei dieser insbesondere prüft, ob die Entscheidung zur Ausstellung der Anordnung den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit entspricht[303] (zum Status und zur Rolle der Judicial Commissioners siehe Erwägungsgründe 251 bis 256 unten). Des Weiteren wird im IPA 2016 präzisiert, dass der Judicial Commissioner bei der Durchführung einer solchen Prüfung die gleichen Grundsätze zugrunde legen muss, die ein Gericht bei einer Anfechtungsklage anwenden würde.[304] Dadurch wird sichergestellt, dass in jedem Fall und vor einem Datenzugriff die Einhaltung der Grundsätze der Notwendigkeit und Verhältnismäßigkeit systematisch durch eine unabhängige Stelle überprüft wird.

(193) Der IPA 2016 sieht wenige spezifische und eng gefasste Ausnahmen für gezielte Abfangmaßnahmen ohne entsprechende Anordnung vor. Die wenigen Fälle sind gesetzlich geregelt[305] und werden – mit Ausnahme der Fälle, für die eine „Einwilligung“ („consent“) des Absenders/Empfängers vorliegt – von Personen (privaten oder öffentlichen Stellen) durchgeführt, die keine nationalen

---

298 Paragraf 17 Absatz 2 IPA 2016. Siehe auch Code of Practice on Interception of Communications, Nummer 5.11 ff., siehe Fußnote 278.

299 Paragraf 31 Absätze 4 und 5 IPA 2016.

300 Paragraf 31 Absatz 8 IPA 2016.

301 Code of Practice on Interception of Communications, Nummern 5.37 und 5.38, siehe Fußnote 278.

302 Eine Genehmigung durch einen Judicial Commissioner ist nicht erforderlich, wenn der Secretary of State der Ansicht ist, dass eine dringende Notwendigkeit für den Erlass der Anordnung besteht (Paragraf 19 Absatz 1 IPA). Der Judicial Commissioner muss jedoch innerhalb kurzer Zeit informiert werden und muss entscheiden, ob er die Anordnung genehmigt oder nicht. Im Falle einer Ablehnung tritt die Anordnung außer Kraft (Paragrafen 24 und 25 IPA 2016).

303 Paragraf 23 Absatz 1 IPA 2016.

304 Paragraf 23 Absatz 2 IPA 2016.

305 Siehe Paragrafen 44 bis 51 IPA 2016 und Abschnitt 12 des Interception Communication Code of Practice (siehe Fußnote 278).

www.parlament.gv.at

Sicherheitsbehörden sind. Darüber hinaus werden diese Arten des Abfangens zu anderen Zwecken als der Gewinnung „nachrichtendienstlicher Erkenntnisse“ („intelligence“)[306] durchgeführt, und für einige von ihnen ist es sehr unwahrscheinlich, dass die Erhebung im Rahmen einer „Übermittlung“ („transfer“) erfolgen kann (z. B. bei Abfangmaßnahmen in psychiatrischen Krankenhäusern oder in Gefängnissen). Angesichts der Art der Stelle, für die spezifischen Fälle gelten (andere als nationale Sicherheitsbehörden), gelten alle in Teil 2 des DPA 2018 und der UK GDPR vorgesehenen Garantien, einschließlich der Aufsicht durch das ICO und der verfügbaren Rechtsbehelfe. Zusätzlich zu den im DPA 2018 vorgesehenen Garantien ist darüber hinaus im IPA 2016 in bestimmten Fällen auch die Ex-post-Aufsicht durch das IPCO vorgesehen.[307]

(194) Bei der Durchführung von Abfangmaßnahmen gelten zusätzliche Beschränkungen und Garantien im Hinblick auf den spezifischen Status der überwachten Person(en).[308] Beispielsweise ist das Abfangen von Kommunikationsinhalten, die einem Rechtsprivileg unterliegen, nur in außergewöhnlichen und zwingenden Umständen zulässig; die Person, die die Anordnung ausstellt, muss das öffentliche Interesse an der Vertraulichkeit von einem Rechtsprivileg unterliegenden Inhalten berücksichtigen und sicherstellen, dass besondere Anforderungen für die Handhabung, Aufbewahrung und Offenlegung des betreffenden Materials bestehen.[309]

(195) Darüber hinaus sieht der IPA 2016 spezielle Garantien in Bezug auf Sicherheit, Aufbewahrung und Offenlegung vor, die der Secretary of State vor der Ausstellung einer gezielten Anordnung berücksichtigen sollte.[310] So ist in Paragraf 53 Absatz 5 IPA 2016 vorgesehen, dass jede Kopie, die von dem im Rahmen der Anordnung gesammelten Material angefertigt wird, sicher aufbewahrt werden muss und vernichtet wird, sobald es keine maßgeblichen Gründe mehr für die Aufbewahrung gibt; Paragraf 53 Absatz 2 IPA 2016 wiederum schreibt vor, dass die Anzahl der Personen, an die das Material weitergegeben wird, und der Umfang, in dem Material offengelegt, zugänglich gemacht oder kopiert wird, auf das für die gesetzlichen Zwecke erforderliche Mindestmaß beschränkt werden müssen.

(196) Schließlich gilt: Wenn das Material, das im Rahmen einer Anordnung zum gezielten Abfangen oder einer Amtshilfeanordnung abgefangen wurde, an ein Drittland übergeben werden soll (Offenlegung gegenüber dem Ausland („overseas disclosures“)), muss der Secretary of State gemäß dem IPA 2016 sicherstellen, dass geeignete Vorkehrungen getroffen werden, um zu gewährleisten, dass in diesem

---

306 Dies ist beispielsweise der Fall, wenn ein Abfangen im Gefängnis oder in einem psychiatrischen Krankenhaus erforderlich ist (zur Überprüfung des Verhaltens einer inhaftierten Person oder eines Patienten) oder durch einen Post- oder Telekommunikationsbetreiber, um beispielsweise missbräuchliche Inhalte aufzudecken.

307 Siehe im Umkehrschluss Paragraf 229Absatz 4 des IPA.

308 Die Paragrafen 26 bis 29 IPA 2016 enthalten Beschränkungen bezüglich der Ausstellung von Anordnungen zum gezielten Abfangen oder zur gezielten Untersuchung im Zusammenhang mit folgenden Maßnahmen: das Abfangen von Kommunikationsvorgängen, deren Urheber oder Adressat ein Mitglied eines Parlaments (eines der Parlamente des Vereinigten Königreichs) ist, das Abfangen von Kommunikationsinhalten, die einem Rechtsprivileg unterliegen, das Abfangen von Kommunikationsvorgängen, die nach Ansicht der abfangenden Behörde vertrauliches journalistisches Material enthalten, und wenn der Zweck der Anordnung darin besteht, eine Quelle für journalistische Informationen zu identifizieren oder zu bestätigen.

309 Paragraf 26 IPA 2016.

310 Paragraf 19 Absatz 1 IPA 2016.

www.parlament.gv.at

Drittland ähnliche Garantien in Bezug auf Sicherheit, Aufbewahrung und Offenlegung bestehen.[311] Außerdem sieht Paragraf 109 Absatz 2 des DPA 2018 vor, dass Nachrichtendienste personenbezogene Daten nur dann aus dem Gebiet des Vereinigten Königreichs übermitteln dürfen, wenn die Übermittlung für die Erfüllung der gesetzlichen Aufgaben des Verantwortlichen oder für andere in Paragraf 2 Absatz 2 Buchstabe a des Security Service Act 1989 oder in Paragraf 2 Absatz 2 Buchstabe a und Paragraf 4 Absatz 2 Buchstabe a des Intelligence Services Act 1994 genannte Zwecke notwendig und verhältnismäßig ist.[312] Wichtig ist, dass diese Anforderungen auch in Fällen gelten, in denen die Ausnahme zum Schutz der nationalen Sicherheit gemäß Paragraf 110 DPA 2018 geltend gemacht wird, da in Paragraf 110 DPA 2018 der Paragraf 109 DPA 2018 nicht als eine der Bestimmungen aufgeführt ist, die unangewendet bleiben können, wenn zum Schutz der nationalen Sicherheit eine Ausnahme von bestimmten Bestimmungen erforderlich ist.

3.3.1.1.2 Gezielte Beschaffung und Speicherung von Kommunikationsdaten

(197) Gemäß dem IPA 2016 darf der Secretary of State Telekommunikationsbetreiber auffordern, Kommunikationsdaten zu speichern, damit bestimmte Behörden, einschließlich Strafverfolgungsbehörden und Nachrichtendiensten, gezielt darauf zugreifen können. In Teil 4 des IPA 2016 ist die Speicherung von Kommunikationsdaten, in Teil 3 die gezielte Beschaffung von Kommunikationsdaten geregelt. Des Weiteren sind in den Teilen 3 und 4 des IPA 2016 spezifische Einschränkungen für die Nutzung dieser Befugnisse sowie spezifische Garantien vorgesehen.

(198) Der Begriff „Kommunikationsdaten“ („communications data“) bezieht sich auf das „Wer“, „Wann“, „Wo“ und „Wie“ eines Kommunikationsvorgangs, nicht aber auf den Inhalt, d. h. was gesagt oder geschrieben wurde. Anders als beim Abfangen besteht das Ziel der Beschaffung und Speicherung von Kommunikationsdaten nicht darin, den Inhalt der Kommunikation zu erfassen, sondern Informationen wie den Teilnehmer eines Telefondienstes oder einen Einzelverbindungsnachweis zu erhalten. Hierzu zählen beispielsweise der Zeitpunkt und die Dauer eines Kommunikationsvorgangs, die Telefonnummer oder E-Mail-Adresse des Urhebers und des Empfängers und mitunter auch der Standort der Geräte, von denen aus die Kommunikation erfolgte.[313]

---

311 Paragraf 54 IPA 2016. Garantien in Bezug auf die Weitergabe von Material an ausländische Behörden werden in den Verhaltenskodizes näher erläutert: siehe insbesondere Nr. 9.26 ff. und 9.87 des Code of Practice on the Interception of Communications sowie Nr. 9.33 ff. und 9.41 des Code of Practice on Equipment Interference (siehe Fußnote 278).

312 Dabei handelt es sich um folgende Zwecke: für den Security Service die Verhütung oder Aufdeckung schwerer Straftaten oder die Zwecke eines Strafverfahrens (Paragraf 2 Absatz 2 Buchstabe a des Security Service Act 1989), für den Intelligence Service die Interessen der nationalen Sicherheit, die Verhütung oder Aufdeckung schwerer Straftaten oder die Zwecke eines Strafverfahrens (Paragraf 2 Absatz 2 Buchstabe a des Intelligence Services Act 1994) und für die GCHQ die Zwecke eines Strafverfahren (Paragraf 4 Absatz 2 Buchstabe a des Intelligence Services Act 1994). Siehe auch Erläuterungen zum DPA 2018, abrufbar unter folgendem Link: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

313 Der Begriff „Kommunikationsdaten“ wird in Paragraf 261 Absatz 5 IPA 2016 definiert. Er umfasst sowohl „Ereignisdaten“ („events data“ – alle Daten, die ein Ereignis (mit oder ohne Verweis auf dessen Ort) in einem Telekommunikationssystem oder auf der Grundlage eines Telekommunikationssystems identifizieren oder beschreiben, wobei das Ereignis darin besteht, dass eine oder mehrere Entitäten eine bestimmte Tätigkeit zu einem bestimmten Zeitpunkt durchführen) als auch „Entitätsdaten“ („entity data“ – alle Daten, die a) sich beziehen auf: i) eine Entität, ii) eine Verbindung zwischen einem Telekommunikationsdienst und einer Entität oder iii) eine Verbindung zwischen einem beliebigen Teil

www.parlament.gv.at

(199) Es ist zu beachten, dass sich die Speicherung und Beschaffung von Kommunikationsdaten in der Regel nicht auf personenbezogene Daten von betroffenen Personen in der EU bezieht, die gemäß diesem Beschluss in das Vereinigte Königreich übermittelt werden. Die Verpflichtung zur Speicherung oder Offenlegung von Kommunikationsdaten gemäß den Teilen 3 und 4 des IPA 2016 bezieht sich auf Daten, die von Telekommunikationsbetreibern im Vereinigten Königreich direkt von den Nutzern eines Telekommunikationsdienstes erhoben werden.[314] Diese Art der „kundenseitigen" Verarbeitung umfasst typischerweise keine Übermittlung auf der Grundlage dieses Beschlusses, d. h. eine Übermittlung von einem Verantwortlichen/Auftragsverarbeiter in der EU an einen Verantwortlichen/Auftragsverarbeiter im Vereinigten Königreich.

(200) Der Vollständigkeit halber werden jedoch in den folgenden Erwägungsgründen die für diese Beschaffungs- und Speicherregelungen geltenden Bedingungen und Garantien analysiert.

(201) Als Prämisse ist festzuhalten, dass sowohl nationale Sicherheitsbehörden[315] als auch bestimmte Strafverfolgungsbehörden auf die Speicherung und die gezielte Beschaffung von Kommunikationsdaten zurückgreifen können. Für die Beantragung der Speicherung bzw. Beschaffung von Kommunikationsdaten gelten unterschiedliche Bedingungen, abhängig von der Begründung des Antrags, d. h. ob Gründe der nationalen Sicherheit oder Strafverfolgungszwecke angegeben werden.

(202) So wurde zwar mit der neuen Regelung das allgemeine Erfordernis einer Vorabgenehmigung durch eine unabhängige Stelle eingeführt, die in allen Fällen gelten wird, in denen Kommunikationsdaten gespeichert und/oder beschafft werden (entweder zu Strafverfolgungszwecken oder zu Zwecken der nationalen Sicherheit),

---

eines Telekommunikationssystems und einer Entität, b) aus Daten bestehen oder Daten beinhalten, die die Entität (mit oder ohne Verweis auf den Standort der Entität) identifizieren oder beschreiben, und c) keine Ereignisdaten sind).

314 Dies ergibt sich aus der Definition von Kommunikationsdaten in Paragraf 261 Absatz 5 IPA 2016, wonach Kommunikationsdaten sich im Besitz eines Telekommunikationsbetreibers befinden oder von diesem erlangt werden und sich entweder auf den Nutzer eines Telekommunikationsdienstes und die Bereitstellung dieses Dienstes beziehen oder in einem Kommunikationsvorgang enthalten, Teil eines Kommunikationsvorgangs oder mit einem Kommunikationsvorgang verknüpft oder logisch mit ihm verbunden sind (siehe auch Code of Practice on Communications Data, abrufbar unter folgendem Link https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, Nummern 2.22 bis 2.33). Darüber hinaus muss es sich bei einem Telekommunikationsbetreiber im Sinne der Definition nach Paragraf 261 Absatz 10 IPA 2016 um eine Person handeln, die einen Telekommunikationsdienst für Personen im Vereinigten Königreich anbietet oder erbringt oder die ein Telekommunikationssystem kontrolliert oder bereitstellt, das sich (ganz oder teilweise) im Vereinigten Königreich befindet oder vom Vereinigten Königreich aus kontrolliert wird. Diese Definitionen machen deutlich, dass Telekommunikationsbetreibern, deren Systeme sich nicht im Vereinigten Königreich befinden oder von dort aus kontrolliert werden und die keine Dienste für Personen im Vereinigten Königreich anbieten oder erbringen, keine Verpflichtungen gemäß dem IPA 2016 auferlegt werden dürfen (siehe auch Code of Practice on Communications Data, Nummer 2.1). Wenn Teilnehmer aus der EU (unabhängig davon, ob sie in der EU oder im Vereinigten Königreich ansässig sind) Dienste im Vereinigten Königreich in Anspruch nehmen, werden sämtliche Kommunikationsdaten im Zusammenhang mit der Erbringung dieses Dienstes direkt vom Diensteanbieter im Vereinigten Königreich erfasst und nicht von der EU aus übermittelt.

315 Die Behörden sind in Anhang 4 des IPA 2016 aufgeführt und umfassen die Polizeikräfte, Nachrichtendienste, einige Ministerien und Regierungsbehörden, die National Crime Agency, Her Majesty's Revenue and Customs, die Competition and Markets Authority, den Information Commissioner, Notarzt-, Feuerwehr- und Rettungsdienste sowie weitere Behörden etwa im Bereich Gesundheit und Lebensmittelsicherheit.

www.parlament.gv.at

doch wurden im Anschluss an das Urteil Tele2/Watson des Europäischen Gerichtshofs[316] für zu Strafverfolgungszwecken beantragte Maßnahmen spezifische Garantien eingeführt. Insbesondere wenn die Speicherung oder die Beschaffung von Kommunikationsdaten zu Strafverfolgungszwecken beantragt wird, muss die Vorabgenehmigung stets vom Investigatory Power Commissioner erteilt werden. Wird die Maßnahme aus Gründen der nationalen Sicherheit beantragt, ist dies nicht immer der Fall, da für diese Art von Maßnahmen, wie nachstehend beschrieben, in bestimmten Fällen die Genehmigung von einer anderen „genehmigenden Person" erteilt werden kann. Darüber hinaus wurde mit der neuen Regelung die Schwelle für die Zulässigkeit der Speicherung und Beschaffung von Kommunikationsdaten auf „schwere Straftaten" angehoben[317].

i) Genehmigung zur Erlangung von Kommunikationsdaten

(203) Gemäß Teil 3 des IPA 2016 sind einschlägige Behörden berechtigt, Kommunikationsdaten von einem Telekommunikationsbetreiber oder einer Person, die in der Lage ist, solche Daten zu erhalten und weiterzugeben, zu erhalten. Die Genehmigung darf nicht die Befugnis zum Abfangen des Inhalts der Kommunikationsvorgänge erteilen[318] und tritt nach einem Monat außer Kraft[319], wobei vorbehaltlich einer zusätzlichen Genehmigung die Möglichkeit einer Verlängerung besteht[320]. Für die Beschaffung von Kommunikationsdaten ist eine Genehmigung des Investigatory Powers Commissioner (IPC)[321] (zum Status und zu den Befugnissen des IPC siehe Erwägungsgründe 250 bis 251) erforderlich. Dies ist immer dann der Fall, wenn die Beschaffung von Kommunikationsdaten von einer einschlägigen Strafverfolgungsbehörde beantragt wird. Nach Paragraf 61 IPA 2016 kann bei der Beschaffung von Daten im Interesse der nationalen Sicherheit oder im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs, sofern es für die nationale Sicherheit relevant ist, oder bei einer Antragstellung durch ein Mitglied eines Nachrichtendienstes nach Paragraf 61 Absatz 7 Buchstabe b[322] die Beschaffung der Daten alternativ[323] auch vom IPC oder von einem benannten hohen Beamten[324]

316 Verbundene Rechtssachen C-203/15 und C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).

317 Siehe Paragraf 61 Absatz 7 Buchstabe b für die Beschaffung von Kommunikationsdaten und Paragraf 87 Absatz 10A für die Speicherung von Kommunikationsdaten.

318 Paragraf 60A Absatz 6 IPA 2016.

319 Dieser Zeitraum verkürzt sich auf drei Tage, wenn die Genehmigung aus Gründen der Dringlichkeit erteilt wird (Paragraf 65 Absatz 3 Buchstabe A IPA 2016).

320 Gemäß Paragraf 65 des IPA 2016 gilt die verlängerte Genehmigung für einen Zeitraum von einem Monat ab dem Datum, an dem die aktuelle Genehmigung abläuft. Die Person, die die Genehmigung erteilt hat, kann die Genehmigung jederzeit widerrufen, wenn sie der Ansicht ist, dass die Anforderungen nicht mehr erfüllt sind.

321 Paragraf 60A Absatz 1 IPA 2016. Das Office for Communications Data Authorisations (OCDA) nimmt diese Funktion im Auftrag des IPC wahr (siehe Communication Data Codes of Practice, Paragraf 5 Absatz 6).

322 Ein Antrag gemäß Paragraf 61 Absatz 7 Buchstabe b IPA 2016 wird für „einen maßgeblichen Zweck in Bezug auf Straftaten" („applicable crime purpose") gestellt; gemäß Paragraf 61 Absatz 7 Buchstabe A IPA 2016 sind dies folgende Zwecke: „wenn es sich bei den Kommunikationsdaten ganz oder teilweise um Ereignisdaten handelt, der Zweck der Verhütung oder Aufdeckung schwerer Straftaten; in allen anderen Fällen der Zweck der Verhütung oder Aufdeckung von Straftaten oder der Aufrechterhaltung der Ordnung".

323 Im Verhaltenskodex zu Kommunikationsdaten (Code of Practice on Communication Data) heißt es hierzu: „Wenn ein Antrag mit Bezug zur nationalen Sicherheit entweder nach Paragraf 60A oder Paragraf 61 gestellt werden könnte, obliegt die Entscheidung, welches Genehmigungsverfahren im

www.parlament.gv.at

genehmigt werden. Der benannte Beamte muss von der betreffenden Ermittlung oder Operation unabhängig sein und über einschlägige Kenntnisse der Grundsätze und Rechtsvorschriften im Bereich der Menschenrechte, insbesondere der Grundsätze der Notwendigkeit und Verhältnismäßigkeit, verfügen[325]. Die von dem benannten Beamten getroffene Entscheidung unterliegt einer Ex-post-Aufsicht durch den IPC (siehe Erwägungsgrund 254 für weitere Einzelheiten zu den Ex-post-Aufsichtsfunktionen des IPC).

(204) Die Genehmigung zur Beschaffung von Kommunikationsdaten beruht auf einer Bewertung der Notwendigkeit und Verhältnismäßigkeit der Maßnahme. Konkret bedeutet dies, dass die Notwendigkeit der Maßnahme im Hinblick auf die in der Gesetzgebung aufgeführten Gründe bewertet wird.[326] In Anbetracht des zielgerichteten Charakters dieser Maßnahme besteht zudem das Erfordernis, dass sie für eine bestimmte Untersuchung oder Operation notwendig ist.[327] Weitere Anforderungen bezüglich der Bewertung der Notwendigkeit der Maßnahmen sind im Code of Practice on Communication Data dargelegt[328]. Demnach muss der von der ersuchenden Behörde eingereichte Antrag drei Mindestelemente aufweisen, mit denen die Notwendigkeit eines solchen Ersuchens begründet wird: i) das zu untersuchende Ereignis, z. B. eine Straftat oder der Aufenthaltsort einer gefährdeten vermissten Person, ii) die Person, deren Daten beschafft werden sollen, z. B. ein Verdächtiger, ein Zeuge oder eine vermisste Person, und Angaben dazu, wie diese Person mit dem Ereignis in Verbindung steht, und iii) die Kommunikationsdaten, die beschafft werden sollen, z. B. eine Telefonnummer oder IP-Adresse, und Angaben dazu, wie diese Daten mit der Person und dem Ereignis in Verbindung stehen[329].

(205) Darüber hinaus muss die Beschaffung von Kommunikationsdaten im Hinblick auf das angestrebte Ziel verhältnismäßig sein[330]. Laut dem Verhaltenskodex zu Kommunikationsdaten (Code of Practice on Communication Data) sollte die

---

jeweiligen Fall am geeignetsten ist, den jeweiligen Behörden. Behörden, die das Verfahren der Genehmigung durch einen benannten hohen Beamten anwenden wollen, sollten klare Leitlinien dazu haben, wann dieses Verfahren geeignet ist“ (Code of Practice on Communications Data, Nummer 5. 19, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

324 Paragraf 70 Absatz 3 IPA 2016 enthält eine Definition des Begriffs „benannter Beamter“ („designated officer“); diese ist je nach Behörde unterschiedlich (wie in Anhang 4 des IPA 2016 dargelegt).

325 Weitere Einzelheiten zur Unabhängigkeit des benannten hohen Beamten sind dem Verhaltenskodex zu Kommunikationsdaten (Code of Practice on Communications Data, Paragrafen 4 Absätze 12 bis 17 zu entnehmen, siehe Fußnote323).

326 Dabei handelt es sich um folgende Gründe: i) im Interesse der nationalen Sicherheit, ii) zur Verhütung oder Aufdeckung von Straftaten oder Aufrechterhaltung der Ordnung (im Falle von „Ereignisdaten“ gilt dies nur für schwere Straftaten), iii) im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs, sofern diese Interessen auch für die Interessen der nationalen Sicherheit relevant sind, iv) im Interesse der öffentlichen Sicherheit, v) zur Verhinderung von Tod oder Verletzung oder einer Schädigung der körperlichen oder geistigen Gesundheit einer Person oder zur Linderung einer Verletzung oder Schädigung der körperlichen oder geistigen Gesundheit einer Person, vi) zur Unterstützung der Ermittlungen bei angeblichen Justizirrtümern oder vii) zur Identifizierung eines Toten oder einer Person, die sich aufgrund eines bestimmten Zustands nicht selbst identifizieren kann (Paragraf 61 Absatz 7 IPA 2016).

327 Paragraf 60A Absatz 1 Buchstabe b IPA 2016.

328 Code of Practice on Communications Data, Nummer 3.3ff., siehe Fußnote 323.

329 Code of Practice on Communications Data, Nummer 3.13, siehe Fußnote 323.

330 Paragraf 60 Absatz 1 Buchstabe c IPA 2016.

www.parlament.gv.at

genehmigende Person bei der Durchführung einer solchen Bewertung eine Abwägung zwischen „dem Ausmaß des Eingriffs in die Rechte und Freiheiten einer Person und einem spezifischen Nutzen für die von einer zuständigen Behörde im öffentlichen Interesse durchgeführte Untersuchung oder Maßnahme“ treffen; ferner könnte unter Berücksichtigung aller Erwägungen eines bestimmten Falls „ein Eingriff in die Rechte einer Person dennoch nicht gerechtfertigt sein, weil die nachteiligen Auswirkungen auf die Rechte einer anderen Person oder Personengruppe zu schwerwiegend sind“. Für die konkrete Bewertung der Verhältnismäßigkeit einer Maßnahme ist im Kodex zudem eine Reihe von Elementen aufgeführt, die in dem Antrag der ersuchenden Behörde enthalten sein sollten[331]. Darüber hinaus ist besonders die Art der zu beschaffenden Kommunikationsdaten („Entitätsdaten“ oder „Ereignisdaten“[332]) zu berücksichtigen, wobei bevorzugt Datenkategorien zu verwenden sind, die mit einem geringeren Eingriff verbunden sind[333]. Des Weiteren enthält der Verhaltenskodex zu Kommunikationsdaten (Code of Practice on Communication Data) spezielle Anweisungen für Genehmigungen, die die Kommunikationsdaten von Personen in bestimmten Berufen (wie Ärzten, Anwälten, Journalisten, Parlamentsmitgliedern oder Geistlichen)[334] betreffen; für diese Art von Daten gelten zusätzliche Garantien[335].

ii) Anordnung zur Speicherung von Kommunikationsdaten

(206) Teil 4 des IPA 2016 enthält Vorschriften für die Speicherung von Kommunikationsdaten, insbesondere die Kriterien, die es dem Secretary of State erlauben, eine Speicherungsanordnung („retention notice“) zu erteilen.[336] Die durch den IPA eingeführten Garantien sind dieselben, wenn die Daten entweder zu Strafverfolgungszwecken oder im Interesse der nationalen Sicherheit gespeichert werden.

---

331 Folgende Informationen müssen enthalten sein: i) eine Beschreibung dessen, welchen Nutzen die Beschaffung der Daten für die Untersuchung oder den Einsatz haben wird, ii) eine Erläuterung der Relevanz der beantragten Zeiträume, einschließlich Angaben dazu, inwieweit diese Zeiträume in einem angemessenen Verhältnis zu dem untersuchten Ereignis stehen, iii) eine Erläuterung dessen, inwieweit der Umfang des Eingriffs unter Berücksichtigung des Nutzens der Daten für die Untersuchung gerechtfertigt ist (hierbei sollte erwogen werden, ob weniger stark eingreifende Untersuchungen durchgeführt werden könnten, um das Ziel zu erreichen), iv) eine Betrachtung der Rechte (insbesondere des Rechts auf Privatsphäre und, in relevanten Fällen, des Rechts auf freie Meinungsäußerung) des Einzelnen und eine Abwägung dieser Rechte gegen den Nutzen der Untersuchung, v) Einzelheiten dazu, zu welchen weiteren („kollateralen“) Eingriffen es kommen könnte und wie sich die beantragten Zeiträume auf diese kollateralen Eingriffe auswirken (Code of Practice on Communications Data, Nummern 3.22 bis 3.26, siehe Fußnote 323).

332 Siehe Fußnote 313.

333 Sollen Kommunikationsdaten beschafft werden, die mit einem stärkeren Eingriff verbunden sind (d. h. Ereignisdaten), ist es gemäß dem Kodex angemessener, zunächst Entitätsdaten zu beschaffen oder in einigen wenigen besonders dringenden Fällen direkt Ereignisdaten zu beschaffen (Code of Practice on Communications Data, Nummern 6.10 bis 6.14, siehe Fußnote 323).

334 Code of Practice on Communications Data, Nummern 8.8 bis 8.44, siehe Fußnote 323.

335 Laut dem Verhaltenskodex „muss eine genehmigende Person bei der Prüfung solcher Anträge besondere Sorgfalt walten lassen. Unter anderem muss zusätzlich geprüft werden, ob derartige Anträge unbeabsichtigte Folgen haben könnten und ob der betreffende Antrag dem öffentlichen Interesse am besten dient“ (Code of Practice on Communications Data, Nummer 8.8). Darüber hinaus müssen Aufzeichnungen für diese Art von Anträgen geführt werden. Zudem sollten die Anträge bei der nächsten Kontrolle zur besonderen Beachtung durch den IPC gekennzeichnet werden (Code of Practice on Communications Data, Nummer 8.10, siehe Fußnote 323).

336 Paragrafen 87 bis 89 IPA 2016.

www.parlament.gv.at

(207) Mit dem Erlass einer solchen Speicherungsanordnung soll sichergestellt werden, dass Telekommunikationsbetreiber relevante Kommunikationsdaten, die ansonsten gelöscht würden, sobald sie nicht mehr für geschäftliche Zwecke benötigt werden, für einen Zeitraum von maximal 12 Monaten speichern.[337] Die gespeicherten Daten müssen so lange zur Verfügung stehen, wie es für den Fall erforderlich wäre, dass eine Behörde sie nachträglich im Rahmen einer in Teil 3 des IPA 2016 vorgesehenen und in den Erwägungsgründen 203 bis 205 beschriebenen Genehmigung für eine gezielte Beschaffung von Kommunikationsdaten beschaffen muss.

(208) Die Ausübung dieser Befugnis, die Speicherung bestimmter Daten zu anzuordnen, unterliegt einer Reihe von Beschränkungen und Garantien. So kann der Secretary of State nur dann einem oder mehreren Betreibern[338] eine Speicherungsanordnung erteilen, wenn er der Meinung ist, dass die Speicherung aus einem der gesetzlichen Zwecke erforderlich ist[339] und im Hinblick auf das angestrebte Ziel verhältnismäßig ist[340]. Daher muss der Secretary of State, wie im IPA 2016 selbst festgelegt ist[341], vor der Erteilung einer Speicherungsanordnung Folgendes berücksichtigen: den voraussichtlichen Nutzen der Anordnung[342]; eine Beschreibung der Telekommunikationsdienste; die Frage, ob es angemessen ist, mit Verweis auf den Ort zu speichernde Daten oder Beschreibungen von Personen, für die Telekommunikationsdienste erbracht werden, zu begrenzen[343]; die voraussichtliche Anzahl der Nutzer (sofern bekannt) aller Telekommunikationsdienste, auf die sich die

---

337 Gemäß Paragraf 90 IPA 2016 kann ein Telekommunikationsbetreiber, der eine Speicherungsanordnung erhalten hat, beim Secretary of State, der sie erteilt hat, eine Überprüfung beantragen.

338 Nach Paragraf 87 Absatz 2 Buchstabe a IPA 2016 kann sich eine Speicherungsanordnung auf „einen bestimmten Betreiber oder eine Beschreibung von Betreibern" beziehen.

339 Die Speicherung muss aus einem der folgenden Zwecke erforderlich sein: i) im Interesse der nationalen Sicherheit, ii) für einen maßgeblichen Zweck in Bezug auf Straftaten (im Sinne der Definition in Paragraf 87 Absatz 10A IPA 2016), iii) im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs, sofern diese Interessen auch für die Interessen der nationalen Sicherheit relevant sind, iv) im Interesse der öffentlichen Sicherheit, v) zur Verhinderung von Tod oder Verletzung oder einer Schädigung der körperlichen oder geistigen Gesundheit einer Person oder zur Linderung einer Verletzung oder Schädigung der körperlichen oder geistigen Gesundheit einer Person, oder vi) zur Unterstützung der Ermittlungen bei angeblichen Justizirrtümern (Paragraf 87 IPA).

340 Paragraf 87 IPA 2016. Darüber hinaus gelten nach dem einschlägigen Verhaltenskodex für die Beurteilung der Verhältnismäßigkeit der Speicherungsanordnung die in Paragraf 2 Absatz 2 IPA 2016 festgelegten Kriterien; insbesondere ist zu bewerten, ob das mit der Anordnung angestrebte Ziel nach vernünftigem Ermessen auch mit anderen, weniger stark eingreifenden Mitteln erreicht werden könnte. Ähnlich wie bei der Beurteilung der Verhältnismäßigkeit bei der Beschaffung von Kommunikationsdaten wird im Verhaltenskodex zu Kommunikationsdaten klargestellt, dass bei einer solchen Beurteilung „eine Abwägung zwischen dem Ausmaß des Eingriffs in das Recht einer Person auf Achtung ihres Privatlebens und dem konkreten Nutzen für die Untersuchung zu treffen ist" (Code of Practice on Communications Data, Nummer 16.3, siehe Fußnote 323).

341 Siehe Paragraf 88 IPA 2016.

342 Dieser Nutzen kann bereits gegeben oder geplant sein und muss sich auf die gesetzlichen Zwecke beziehen, für die die Daten gespeichert werden dürfen (Code of Practice on Communications Data, Nummer 17.17, siehe Fußnote 323).

343 Im Rahmen dieser Erwägungen wird unter anderem bestimmt, ob der gesamte geografische Anwendungsbereich der Speicherungsanordnung notwendig und verhältnismäßig ist und ob es notwendig und verhältnismäßig ist, bestimmte Beschreibungen von Personen aufzunehmen oder auszuschließen (Code of Practice on Communications Data, Nummer 17.17, siehe Fußnote 323).

www.parlament.gv.at

Anordnung bezieht[344]; die technische Durchführbarkeit der Erfüllung der Anordnung; die voraussichtlichen Kosten der Erfüllung der Anordnung und alle sonstigen Auswirkungen der Anordnung auf den Telekommunikationsbetreiber (oder Beschreibung der Betreiber), auf den sie sich bezieht[345]. Wie in Kapitel 17 des Verhaltenskodex zu Kommunikationsdaten weiter ausgeführt, ist in jeder Speicherungsanordnung anzugeben, welche Art von Daten zu speichern ist und inwieweit diese Art von Daten die für die Speicherung erforderlichen Voraussetzungen erfüllt.

(209) In allen Fällen (sowohl aus Gründen der nationalen Sicherheit als auch für Strafverfolgungszwecke) muss die Entscheidung des Secretary of State, eine Speicherungsanordnung auszustellen, von einem unabhängigen Judicial Commissioner im Rahmen des sogenannten „Double-Lock-Verfahrens“ genehmigt werden, der insbesondere prüfen muss, ob die Anordnung zur Speicherung der relevanten Kommunikationsdaten für einen oder mehrere gesetzliche Zwecke erforderlich und verhältnismäßig ist[346].

3.3.1.1.3 Zugriff auf Geräte

(210) Der Zugriff auf Geräte („equipment interference“) umfasst eine Reihe von Techniken, mit denen eine Vielzahl unterschiedlicher Daten von Geräten[347] erfasst wird, unter anderem von Computern, Tablets und Smartphones sowie Kabeln, Drähten und Speichergeräten.[348] Durch Gerätezugriff können sowohl Inhalte von Kommunikationsvorgängen als auch Gerätedaten[349] erfasst werden.

(211) Gemäß Paragraf 13 Absatz 1 IPA 2016 bedarf es für den Gerätezugriff durch einen Nachrichtendienst einer Genehmigung mittels einer Anordnung im Rahmen des durch den IPA 2016 eingeführten „Double-Lock“-Verfahrens, sofern eine „Verbindung zu den Britischen Inseln“ vorliegt.[350] Laut den Erläuterungen der britischen Behörden

---

344 Anhand dieser Angaben ist es für den Secretary of State leichter, sowohl das Ausmaß des Eingriffs in die Privatsphäre der Kunden als auch den voraussichtlichen Nutzen der zu speichernden Daten zu prüfen (Code of Practice on Communications Data, Nummer 17.17, siehe Fußnote 323).

345 Paragraf 88 IPA 2016.

346 Paragraf 89 IPA 2016.

347 Gemäß Paragraf 135 Absatz 1 und Paragraf 198 Absatz 1 IPA 2016 umfasst der Begriff „Geräte“ („equipment“) Geräte, die elektromagnetische, akustische oder sonstige Emissionen erzeugen, oder jegliche Vorrichtung, die in Verbindung mit solchen Geräten genutzt werden kann.

348 Code of Practice on Equipment Interference, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, Nummer 2.2.

349 Bei Gerätedaten handelt es sich laut Definition in Paragraf 100 des IPA 2016 um Systemdaten und Daten, die a) in einem Kommunikationsvorgang oder einem sonstigen Informationsgegenstand enthalten, Teil eines Kommunikationsvorgangs oder eines sonstigen Informationsgegenstands oder mit einem Kommunikationsvorgang oder einem sonstigen Informationsgegenstand verknüpft oder logisch mit ihm verbunden sind (durch den Sender oder auf andere Weise), b) logisch von dem restlichen Kommunikationsvorgang oder Informationsgegenstand getrennt werden können und c) wenn sie auf diese Weise getrennt werden, nichts von dem preisgeben , was nach vernünftigem Ermessen als der Inhalt (sofern vorhanden) des Kommunikationsvorgangs oder Informationsgegenstands angesehen werden könnte.

350 Damit das Erfordernis einer Anordnung zwingend ist, ist es nach Paragraf 13 Absatz 1 IPA 2016 zudem erforderlich, dass das Verhalten des Nachrichtendienstes einen oder mehrere Straftatbestände im Sinne der Paragrafen 1 bis 3A des Gesetzes über den Missbrauch von Computern von 1990 (Computer Misuse Act 1990) erfüllen würde, was in der überwiegenden Mehrheit der Fälle der Fall wäre (siehe Code of Practice on Equipment Interference, Nummern 3.32 und 3.6 bis 3.9). Gemäß Paragraf 13 Absatz 2

www.parlament.gv.at

würde in Situationen, in denen Daten im Rahmen dieses Beschlusses von der Europäischen Union an das Vereinigte Königreich übermittelt werden, immer eine „Verbindung zu den Britischen Inseln“ bestehen, sodass jeder Gerätezugriff, der sich auf derartige Daten bezieht, zwingend einer Anordnung gemäß Paragraf 13 Absatz 1 IPA 2016 unterliegen würde[351].

(212) Die Vorschriften für Anordnungen zum gezielten Gerätezugriff sind in Teil 5 des IPA 2016 festgelegt. Ähnlich wie beim gezielten Abfangen muss sich der gezielte Gerätezugriff auf ein bestimmtes „Ziel“ beziehen, das in der Anordnung genannt sein muss.[352] Die Einzelheiten dazu, wie ein „Ziel“ zu identifizieren ist, hängen vom jeweiligen Sachverhalt und der Art der zu überwachenden Geräte ab. In Paragraf 115 Absatz 3 IPA sind die Elemente aufgeführt, die in der Anordnung enthalten sein sollten (z. B. Name der Person oder Organisation, Beschreibung des Ortes); diese hängen beispielsweise davon ab, ob der Zugriff ein Gerät betrifft, das einer bestimmten Person oder einer Organisation oder einer Gruppe von Personen gehört, von ihnen benutzt wird oder sich in ihrem Besitz befindet, sich an einem bestimmten Ort befindet usw.[353] Die Zwecke, für die Anordnungen zum gezielten Gerätezugriff ausgestellt werden können, hängen davon ab, welche Behörde den Antrag stellt.[354]

IPA 2016 liegt eine „Verbindung zu den Britischen Inseln“ vor, wenn a) eine der Handlungen auf den Britischen Inseln stattfindet (unabhängig vom Standort des überwachten bzw. zu überwachenden Geräts), b) der Nachrichtendienst der Ansicht ist, dass sich eines der überwachten bzw. zu überwachenden Geräte zum Zeitpunkt des Zugriffs auf den Britischen Inseln befindet bzw. befinden könnte, oder c) ein Ziel des Zugriffs darin besteht, i) Kommunikationsdaten zu erhalten, die von einer Person oder an eine Person übermittelt werden, die sich einstweilen tatsächlich oder nach Annahme des Nachrichtendienstes auf den Britischen Inseln befindet, ii) private Informationen über eine Person zu erhalten, die sich einstweilen tatsächlich oder nach Annahme des Nachrichtendienstes auf den Britischen Inseln befindet, oder iii) Gerätedaten zu erhalten, die Teil von Kommunikationsvorgängen oder privaten Informationen sind, die unter die Ziffern i bzw. ii fallen, bzw. mit diesen Kommunikationsvorgängen oder privaten Informationen in Zusammenhang stehen.

351 Aus Gründen der Vollständigkeit sei darauf hingewiesen, dass ein Nachrichtendienst, der eine Tätigkeit plant, für die er eine Anordnung zum massenhaften Gerätezugriff erhalten kann, auch in Situationen, in denen keine „Verbindung zu den Britischen Inseln“ besteht und ein Gerätezugriff daher nicht zwingend einer Anordnung nach Paragraf 13 Absatz 1 IPA 2016 bedarf, grundsätzlich („as a matter of policy“) eine solche Anordnung einholen sollte (siehe Code of Practice on Equipment Interference, Nummer 3.24). Selbst wenn eine Anordnung zum Gerätezugriff gemäß dem IPA 2016 weder gesetzlich vorgeschrieben ist noch im Rahmen einer Grundsatzentscheidung eingeholt wird, unterliegen die Maßnahmen der Nachrichtendienste einer Reihe von Bedingungen und Beschränkungen nach Maßgabe von Paragraf 7 des Intelligence Services Act 1994. Hierzu zählt insbesondere das Erfordernis einer Genehmigung durch den Secretary of State, der davon überzeugt sein muss, dass eine Maßnahme nicht über das hinausgeht, was für die ordnungsgemäße Erfüllung der Aufgaben des Nachrichtendienstes erforderlich ist.

352 Paragraf 115 IPA 2016 regelt den Inhalt der Anordnung; demnach müssen der Namen oder eine Beschreibung der Personen, Organisationen, Orte oder Personengruppen, die das „Ziel“ darstellen, eine Beschreibung der Art der Untersuchung sowie eine Beschreibung der Aktivitäten, für die das betreffende Gerät verwendet wird, enthalten sein. Darüber hinaus sind die Art des Gerätes und die Handlungen zu beschreiben, die der Person, an die die Anordnung gerichtet ist, gestattet werden.

353 Siehe auch Code of Practice on Equipment Interference, Nummer 5.7, siehe Fußnote 348.

354 Nationale Sicherheitsbehörden können eine Anordnung zum Gerätezugriff beantragen, wenn dies für Zwecke der nationalen Sicherheit, zur Aufdeckung schwerer Straftaten und/oder im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs, sofern diese Interessen auch für die Interessen der nationalen Sicherheit relevant sind, erforderlich ist (Paragrafen 102 und 103 IPA 2016). Je nach Behörde kann eine Anordnung zum Gerätezugriff zu Strafverfolgungszwecken beantragt werden, wenn dies zur Aufdeckung oder Verhütung einer schweren Straftat oder zur Verhinderung von Tod oder Verletzung oder einer Schädigung der körperlichen oder geistigen Gesundheit einer Person oder zur

www.parlament.gv.at

(213) Ähnlich wie beim gezielten Abfangen muss die anordnende Behörde prüfen, ob die Maßnahme zur Erreichung eines bestimmten Ziels erforderlich und im Hinblick auf das angestrebte Ziel verhältnismäßig ist.[355] Darüber hinaus sollte sie prüfen, ob Garantien in Bezug auf Sicherheit, Aufbewahrung und Offenlegung sowie in Bezug auf die „Offenlegung gegenüber dem Ausland“ bestehen (siehe Erwägungsgrund 196).[356]

(214) Die Anordnung muss von einem Judicial Commissioner genehmigt werden, ausgenommen in dringenden Fällen.[357] In dringenden Fällen muss ein Judicial Commissioner über die Ausstellung einer Anordnung unterrichtet werden, und er muss diese innerhalb von drei Arbeitstagen genehmigen. Verweigert der Judicial Commissioner die Genehmigung, tritt die Anordnung außer Kraft und kann nicht erneuert werden.[358] Darüber hinaus ist der Judicial Commissioner befugt, die Löschung der im Rahmen der Anordnung erlangten Daten zu verlangen[359]. Die Dringlichkeit der Ausstellung einer Anordnung beeinflusst nicht die Ex-post-Aufsicht (siehe Erwägungsgründe 244 bis 255) oder die Möglichkeit, dass Einzelpersonen Rechtsbehelfe einlegen (siehe Erwägungsgründe 260 bis 270). Einzelpersonen können beim ICO eine Beschwerde einlegen oder beim Investigatory Powers Tribunal in der üblichen Weise Ansprüche in Bezug auf mutmaßliche Handlungen geltend machen. Um über die Genehmigung einer Anordnung zu entscheiden, führt der Judicial Commissioner in allen Fällen eine Prüfung der Notwendigkeit und Verhältnismäßigkeit durch, wie sie auch für Anträge auf gezieltes Abfangen gilt (siehe Erwägungsgrund 192 oben)[360].

(215) Schließlich finden bestimmte für das gezielte Abfangen geltende Garantien auch auf Gerätezugriffe Anwendung, beispielsweise Garantien in Bezug auf die Dauer, Verlängerung und Änderung der Anordnung sowie für das Überwachen von Mitgliedern des Parlaments und das Abfangen von einem Rechtsprivileg unterliegenden Kommunikationsinhalten sowie von journalistischem Material (für weitere Einzelheiten siehe Erwägungsgrund 193).

3.3.1.1.4 Ausübung von Massenbefugnissen

(216) Die Ausübung von Massenbefugnissen („bulk powers“) ist in Teil 6 des IPA 2016 geregelt. Weitere Einzelheiten enthalten auch die einschlägigen Verhaltenskodizes.

Linderung einer Verletzung oder Schädigung der körperlichen oder geistigen Gesundheit einer Person erforderlich ist (siehe Paragraf 106 Absätze 1 und 3 IPA 2016).

355 Paragraf 102 Absatz 1 IPA 2016.

356 Paragrafen 129 bis 131 IPA 2016.

357 Paragraf 109 IPA 2016.

358 Paragraf 109 Absatz 4 IPA 2016.

359 Paragraf 110 Absatz 3 Buchstabe b IPA 2016. Nach dem Code of Practice on Equipment Interference Paragraf 5 Absatz 67 bestimmt sich die Dringlichkeit dadurch, ob es nach vernünftigem Ermessen praktikabel ist, in der mit Blick auf das operative oder investigative Erfordernis verfügbaren Zeit den Judicial Commissioner zu ersuchen, die Ausstellung einer Anordnung zu genehmigen. Dringende Anordnungen fallen in eine oder beide der folgenden Kategorien: i) es besteht eine unmittelbare Gefahr für Leben oder ernsthaften Schaden – z. B. wenn eine Person entführt wurde und davon ausgegangen wird, dass ihr Leben in unmittelbarer Gefahr ist; oder ii) es wurden Erkenntnisse gewonnen oder bei Ermittlungen hat sich eine Chance ergeben, wobei nur wenig Zeit zum Handeln bleibt – wenn beispielsweise die Verbringung einer Sendung harter Drogen in das Vereinigte Königreich kurz bevorsteht und die Strafverfolgungsbehörden die Personen, die eine schwere Straftat begehen, verfolgen und verhaften wollen. Siehe Fußnote 348.

360 Paragraf 108 IPA 2016.

www.parlament.gv.at

Zwar enthält das britische Recht keine Definition des Begriffs der „Massenbefugnis“, dennoch wird er im Zusammenhang mit dem IPA 2016 umschrieben als die Sammlung und Speicherung großer Datenmengen, welche die Regierung auf verschiedene Weise (d. h. im Rahmen der Befugnisse zum massenhaften Abfangen, zur massenhaften Beschaffung, zum massenhaften Gerätezugriff und für personenbezogene Massendatensätze) beschafft hat und auf die die Behörden anschließend zugreifen können. Diese Beschreibung wird deutlicher, wenn man sich vor Augen führt, was eine „Massenbefugnis“ nicht ist: nämlich die sogenannte „Massenüberwachung“ („mass surveillance“) ohne Beschränkungen oder Garantien. Im Gegenteil: Für Massenbefugnisse gelten, wie nachstehend erläutert, sehr wohl Beschränkungen und Garantien, durch die sichergestellt werden soll, dass der Zugang zu Daten nicht auf wahllose oder ungerechtfertigte Weise gewährt wird.[361] So können Massenbefugnisse nur dann genutzt werden, wenn ein Zusammenhang zwischen der technischen Maßnahme, die ein nationaler Nachrichtendienst einzusetzen beabsichtigt, und dem operativen Ziel, für das die betreffende Maßnahme beantragt wird, besteht.

(217) Darüber hinaus stehen Massenbefugnisse nur Nachrichtendiensten zur Verfügung und erfordern stets eine Anordnung, die vom Secretary of State ausgestellt und von einem Judicial Commissioner genehmigt werden muss. Bei der Wahl der Mittel zur Sammlung nachrichtendienstlicher Erkenntnisse gilt es zu berücksichtigen, ob das betreffende Ziel mit „weniger stark eingreifenden Mitteln“ („less intrusive means“) erreicht werden kann.[362] Dieser Ansatz leitet sich aus dem rechtlichen Rahmen ab, der auf dem Grundsatz der Verhältnismäßigkeit aufbaut und daher der gezielten Erfassung gegenüber der massenhaften Erfassung den Vorzug gibt.

3.3.1.1.4.1 Massenhaftes Abfangen und massenhafter Gerätezugriff

(218) Das massenhafte Abfangen ist in Teil 6 Kapitel 1 des IPA 2016 geregelt, der massenhafte Gerätezugriff in Teil 6 Kapitel 3. Die Regelungen sind im Wesentlichen gleich; die für diese Anordnungen geltenden Bedingungen und zusätzlichen Garantien werden daher gemeinsam analysiert.

i) Bedingungen und Kriterien für die Ausstellung einer Anordnung

(219) Eine Anordnung zum massenhaften Abfangen beschränkt sich auf das Abfangen von Kommunikationsvorgängen während ihrer Übertragung, die von Personen gesendet oder empfangen werden, die sich außerhalb der Britischen Inseln[363] befinden

---

361 Laut dem Bericht über Massenbefugnisse, den Lord David Anderson, der unabhängige Prüfer der Antiterror-Rechtsvorschriften, im Vorfeld der Annahme des IPA 2016 vorgelegt hat, „*sollte klar sein, dass die Sammlung und Speicherung von Daten in großen Mengen nicht mit einer sogenannten ‚Massenüberwachung‘ gleichzusetzen ist. Jedes Rechtssystem, das diesen Namen verdient, enthält Beschränkungen und Garantien, die genau dazu gedacht sind, sicherzustellen, dass der Zugang zu Speichern sensibler Daten (...) nicht auf wahllose oder ungerechtfertigte Weise gewährt wird. Derartige Beschränkungen und Garantien sind in dem Gesetzesentwurf zweifelsohne enthalten.*“ Lord David Anderson, Report of the Bulk Power Review, August 2016, Nummer 1.9 (Unterstreichung hinzugefügt), abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

362 Paragraf 2 Absatz 2 IPA 2016. Siehe zum Beispiel den Code of Practice on Bulk Acquisition of Communications Data, Nummer 4.11, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

363 Die „Britischen Inseln“ umfassen das Vereinigte Königreich, die Kanalinseln und die Isle of Man und sind in Anhang 1 des Gesetzes zur Auslegung von gesetzlichen Bestimmungen von 1978 (Interpretation

www.parlament.gv.at

(sogenannte auslandsbezogene Kommunikationsvorgänge („overseas-related communications“))[364], sowie auf andere relevante Daten und die anschließende Auswahl des abgefangenen Materials zur Überprüfung.[365] Durch eine Anordnung zum massenhaften Gerätezugriff[366] erhält der Adressat die Befugnis zum Zugriff auf jegliche Geräte zum Zwecke der Beschaffung von auslandsbezogenen Kommunikationsvorgängen (einschließlich aller Arten von Sprache, Musik, Tönen, visuellen Bildern oder Daten), Gerätedaten (Daten, die das Funktionieren eines Postdienstes, eines Telekommunikationssystems oder eines Telekommunikationsdienstes ermöglichen oder erleichtern) oder sonstigen Informationen.[367]

(220) Der Secretary of State kann eine Massenanordnung ausschließlich auf Antrag eines Leiters eines Nachrichtendienstes ausstellen.[368] Eine Anordnung zum massenhaften Abfangen oder massenhaften Gerätezugriff darf nur dann erteilt werden, wenn dies im Interesse der nationalen Sicherheit und für einen weiteren Zweck der Verhütung oder Aufdeckung schwerer Straftaten oder im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs erforderlich ist, sofern dies für die nationale Sicherheit relevant ist.[369] Des Weiteren muss eine Anordnung zum massenhaften Abfangen gemäß Paragraf 142 Absatz 7 IPA 2016 präzisere Angaben enthalten als den bloßen Verweis auf die „Interessen der nationalen Sicherheit“, das „wirtschaftliche Wohl des

---

Act 1978) definiert, der unter folgendem Link abrufbar ist: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

364 Gemäß Paragraf 136 IPA 2016 bezeichnet der Begriff „auslandsbezogene Kommunikationsvorgänge“ („overseas-related communications“): i) Kommunikationsvorgänge, die von Einzelpersonen, die sich außerhalb der Britischen Inseln befinden, gesendet werden, oder ii) Kommunikationsvorgänge, die von Einzelpersonen, die sich außerhalb der Britischen Inseln befinden, empfangen werden. Wie von den britischen Behörden bestätigt wurde, gilt diese Regelung auch für Kommunikationsvorgänge zwischen zwei Personen, die sich beide außerhalb der Britischen Inseln befinden. Die Große Kammer des Europäischen Gerichtshofs für Menschenrechte hat in der Rechtssache Big Brother Watch u. a. gegen das Vereinigte Königreich (siehe oben, Fn. 279), Randnr. 376, mit Blick auf eine ähnliche Beschränkung der Kommunikation (in Bezug auf „externe Kommunikation“), die im Rahmen des RIPA 2000 als massenhaftes Abfangen erfasst werden kann, festgestellt, dass sie hinreichend abgegrenzt und vorhersehbar war.

365 Paragraf 136 Absatz 4 IPA 2016. Laut den Erläuterungen der britischen Regierung kann das massenhafte Abfangen beispielsweise dazu dienen, bisher unbekannte Bedrohungen für die nationale Sicherheit des Vereinigten Königreichs zu ermitteln, indem abgefangenes Material gefiltert und analysiert wird, um nachrichtendienstlich wertvolle Kommunikationsvorgänge zu identifizieren (Explanatory Framework, Section H: National security, S. 27 und 28, siehe Fußnote 29). Wie von den britischen Behörden erläutert, können solche Instrumente eingesetzt werden, um Verbindungen zwischen bekannten Subjekten von Interesse herzustellen, um nach Spuren von Aktivitäten von Personen zu suchen, die vielleicht noch nicht bekannt sind, aber im Laufe einer Untersuchung zutage treten, und um Aktivitätsmuster zu erkennen, die auf eine Bedrohung des Vereinigten Königreichs hindeuten könnten.

366 Gemäß Paragraf 13 Absatz 1 IPA 2016 bedarf es für den Gerätezugriff durch einen Nachrichtendienst einer Genehmigung mittels einer Anordnung gemäß dem IPA 2016, sofern eine „Verbindung zu den Britischen Inseln“ vorliegt, siehe Erwägungsgrund 211.

367 Paragraf 176 IPA 2016. Eine Anordnung zum massenhaften Gerätezugriff darf nicht zu einer Handlung ermächtigen, die (sofern sie nicht im Rahmen einer gesetzlichen Befugnis erfolgt) ein unrechtmäßiges Abfangen darstellen würde (außer in Bezug auf einen gespeicherten Kommunikationsvorgang). Gemäß dem UK Explanatory Framework können die gewonnenen Informationen für die Identifizierung von Subjekten von Interesse erforderlich sein und sind in der Regel für groß angelegte Einsätze geeignet (The UK Explanatory Framework, Section H: National security, S. 28, siehe Fußnote 29).

368 Paragraf 138 Absatz 1 und Paragraf 178 Absatz 1 IPA 2016.

369 Paragraf 138 Absatz 2 und Paragraf 178 Absatz 2 IPA 2016.

www.parlament.gv.at

Vereinigten Königreichs“ und die „Verhütung und Bekämpfung schwerer Straftaten“; demnach muss ein Zusammenhang zwischen der beantragten Maßnahme und einem oder mehreren Einsatzzwecken („operational purposes“) bestehen, die in der Anordnung aufgeführt sein müssen.

(221) Die Wahl des Einsatzzwecks ist das Ergebnis eines mehrstufigen Prozesses. Gemäß Paragraf 142 Absatz 4 müssen die in der Anordnung genannten Einsatzzwecke in einer von den Leitern der Nachrichtendienste geführten Liste als Zwecke angegeben werden, die sie als Einsatzzwecke erachten, für die abgefangene Inhalte oder Sekundärdaten, die im Rahmen einer Anordnung zum massenhaften Abfangen erlangt wurden, für eine Überprüfung ausgewählt werden können. Die Liste der Einsatzzwecke muss vom Secretary of State genehmigt werden. Der Secretary of State darf diese Genehmigung nur erteilen, wenn er sich davon überzeugt hat, dass der Einsatzzweck präziser definiert ist als die allgemeinen Gründe für die Genehmigung der Anordnung (nationale Sicherheit oder nationale Sicherheit und wirtschaftliches Wohl oder Verhütung schwerer Straftaten).[370] Am Ende eines Zeitraums von jeweils drei Monaten muss der Secretary of State dem parlamentarischen Ausschuss für Nachrichtendienste und Sicherheit (Intelligence and Security Committee – ISC) eine Kopie der Liste der Einsatzzwecke zukommen lassen. Schließlich muss der Premierminister die Liste der Einsatzzwecke mindestens einmal jährlich überprüfen.[371] Wie der High Court feststellte, dürfen „diese nicht als unbedeutende Garantien abgewertet werden, da sie ein komplexes System von Rechenschaftspflichten bilden, an dem sowohl das Parlament als auch Mitglieder der Regierung auf höchster Ebene beteiligt sind“.[372]

(222) Ferner bewirken derartige Einsatzzwecke Einschränkungen dahingehend, inwieweit abgefangenes Material für eine Überprüfung ausgewählt werden kann. Die Auswahl jeglichen im Rahmen der Massenanordnung gesammelten Materials für eine Überprüfung muss im Hinblick auf den bzw. die Einsatzzweck(e) gerechtfertigt sein. Laut den Erläuterungen der britischen Behörden bedeutet dies, dass der Secretary of State die praktischen Vorkehrungen bezüglich der Überprüfung bereits in der Phase der Ausstellung der Anordnung bewerten muss, wobei ausreichende Angaben gemacht werden müssen, um die gesetzlichen Pflichten gemäß den Paragrafen 152 und 193 IPA 2016 zu erfüllen.[373] Die Angaben, die der Secretary of State bezüglich dieser Vorkehrungen erhält, müssen beispielsweise (gegebenenfalls) Informationen darüber enthalten, wie sich die Filtereinrichtungen während der Zeit, in der eine Anordnung wirksam ist, ändern könnten.[374] Weitere Einzelheiten zum Verfahren und zu den

---

370 Laut den Erläuterungen der britischen Behörden kann im Rahmen eines Einsatzzweckes beispielsweise der Anwendungsbereich einer Maßnahme auf eine Bedrohung in einem bestimmten geografischen Gebiet beschränkt werden.

371 Paragraf 142 Absätze 4 bis 10 IPA 2016.

372 High Court of Justice, Liberty, [2019] EWHC 2057 (Admin), Rn. 167.

373 Gemäß den Paragrafen 152 und 193 IPA 2016 gelten folgende Erfordernisse: a) die Auswahl für eine Überprüfung darf nur für die in der Anordnung angegebenen Einsatzzwecke erfolgen, b) die Auswahl für eine Überprüfung muss unter allen Umständen notwendig und verhältnismäßig sein, und c) die Auswahl für eine Überprüfung darf keinen Verstoß gegen das Verbot darstellen, Material auszuwählen und Kommunikationsvorgänge zu identifizieren, die von Personen gesendet wurden oder für Personen bestimmt sind, von denen bekannt ist, dass sie sich zu diesem Zeitpunkt auf den Britischen Inseln aufhalten.

374 Siehe Code of Practice on Interception of Communications, Nummer 6.6, siehe Fußnote 278.

www.parlament.gv.at

Garantien im Hinblick auf die Filter- und Überprüfungsphase finden sich im Erwägungsgrund 229.

(223) Eine Massenbefugnis darf nur dann genehmigt werden, wenn sie im Hinblick auf das angestrebte Ziel verhältnismäßig ist.[375] Laut dem Verhaltenskodex für das Abfangen von Kommunikationsvorgängen muss bei jeder Beurteilung der Verhältnismäßigkeit „die Schwere des Eingriffs in die Privatsphäre (sowie weitere Erwägungen gemäß Paragraf 2 Absatz 2) gegen die Notwendigkeit der Aktivität im Hinblick auf Ermittlungen, Einsatzzwecke oder Kapazitäten abgewogen werden. Die genehmigte Handlung sollte eine realistische Aussicht bieten, dass sich der erwartete Nutzen einstellt, und darf nicht unverhältnismäßig oder willkürlich sein.“[376] Wie bereits erwähnt, bedeutet dies in der Praxis, dass die Verhältnismäßigkeitsprüfung auf einer Abwägung zwischen dem angestrebten Ziel („Einsatzzweck(e)“ („operational purpose/s)) und den zur Verfügung stehenden technischen Optionen (z. B. gezieltes oder massenhaftes Abfangen, gezielter oder massenhafter Gerätezugriff, gezielte oder massenhafte Beschaffung von Kommunikationsdaten) beruht, wobei den am wenigsten eingreifenden Mitteln der Vorzug gegeben wird (siehe Erwägungsgründe 181 und 182). Ist mehr als eine Maßnahme zur Erreichung des Ziels geeignet, ist dem weniger stark eingreifenden Mittel der Vorzug zu geben.

(224) Eine weitere Garantie im Hinblick auf die Beurteilung der Verhältnismäßigkeit der beantragten Maßnahme besteht darin, dass der Secretary of State die relevanten Informationen erhalten muss, die er für die ordnungsgemäße Durchführung seiner Beurteilung benötigt. So ist im Verhaltenskodex für das Abfangen von Kommunikationsvorgängen (Code of Practice on Interception of Communications) sowie im Verhaltenskodex für den Gerätezugriff (Code of Practice on Equipment Interference) insbesondere vorgesehen, dass der von der zuständigen Behörde eingereichte Antrag folgende Angaben enthalten muss: die Hintergründe des Antrags, eine Beschreibung der abzufangenden Kommunikationsvorgänge und der Telekommunikationsbetreiber, deren Unterstützung erforderlich ist, eine Beschreibung der zu genehmigenden Handlung, die Einsatzzwecke und eine Erläuterung dazu, warum die Handlung notwendig und verhältnismäßig ist.[377]

(225) Schließlich – und dies ist ein wichtiger Punkt – muss die Entscheidung des Secretary of State zur Ausstellung einer Anordnung von einem unabhängigen Judicial Commissioner genehmigt werden, der die Notwendigkeit und Verhältnismäßigkeit der vorgeschlagenen Maßnahme nach denselben Grundsätzen beurteilt, die ein Gericht bei einer Anfechtungsklage zugrunde legen würde.[378] Konkret überprüft der Judicial Commissioner die Schlussfolgerungen des Secretary of State dahin gehend, ob die Anordnung notwendig ist und ob die Handlung im Lichte der Grundsätze gemäß

---

375 Paragraf 138 Absatz 1 Buchstaben b und c und Paragraf 178 Buchstaben b und c IPA 2016.

376 Code of Practice on Interception of Communications, Nummer 4.10, siehe Fußnote 278.

377 Code of Practice on Interception of Communications, Nummer 6.20, siehe Fußnote 278, und Code of Practice on Equipment Interference, Nummer 6.13, siehe Fußnote 348.

378 Paragraf 138 Absatz 1 Buchstabe g und Paragraf 178 Absatz 1 Buchstabe f IPA 2016. Die vorherige Genehmigung durch eine unabhängige Stelle wurde vom Europäischen Gerichtshof für Menschenrechte als wichtiger Schutz gegen Missbrauch im Zusammenhang mit dem massenhaften Abfangen genannt. Europäischer Gerichtshof für Menschenrechte (Große Kammer), Big Brother Watch u. a./Vereinigtes Königreich (siehe oben, Fn. 269), Rn. 351 und 352. Es sei darauf hingewiesen, dass dieses Urteil den früheren Rechtsrahmen (RIPA 2000) betraf, der einige der mit dem IPA 2016 eingeführten Garantien (einschließlich der vorherigen Genehmigung durch einen Judicial Commissioner) nicht enthielt.

www.parlament.gv.at

Paragraf 2 Absatz 2 IPA 2016 (allgemeine Pflichten in Bezug auf den Schutz der Privatsphäre) verhältnismäßig ist. Darüber hinaus prüft der Judicial Commissioner die Schlussfolgerungen des Secretary of State dahin gehend, ob jeder der in der Anordnung angegebenen Einsatzzwecke ein Zweck ist, für den eine Auswahl erforderlich ist oder sein kann. Verweigert der Judicial Commissioner die Genehmigung einer Entscheidung zur Erteilung einer Anordnung, so kann der Secretary of State i) die Entscheidung entweder akzeptieren und folglich keine Anordnung erteilen oder ii) die Angelegenheit an den Investigatory Powers Commissioner zur Entscheidung weiterleiten (sofern der Investigatory Powers Commissioner nicht die ursprüngliche Entscheidung getroffen hat).[379]

ii) Zusätzliche Garantien

(226) Mit dem IPA 2016 wurden weitere Beschränkungen in Bezug auf die Dauer, Verlängerung und Änderung einer Massenanordnung eingeführt. Die Geltungsdauer einer Anordnung darf höchstens sechs Monate betragen, und jede Entscheidung zur Verlängerung oder Änderung (mit Ausnahme geringfügiger Änderungen) einer Anordnung muss ebenfalls von einem Judicial Commissioner genehmigt werden.[380] Gemäß dem Verhaltenskodex für das Abfangen von Kommunikationsvorgängen sowie dem Verhaltenskodex für den Gerätezugriff gilt eine Änderung der Einsatzzwecke der Anordnung als wesentliche Änderung der Anordnung.[381]

(227) Ähnlich wie in den Bestimmungen für das gezielte Abfangen ist in Teil 6 des IPA 2016 vorgesehen, dass der Secretary of State sicherstellen muss, dass Vorkehrungen für Garantien in Bezug auf die Aufbewahrung und Offenlegung von im Rahmen der Anordnung erlangtem Material[382] sowie für die Offenlegung gegenüber dem Ausland[383] getroffen werden. So ist in Paragraf 150 Absatz 5 und Paragraf 191 Absatz 5 IPA 2016 vorgesehen, dass jede Kopie, die von dem im Rahmen der Anordnung gesammelten Material angefertigt wird, sicher aufbewahrt werden muss und vernichtet wird, sobald es keine maßgeblichen Gründe mehr für die Aufbewahrung gibt; Paragraf 150 Absatz 2 und Paragraf 191 Absatz 2 IPA 2016 wiederum schreiben vor, dass die Anzahl der Personen, an die das Material weitergegeben wird, und der Umfang, in dem Material offengelegt, zugänglich gemacht oder kopiert wird, auf das für die gesetzlichen Zwecke erforderliche Mindestmaß beschränkt werden müssen[384].

---

379 Paragraf 159 Absätze 3 und 4 IPA 2016.

380 Paragrafen 143 bis 146 und 184 bis 188 IPA 2016. Im Falle einer dringenden Änderung kann der Secretary of State die Änderung ohne Genehmigung vornehmen, muss aber den Commissioner davon in Kenntnis setzen; der Commissioner muss daraufhin entscheiden, ob er die Änderung genehmigt oder ablehnt (Paragraf 147 IPA 2016). Die Anordnung ist aufzuheben, wenn sie nicht mehr notwendig oder verhältnismäßig ist oder wenn die Überprüfung der abgefangenen Inhalte, Metadaten oder sonstigen Daten, die im Rahmen der Anordnung erlangt wurden, für keinen der in der Anordnung angegebenen Einsatzzwecke mehr erforderlich ist (Paragrafen 148 und 189 IPA 2016).

381 Code of Practice on Interception of Communications, Nummern 6.44 bis 6.47, siehe Fußnote 278, und Code of Practice on Equipment Interference, Nummer 6.48, siehe Fußnote 348.

382 Paragraf 156 IPA 2016.

383 Paragrafen 150 und 191 IPA 2016.

384 Die Große Kammer des Europäischen Gerichtshofs für Menschenrechte in der Rechtssache Big Brother Watch u. a./Vereinigtes Königreich (siehe Fußnote 268) bestätigte das mit dem RIPA 2000 vorgesehene System zusätzlicher Garantien für Speicherung, Zugang und Offenlegung (siehe Rn. 392-394 und 402-405). Dasselbe System von Garantien ist im IPA 2016 vorgesehen.

www.parlament.gv.at

(228) Schließlich gilt: Wenn das Material, das im Rahmen eines massenhaften Abfangens oder eines massenhaften Gerätezugriffs abgefangen wurde, an ein Drittland übergeben werden soll (Offenlegung gegenüber dem Ausland), muss der Secretary of State gemäß dem IPA 2016 sicherstellen, dass geeignete Vorkehrungen getroffen werden, um zu gewährleisten, dass in diesem Drittland ähnliche Garantien in Bezug auf Sicherheit, Speicherung und Offenlegung bestehen.[385] Zudem enthält Paragraf 109 DPA 2018 konkrete Anforderungen an die internationale Übermittlung personenbezogener Daten durch Nachrichtendienste an Drittländer oder internationale Organisationen und erlaubt die Übermittlung von Daten in ein Land oder Gebiet außerhalb des Vereinigten Königreichs oder an eine internationale Organisation nur dann, wenn die Übermittlung für die Erfüllung der gesetzlichen Aufgaben des Verantwortlichen oder für andere in Paragraf 2 Absatz 2 Buchstabe a des Security Services Act 1989 oder in Paragraf 2 Absatz 2 Buchstabe a und Paragraf 4 Absatz 2 Buchstabe a des Intelligence Service Act 1994 genannte Zwecke notwendig und verhältnismäßig ist.[386] Wichtig ist, dass diese Anforderungen auch in Fällen gelten, in denen die Ausnahme zum Schutz der nationalen Sicherheit nach Paragraf 110 DPA 2018 geltend gemacht wird, da Paragraf 110 DPA 2018 den Paragraf 109 DPA 2018 nicht als eine der Bestimmungen aufführt, die außer Kraft gesetzt werden können, wenn eine Ausnahme von bestimmten Bestimmungen zum Schutz der nationalen Sicherheit erforderlich ist.

(229) Sobald die Anordnung genehmigt wurde und die massenhafte Sammlung der Daten abgeschlossen ist, werden die Daten einem Auswahlverfahren unterzogen, bevor sie überprüft werden. In der Phase der Auswahl und der Überprüfung erfolgt eine weitere Verhältnismäßigkeitsprüfung durch einen Analysten, der auf der Grundlage der in der Anordnung angegebenen Einsatzzwecke (und möglicherweise vorhandener Filtereinrichtungen) die Kriterien für die Auswahl festlegt. Gemäß den Paragrafen 152 und 193 IPA muss der Secretary of State bei der Ausstellung der Anordnung sicherstellen, dass Vorkehrungen getroffen werden, um zu gewährleisten, dass die Auswahl des Materials nur für die angegebenen Einsatzzwecke erfolgt und unter allen Umständen notwendig und verhältnismäßig ist. Diesbezüglich haben die britischen Behörden erläutert, dass die Auswahl des massenhaft abgefangenen Materials zunächst durch automatisches Filtern erfolgt, um diejenigen Daten auszusortieren, die voraussichtlich nicht von Interesse für die nationale Sicherheit sind. Die Filter können im Laufe der Zeit variieren (da sich Muster, Typen und Protokolle des Internetverkehrs ändern) und hängen vom technologischen und operativen Kontext ab. Nach dieser Phase können die Daten nur dann für eine Überprüfung ausgewählt werden, wenn sie für die in der Anordnung angegebenen Einsatzzwecke relevant sind.[387] Die im IPA 2016 vorgesehenen Garantien für die Prüfung des gesammelten

385 Paragrafen 151 und 192 IPA 2016.

386 Nähere Angaben zu diesen Zwecken siehe Fußnote 312.

387 Dem Verhaltenskodex für das Abfangen von Kommunikationsvorgängen ist diesbezüglich zu entnehmen, dass „diese Verarbeitungssysteme Daten aus den Kommunikationsverbindungen oder -signalen verarbeiten, welche die jeweilige Behörde abgefangen hat. Der Datenverkehr über diese Verbindungen und Signale wird dann bis zu einem gewissen Grad gefiltert, um die Arten von Kommunikationsvorgängen auszuwählen, die einen potenziellen nachrichtendienstlichen Wert aufweisen, und diejenigen auszusortieren, deren nachrichtendienstlicher Wert am geringsten sein dürfte. Infolge dieses Filterverfahrens, das je nach Verarbeitungssystem unterschiedlich ausgestaltet ist, wird ein erheblicher Teil der Kommunikationsvorgänge über diese Verbindungen und Signale automatisch aussortiert. Daraufhin können weitere komplexe Suchen durchgeführt werden, um weitere Kommunikationsvorgänge zu ermitteln, deren nachrichtendienstlicher Wert am größten sein dürfte und

www.parlament.gv.at

Materials gelten für alle Arten von Daten (sowohl abgefangene Inhalte als auch Sekundärdaten)[388]. Gemäß den Paragrafen 152 und 193 IPA 2016 besteht zudem ein allgemeines Verbot, Material für eine Überprüfung auszuwählen, das sich auf Kommunikationsvorgänge bezieht, die von Personen gesendet wurden oder für Personen bestimmt sind, die sich auf den Britischen Inseln aufhalten. Wollen die Behörden derartiges Material untersuchen, müssen sie einen Antrag auf eine gezielte Überprüfung gemäß Teil 2 und Teil 4 des IPA 2016 stellen, der vom Secretary of State ausgestellt und von einem Judicial Commissioner genehmigt werden muss[389]. Wer abgefangene Inhalte vorsätzlich entgegen den gesetzlichen Vorgaben zur Überprüfung[390] auswählt, begeht eine Straftat.[391]

(230) Die vom Analysten im Hinblick auf die Auswahl des Materials durchgeführte Bewertung unterliegt einer Ex-post-Aufsicht durch den IPC; dabei beurteilt dieser die Einhaltung der im IPA 2016 für die Überprüfungsphase festgelegten spezifischen Garantien (siehe auch Erwägungsgrund 229).[392] Der IPC muss die Ausübung der im IPA 2016 aufgeführten Ermittlungsbefugnisse durch öffentliche Behörden laufend überprüfen (unter anderem durch Überprüfungen, Kontrollen und Untersuchungen).[393] Diesbezüglich ist im Verhaltenskodex für das Abfangen von Kommunikationsvorgängen und im Verhaltenskodex für den Gerätezugriff vorgesehen, dass der betreffende Nachrichtendienst Aufzeichnungen für spätere Untersuchungen und Überprüfungen führen muss; aus diesen Aufzeichnungen muss hervorgehen, warum der Zugriff auf das Material durch befugte Personen notwendig und verhältnismäßig ist und welche Einsatzzwecke damit verfolgt werden.[394] In seinem Jahresbericht 2018 gelangte das Investigatory Powers Commissioner Office (IPCO)[395] beispielsweise zu dem Schluss, dass die von den Analysten dokumentierten Begründungen für die Überprüfung von bestimmtem, massenhaft gesammeltem Material dem erforderlichen Grundsatz der Verhältnismäßigkeit entsprachen, da die Gründe für die Abfragen („queries“) im Hinblick auf das zu erreichende Ziel ausreichend detailliert beschrieben waren.[396] In seinem Bericht aus dem Jahr 2019 zu

---

die einen Bezug zu den gesetzlichen Aufgaben des Dienstes aufweisen. Diese Kommunikationsvorgänge können dann für eine Überprüfung für einen oder mehrere der in der Anordnung angegebenen Einsatzzwecke ausgewählt werden, wenn die Bedingungen der Notwendigkeit und Verhältnismäßigkeit erfüllt sind. Dabei können nur solche Elemente, die nicht herausgefiltert wurden, potenziell für eine Überprüfung durch befugte Personen ausgewählt werden“ (Codes of practice on interception of communications, Nummer 6.6, siehe Fußnote 278).

388 Siehe Paragraf 152 Absatz 1 Buchstaben a und b IPA 2016, wonach die Prüfung beider Arten von Daten (abgefangene Inhalte und Sekundärdaten) nur für den angegebenen Zweck durchgeführt werden darf und unter allen Umständen notwendig und verhältnismäßig sein muss.

389 Diese Art von Anordnung ist nicht erforderlich, wenn es sich bei den Daten zu Personen, die sich auf der britischen Insel aufhalten, um „Sekundärdaten“ handelt (siehe Paragraf 152 Absatz 1 Buchstabe c IPA 2016).

390 Paragrafen 152 und 193 IPA 2016.

391 Paragrafen 155 und 196 IPA 2016.

392 Paragrafen 152 und 193 IPA 2016.

393 Paragraf 229 IPA 2016.

394 Code of Practice on Interception of Communications, Nummer 6.74, siehe Fußnote 278, und Code of Practice on Equipment Interference, Nummer 6.78, siehe Fußnote 348.

395 Das IPCO wurde gemäß Paragraf 238 IPA 2016 eingerichtet, um dem IPC das Personal, die Räumlichkeiten, die Ausrüstung sowie sonstige Einrichtungen und Dienstleistungen zur Verfügung zu stellen, die er für die Ausübung seiner Aufgaben benötigt (siehe Erwägungsgrund 251).

396 Dem Jahresbericht 2018 des IPCO war zu entnehmen, dass die von den Analysten der GCHQ dokumentierten Begründungen „dem geforderten Standard entsprachen und die Analysten die

www.parlament.gv.at

den Massenbefugnissen stellte das IPCO ganz klar seine Absicht fest, das massenhafte Abfangen auch weiterhin zu kontrollieren und dabei auch die Selektoren und Suchkriterien im Einzelnen zu überprüfen[397]. Darüber hinaus wird es die Wahl der Überwachungsmaßnahmen (gezielt oder massenhaft) sowohl bei der Prüfung von Anträgen auf Anordnungen im Rahmen des „Double-Lock"-Verfahrens als auch bei Inspektionen weiterhin im Einzelfall sorgfältig prüfen[398]. Diese weitere Überwachung wird im Zusammenhang mit der in den Erwägungsgründen 281 bis 284 genannten Überwachung dieses Beschlusses durch die Kommission gebührend berücksichtigt.

3.3.1.1.4.2 Massenhafte Beschaffung von Kommunikationsdaten

(231) Teil 6 Kapitel 2 des IPA 2016 enthält Bestimmungen zu Anordnungen zur massenhaften Beschaffung; durch eine solche Anordnung enthält der Adressat die Befugnis, von einem Telekommunikationsbetreiber die Offenlegung oder die Herausgabe von in seinem Besitz befindlichen Kommunikationsdaten zu verlangen. Des Weiteren erhält die ersuchende Behörde die Befugnis zur Auswahl der Daten für eine weitere Überprüfung. Ähnlich wie die gezielte Speicherung und Beschaffung von Kommunikationsdaten (siehe Erwägungsgrund 199) bezieht sich auch die massenhafte Beschaffung von Kommunikationsdaten in der Regel nicht auf personenbezogene Daten von betroffenen Personen in der EU, die gemäß diesem Beschluss in das Vereinigte Königreich übermittelt werden. Die Verpflichtung zur Offenlegung von Kommunikationsdaten gemäß Teil 6 Kapitel 2 des IPA 2016 bezieht sich auf Daten, die von Telekommunikationsbetreibern im Vereinigten Königreich direkt von den Nutzern eines Telekommunikationsdienstes erhoben werden.[399] Diese Art der „kundenseitigen" Verarbeitung umfasst typischerweise keine Übermittlung auf der Grundlage dieses Beschlusses, d. h. eine Übermittlung von einem Verantwortlichen/Auftragsverarbeiter in der EU an einen Verantwortlichen/Auftragsverarbeiter im Vereinigten Königreich.

Verhältnismäßigkeit ihrer Abfragen von Massendaten ausreichend detailliert dargelegt hatten". Jahresbericht 2018 des Investigatory Powers Commissioner, Nummer 6.22, siehe Fußnote 464.

397 Jahresbericht 2019 des Investigatory Powers Commissioner, Nummer 6.22, siehe Fußnote 463.

398 Jahresbericht 2019 des Investigatory Powers Commissioner, Nummer 10.22, siehe Fußnote 463.

399 Dies ergibt sich aus der Definition von Kommunikationsdaten in Paragraf 261 Absatz 5 des IPA 2016, wonach Kommunikationsdaten sich im Besitz eines Telekommunikationsbetreibers befinden oder von diesem erlangt werden und sich entweder auf den Nutzer eines Telekommunikationsdienstes und die Bereitstellung dieses Dienstes beziehen oder in einem Kommunikationsvorgang enthalten, Teil eines Kommunikationsvorgangs oder mit einem Kommunikationsvorgang verknüpft oder logisch mit ihm verbunden sind (siehe auch Code of Practice on Bulk Acquisition of Communications Data, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf Nummern 2.15 bis 2.22). Darüber hinaus muss es sich bei einem Telekommunikationsbetreiber im Sinne der Definition nach Paragraf 261 Absatz 10 IPA 2016 um eine Person handeln, die einen Telekommunikationsdienst für Personen im Vereinigten Königreich anbietet oder erbringt oder die ein Telekommunikationssystem kontrolliert oder bereitstellt, das sich (ganz oder teilweise) im Vereinigten Königreich befindet oder vom Vereinigten Königreich aus kontrolliert wird. Diese Definitionen machen deutlich, dass Telekommunikationsbetreibern, deren Systeme sich nicht im Vereinigten Königreich befinden oder von dort aus kontrolliert werden und die keine Dienste für Personen im Vereinigten Königreich anbieten oder erbringen, keine Verpflichtungen gemäß dem IPA 2016 auferlegt werden dürfen (siehe auch Code of Practice on Bulk Acquisition of Communications Data, Nummer 2.2). Wenn Teilnehmer aus der EU (unabhängig davon, ob sie in der EU oder im Vereinigten Königreich ansässig sind) Dienste im Vereinigten Königreich in Anspruch nehmen, werden sämtliche Kommunikationsdaten im Zusammenhang mit der Erbringung dieses Dienstes direkt vom Diensteanbieter im Vereinigten Königreich erfasst und nicht von der EU aus übermittelt.

www.parlament.gv.at

(232) Der Vollständigkeit halber werden jedoch im Folgenden die für die massenhafte Beschaffung von Kommunikationsdaten geltenden Bedingungen und Garantien beschrieben.

(233) Der IPA 2016 ersetzt die Rechtsvorschrift über die massenhafte Beschaffung von Kommunikationsdaten, die Gegenstand des EuGH-Urteils in der Rechtssache Privacy International war. Die Rechtsvorschrift, um die es in dieser Rechtssache ging, wurden aufgehoben, und die neue Regelung sieht spezifische Bedingungen und Garantien für die Genehmigung einer solchen Maßnahme vor.

(234) Anders als bei der vorherigen Regelung, gemäß der der Secretary of State die Maßnahme nach freiem Ermessen genehmigen konnte[400], darf er gemäß dem IPA 2016 nur noch dann eine Anordnung ausstellen, wenn die Maßnahme notwendig und verhältnismäßig ist. In der Praxis bedeutet das, dass ein Zusammenhang zwischen dem Datenzugriff und dem verfolgten Ziel bestehen sollte.[401] Konkret muss der Secretary of State prüfen, ob ein Zusammenhang zwischen der beantragten Maßnahme und einem oder mehreren in der Anordnungen angegebenen „Einsatzzweck(en)" besteht (siehe Erwägungsgrund 219). In Bezug auf die Beurteilung der Verhältnismäßigkeit heißt es im einschlägigen Verhaltenskodex, dass „der Secretary of State berücksichtigen muss, ob das mit der Anordnung angestrebte Ziel nach vernünftigem Ermessen auch mit anderen, weniger stark eingreifenden Mitteln erreicht werden könnte (Paragraf 2 Absatz 2 Buchstabe a IPA 2016). So ist beispielsweise zu prüfen, ob die benötigten Informationen durch Ausübung einer weniger stark eingreifenden Befugnis wie der gezielten Beschaffung von Kommunikationsdaten erlangt werden könnten."[402]

(235) Bei der Durchführung dieser Beurteilung stützt sich der Secretary of State auf Informationen, die die Leiter der Nachrichtendienste[403] in ihrem Antrag angeben müssen, z. B. die Gründe, warum die Maßnahme aus einem der gesetzlichen Gründe als notwendig erachtet wird, und die Gründe, weshalb das angestrebte Ziel nach vernünftigem Ermessen nicht mit anderen, weniger stark eingreifenden Mitteln erreicht werden kann.[404] Ferner bewirken die Einsatzzwecke Einschränkungen dahin gehend, inwieweit die im Rahmen einer Anordnung erlangten Daten für eine Überprüfung ausgewählt werden können.[405] Gemäß dem einschlägigen Verhaltenskodex müssen die Einsatzzwecke eine klare Anforderung umfassen und ausreichend detailliert sein, damit sich der Secretary of State davon überzeugen kann, dass die beschafften Daten nur aus bestimmten Gründen für eine Überprüfung

---

400 Gemäß Paragraf 94 Absatz 1 des Telekommunikationsgesetzes (Telecommunication Act) von 1984 konnte der Secretary of State „Anweisungen allgemeiner Art erlassen, die ihm im Interesse der nationalen Sicherheit erforderlich oder zweckmäßig erschienen" (siehe Fußnote 451).

401 Siehe Rechtssache Privacy International, Rn. 78.

402 Siehe Code of Practice on Bulk Acquisition of Communications Data, Nummer 4.11 (siehe Fußnote 399).

403 Eine Anordnung zur massenhaften Beschaffung kann nur von den Leitern der Nachrichtendienste beantragt werden, nämlich vom: i) Generaldirektor des Security Service, ii) Leiter des Secret Intelligence Service oder iii) Direktor der GCHQ (siehe Paragrafen 158 und 263 IPA 2016).

404 Code of Practice on Bulk Acquisition of Communications Data, Nummer 4.5 (siehe Fußnote 399).

405 Gemäß Paragraf 161 IPA 2016 müssen die in der Anordnung genannten Einsatzzwecke in einer von den Leitern der Nachrichtendienste geführten Liste („Liste der Einsatzzwecke") als Zwecke angegeben werden, die sie als Einsatzzwecke erachten, für die Kommunikationsdaten, die im Rahmen einer Anordnung zur massenhaften Beschaffung erlangt wurden, für eine Überprüfung ausgewählt werden können.

www.parlament.gv.at

ausgewählt werden.[406] So muss der Secretary of State vor der Genehmigung der Anordnung sicherstellen, dass besondere Vorkehrungen getroffen wurden, um zu gewährleisten, dass nur das Material für eine Überprüfung ausgewählt wird, das für einen Einsatzzweck und einen gesetzlichen Zweck als notwendig erachtet wurde, und dass die Auswahl unter allen Umständen verhältnismäßig und notwendig ist. Dieses in den Paragrafen 158 und 172 IPA 2016 beschriebene spezifische Erfordernis[407], wonach die für die Zwecke der Auswahl verwendeten Kriterien im Vorfeld auf ihre Notwendigkeit und Verhältnismäßigkeit hin bewertet werden müssen, stellt eine weitere wichtige Neuerung der durch den IPA 2016 eingeführten Regelung im Vergleich zu der zuvor geltenden Regelung dar.

(236) Zudem wurde mit dem IPA 2016 die Verpflichtung eingeführt, wonach der Secretary of State vor dem Erlass der Anordnung für die massenhafte Beschaffung von Kommunikationsdaten sicherstellen muss, dass spezifische Beschränkungen in Bezug auf die Sicherheit, Speicherung und Offenlegung der gesammelten personenbezogenen Daten gelten.[408] Im Falle einer Offenlegung gegenüber dem Ausland gelten die in Erwägungsgrund 227 beschriebenen Garantien für das massenhafte Abfangen und den massenhaften Gerätezugriff auch in diesem Kontext.[409] Weitere Beschränkungen sind in den Bestimmungen über die Dauer[410], Verlängerung[411] und Änderung von Massenanordnungen festgelegt.[412]

(237) Wichtig ist, dass der Secretary of State, wie auch bei den anderen Massenbefugnissen, vor dem Erlass der Anordnung die Genehmigung eines Judicial Commissioner einholen muss.[413] Dies ist ein zentrales Merkmal der mit dem IPA 2016 eingeführten Regelung.

(238) Der IPC führt eine Ex-post-Aufsicht über das Verfahren zur Überprüfung des massenhaft beschafften Materials (Kommunikationsdaten) durch (siehe Erwägungsgrund 254). Diesbezüglich wurde mit dem IPA 2016 die Anforderung eingeführt, wonach der Analyst des Nachrichtendienstes, der die Überprüfung durchführt, vor der Auswahl der zu überprüfenden Daten den Grund festhalten muss, warum die vorgeschlagene Überprüfung für einen bestimmten Einsatzzweck notwendig und verhältnismäßig ist.[414] In seinem Jahresbericht 2019 stellte das IPCO im Hinblick die Methoden der GCHQ und des MI5 fest, dass „die kritische Rolle von Massenkommunikationsdaten für die verschiedenen Tätigkeiten der GCHQ in den vom IPCO geprüften Fällen klar dargelegt wurde. Wir [das IPCO] haben die Art der angeforderten Daten und die angegebenen nachrichtendienstlichen Erfordernisse geprüft und sind zu der Überzeugung gelangt, dass die Dokumentation belegt, dass die

406 Code of Practice on Bulk Acquisition of Communications Data, Nummer 6.6 (siehe Fußnote 399).

407 Gemäß Paragraf 172 IPA 2016 müssen für die Phase des Filterns und der Auswahl von massenhaft beschafften Kommunikationsdaten für eine Überprüfung besondere Garantien gelten. Darüber hinaus stellt eine Überprüfung, die vorsätzlich unter Verletzung dieser Garantien vorgenommen wird, einen Straftatbestand dar (siehe Paragraf 173 IPA 2016).

408 Paragraf 171 IPA 2016.

409 Paragraf 171 Absatz 9 IPA 2016.

410 Paragraf 162 IPA 2016.

411 Paragraf 163 IPA 2016.

412 Paragrafen 164 bis 166 IPA 2016.

413 Paragraf 159 IPA 2016.

414 Jahresbericht 2019 des IPCO, Nummer 8.6, siehe Fußnote 463.

www.parlament.gv.at

Vorgehensweise der GCHQ notwendig und verhältnismäßig war.[415] […] Die vom MI5 dokumentierten Begründungen entsprachen einem guten Standard sowie den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit.“[416]

3.3.1.1.4.3 Speicherung und Überprüfung von personenbezogenen Massendatensätzen

(239) Durch Anordnungen für personenbezogene Massendatensätze (Bulk Personal Datasets – im Folgenden „BPD“)[417] erhalten Nachrichtendienste die Befugnis, Datensätzen, die personenbezogene Daten zu einer Reihe von Personen enthalten, zu speichern und zu überprüfen. Laut den Erläuterungen der britischen Behörden stellt die Analyse solcher Datensätze mitunter „die einzige Möglichkeit für die UK Intelligence Community (UKIC) dar, Ermittlungsfortschritte zu erzielen und Terroristen zu identifizieren, wenn nur sehr wenige nachrichtendienstliche Hinweise vorliegen oder wenn Kommunikationsvorgänge absichtlich verheimlicht wurden“.[418] Es gibt zwei Arten von Anordnungen: Anordnungen für personenbezogene Massendatensätze einer Klasse („Class BPD warrants“)[419], die sich auf eine bestimmte Kategorie von Datensätzen beziehen, d. h. Datensätze, die sich in Bezug auf ihren Inhalt und ihre vorgeschlagene Verwendung ähneln und bei denen ähnliche Erwägungen – z. B. in Bezug auf das Ausmaß des Eingriffs sowie die Sensibilität und Verhältnismäßigkeit der Verwendung der Daten – zu berücksichtigen sind, sodass der Secretary of State die Notwendigkeit und Verhältnismäßigkeit der Beschaffung aller Daten innerhalb der betreffenden Klasse auf einmal prüfen kann. Eine solche Anordnung kann sich beispielsweise auf Datensätze von Reisedaten erstrecken, die sich auf ähnliche Reiserouten beziehen.[420] Anordnungen für einen spezifischen personenbezogenen Massendatensatz („Specific BPD warrants“)[421] betreffen hingegen einen bestimmten Datensatz, z. B. einen Datensatz mit einer neuartigen oder ungewöhnlichen Art von Informationen, der nicht unter eine bestehende Anordnung für BPD einer Klasse fällt, oder einen Datensatz, der bestimmte Arten von personenbezogenen Daten betrifft[422] und daher zusätzliche Garantien erfordert.[423] Gemäß den Bestimmungen des IPA 2016 zu BPD dürfen derartige Datensätze nur dann überprüft und gespeichert werden, wenn

---

415 Jahresbericht 2019 des IPCO, Nummer 10.4, siehe Fußnote 463.

416 Jahresbericht 2019 des IPCO, Nummer 8.37, siehe Fußnote 463.

417 Paragraf 200 IPA 2016.

418 The UK Explanatory Framework for Adequacy Discussions, section H: National Security, S. 34, siehe Fußnote 29.

419 Paragraf 204 IPA 2016.

420 Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, Nummer 4.7, abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.

421 Paragraf 205 IPA 2016.

422 Beispielsweise sensible personenbezogene Daten, siehe Paragraf 202 IPA 2016 und Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, Nummern 4.21 und 4.12, siehe Fußnote 469.

423 Ein Antrag auf eine Anordnung für einen spezifischen BPD muss vom Secretary of State individuell, d. h. in Bezug auf einen bestimmten Datensatz, geprüft werden. Ein Nachrichtendienst ist gemäß Paragraf 205 IPA verpflichtet, seinem Antrag auf eine Anordnung für einen spezifischen BPD eine detaillierte Erläuterung der Art und des Umfangs des fraglichen Materials sowie eine Liste der „Einsatzzwecke“ („operational purposes“) beizufügen, für die er den BPD überprüfen möchte (sofern er eine Anordnung zur Speicherung und Überprüfung und nicht nur zur Speicherung beantragt). Bei der Ausstellung einer Anordnung für BPD einer Klasse hingegen prüft der Secretary of State die gesamte Kategorie von Datensätzen auf einmal.

www.parlament.gv.at

dies notwendig und verhältnismäßig ist[424] und im Einklang mit den allgemeinen Verpflichtungen in Bezug auf den Datenschutz steht[425].

(240) Die Befugnis zum Erlass einer BPD-Anordnung unterliegt dem „Double-Lock"-Verfahren: Die Beurteilung der Notwendigkeit und Verhältnismäßigkeit der Maßnahme erfolgt zunächst durch den Secretary of State und anschließend durch den Judicial Commissioner.[426] Dabei muss der Secretary of State Folgendes berücksichtigen: die Art und den Umfang der beantragten Anordnung, die Kategorie der betroffenen Daten und die Anzahl der einzelnen personenbezogenen Massendatensätze, die voraussichtlich unter die jeweilige Art der Anordnung fallen.[427] Darüber hinaus müssen gemäß dem Verhaltenskodex für die Speicherung und Verwendung von personenbezogenen Massendatensätzen durch die Nachrichtendienste (Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets) detaillierte Aufzeichnungen geführt werden, die der Prüfung durch den IPC unterliegen.[428] Die Speicherung und Überprüfung von BPD außerhalb des gesetzlichen Rahmens des IPA 2016 stellt eine Straftat dar.[429]

3.3.2 Weitere Verwendung der erhobenen Daten

(241) Personenbezogene Daten, die gemäß Teil 4 des DPA 2018 verarbeitet werden, dürfen nicht in einer Weise verarbeitet werden, die mit dem Zweck, für den sie erhoben wurden, unvereinbar ist.[430] Gemäß dem DPA 2018 kann der Verantwortliche die Daten für einen anderen Zweck verarbeiten als den, für den die Daten erhoben wurden, wenn dieser Zweck mit dem ursprünglichen Zweck vereinbar ist, wenn der Verantwortliche gesetzlich befugt ist, die Daten zu verarbeiten, und wenn diese Verarbeitung notwendig und verhältnismäßig ist.[431] Ferner sind die Leiter der Nachrichtendienste gemäß dem Security Service Act 1989 und dem Intelligence Services Act 1994 verpflichtet, sicherzustellen, dass Informationen nur dann erlangt oder offengelegt werden, wenn dies für die ordnungsgemäße Erfüllung der Aufgaben der Nachrichtendienste oder für andere begrenzte und spezifische Zwecke, die in den entsprechenden Bestimmungen aufgeführt sind,[432] erforderlich ist.

---

424 Paragrafen 204 und 205 IPA 2016.

425 Paragraf 2 IPA 2016.

426 Paragrafen 204 und 205 IPA 2016.

427 Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, Nummer 5.2, siehe Fußnote 420.

428 Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, Nummern 8.1 bis 8.15, siehe Fußnote 420.

429 The UK Explanatory Framework for Adequacy Discussions, section H: National Security, S. 34, siehe Fußnote 29.

430 Paragraf 87 Absatz 1 DPA 2018.

431 Paragraf 87 Absatz 3 DPA 2018. Zwar können Verantwortliche gemäß Paragraf 110 DPA 2018 von diesem Grundsatz ausgenommen werden, soweit dies zum Schutz der nationalen Sicherheit erforderlich ist, doch muss eine solche Ausnahme von Fall zu Fall geprüft werden und kann nur insoweit in Anspruch genommen werden, als die Anwendung einer bestimmten Bestimmung negative Folgen für die nationale Sicherheit hätte (siehe Erwägungsgrund 132). Die nationalen Sicherheitsbescheinigungen für britische Nachrichtendienste (abrufbar unter folgendem Link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) beziehen sich nicht auf Paragraf 87 Absatz 3 DPA 2018. Da außerdem jede Verarbeitung für einen anderen Zweck gesetzlich zulässig sein muss, müssen Nachrichtendienste eine eindeutige Rechtsgrundlage für die Weiterverarbeitung haben.

432 Nähere Angaben zu diesen Zwecken siehe Fußnote 312.

www.parlament.gv.at

(242) Darüber hinaus enthält Paragraf 109 DPA 2018 besondere Anforderungen in Bezug auf internationale Übermittlungen personenbezogener Daten durch Nachrichtendienste an Drittländer oder internationale Organisationen. Nach diesen Bestimmungen dürfen personenbezogene Daten nur dann in ein Land oder Gebiet außerhalb des Vereinigten Königreichs oder an eine internationale Organisation übermittelt werden, wenn die Übermittlung für die Erfüllung der gesetzlichen Aufgaben des Verantwortlichen oder für andere in Paragraf 2 Absatz 2 Buchstabe a des Security Service Act 1989 oder in Paragraf 2 Absatz 2 Buchstabe a und Paragraf 4 Absatz 2 Buchstabe a des Intelligence Services Act 1994 genannte Zwecke notwendig und verhältnismäßig ist.[433] Wichtig ist, dass diese Anforderungen auch in Fällen gelten, in denen die Ausnahme zum Schutz der nationalen Sicherheit nach Paragraf 110 DPA 2018 geltend gemacht wird, da Paragraf 110 DPA 2018 den Paragraf 109 DPA 2018 nicht als eine der Bestimmungen aufführt, die außer Kraft gesetzt werden können, wenn eine Ausnahme von bestimmten Bestimmungen zum Schutz der nationalen Sicherheit erforderlich ist.

(243) Darüber hinaus unterliegt ein Nachrichtendienst, wie die ICO in ihren Leitlinien zur Verarbeitung durch Nachrichtendienste betont hat, zusätzlich zu den in Teil 4 des DPA 2018 vorgesehenen Garantien beim Austausch von Daten mit einem Nachrichtendienst eines Drittlands auch Garantien, die in anderen für sie geltenden Rechtsvorschriften vorgesehen sind, damit sichergestellt ist, dass personenbezogene Daten rechtmäßig und verantwortungsbewusst erhoben, weitergegeben und verarbeitet werden[434]. Beispielsweise enthält der IPA 2016 weitere Garantien in Bezug auf die Übermittlung von Material, das durch gezieltes Abfangen[435], gezielten Gerätezugriff[436], massenhaftes Abfangen[437], massenhafte Beschaffung von Kommunikationsdaten[438] und massenhaften Gerätezugriff[439] gesammelt wurde, an ein Drittland (Offenlegung gegenüber dem Ausland). Insbesondere muss die Behörde, die die Anordnung ausstellt, sicherstellen, dass Vorkehrungen getroffen werden, um zu gewährleisten, dass das Drittland, das die Daten erhält, die Anzahl der Personen, denen gegenüber das Material offengelegt wird, den Umfang, in dem das Material offengelegt wird, und die Anzahl der Kopien, die von dem Material angefertigt werden, auf das für die genehmigten Zwecke gemäß IPA 2016 notwendige Mindestmaß beschränkt.[440]

3.3.3 Aufsicht

---

433 Siehe Fußnote 312.

434 ICO guidance on intelligence services processing (siehe Fußnote 161).

435 Paragraf 54 IPA 2016.

436 Paragraf 130 IPA 2016.

437 Paragraf 151 IPA 2016.

438 Paragraf 171 Absatz 9 IPA 2016.

439 Paragraf 192 IPA 2016.

440 Im Rahmen dieser Vorkehrungen sind auch Maßnahmen zu treffen, um sicherzustellen, dass jede von diesem Material angefertigte Kopie für die Dauer ihrer Aufbewahrung sicher aufbewahrt wird. Das im Rahmen einer Anordnung erlangte Material und jede davon angefertigte Kopie müssen vernichtet werden, sobald keine relevanten Gründe mehr für die Aufbewahrung bestehen (siehe Paragrafen 150 Absätze 2 und 5 sowie Paragraf 151 Absatz 2 IPA 2016). Im Übrigen wurde festgestellt, dass ähnliche, im früheren Rechtsrahmen (RIPA 2000) vorgesehene Garantien den Anforderungen des Europäischen Gerichtshofs für Menschenrechte für den Austausch von Material, das durch Massenüberwachung mit ausländischen Staaten oder internationalen Organisationen gewonnen wurde, genügten (Europäischer Gerichtshof für Menschenrechte (Große Kammer), Big Brother Watch u. a./Vereinigtes Königreich, siehe oben, Fn. 279), Rn. 362 und 399.

www.parlament.gv.at

(244) Der staatliche Zugriff für Zwecke der nationalen Sicherheit unterliegt der Aufsicht durch eine Reihe unterschiedlicher Stellen. Der Information Commissioner beaufsichtigt die Verarbeitung personenbezogener Daten im Lichte des DPA 2018 (weitere Informationen zur Unabhängigkeit, Ernennung, Rolle und zu den Befugnissen des Information Commissioner enthalten die Erwägungsgründe 85 bis 98); für die unabhängige und gerichtliche Aufsicht über die Ausübung von Ermittlungsbefugnissen gemäß dem IPA 2016 ist hingegen der IPC zuständig. Der IPC beaufsichtigt die Ausübung der durch den IPA 2016 gewährten Ermittlungsbefugnisse sowohl durch Strafverfolgungsbehörden als auch durch nationale Sicherheitsbehörden. Auf politischer Ebene wird die Aufsichtsfunktion durch den Nachrichtendienstausschuss (Intelligence Service Committee) des Parlaments wahrgenommen.

3.3.3.1 Aufsicht gemäß Teil 4 des DPA

(245) Die Verarbeitung personenbezogener Daten durch die Nachrichtendienste gemäß Teil 4 des DPA 2018 wird durch den Information Commissioner beaufsichtigt.[441]

(246) 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 diesen Aufgaben gehören unter anderem 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, die Durchführung von Untersuchungen usw.

(247) 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 erteilen, wenn der Verstoß bestätigt wird. Ferner kann er Durchsetzungs- und Bußgeldbescheide für Verstöße gegen bestimmte Bestimmungen des Rechtsaktes erteilen.[442] Anders als bei anderen Teilen des DPA 2018 kann der Information Commissioner jedoch keinen Bewertungsbescheid an eine nationale Sicherheitsbehörde erteilen.[443]

(248) Darüber hinaus sieht Paragraf 110 DPA 2018 bezüglich der Ausübung bestimmter Befugnisse des Information Commissioner eine Ausnahme vor, wenn dies zum Schutz

441 Paragraf 116 DPA 2018.

442 Gemäß Anhang 13 Nummer 2 des 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 des 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 mitzuteilen, 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 Erwägungsgrund 92).

443 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 die Government Communications Headquarters.

www.parlament.gv.at

der nationalen Sicherheit erforderlich ist. Dies betrifft die Befugnis des Information Commissioner, Bescheide (Informations-, Bewertungs-, Durchsetzungs- und 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.[444] Wie in Erwägungsgrund 126 erläutert, gelten diese Ausnahmen nur im Einzelfall und nur dann, wenn sie notwendig und verhältnismäßig sind.

(249) Das ICO und die britischen Nachrichtendienste haben eine Absichtserklärung[445] 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 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.[446]

3.3.3.2 Aufsicht über die Ausübung von Ermittlungsbefugnissen im Rahmen des IPA 2016

(250) Für die Aufsicht über die Ausübung von Ermittlungsbefugnissen ist gemäß Teil 8 des IPA 2016 der Investigatory Powers Commissioner (IPC) zuständig. Unterstützt wird er dabei von anderen Judicial Commissioners, die gemeinsam als Judicial Commissioners bezeichnet werden.[447] Das IPA 2016 enthält Garantien zum Schutz der Unabhängigkeit der Judicial Commissioners. Judicial Commissioners müssen ein

---

444 Folgende Bestimmungen können Gegenstand der Ausnahme sein: Paragraf 108 (Mitteilung 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); Paragrafen 170 bis 173 (Straftaten im Zusammenhang mit personenbezogenen Daten). Darüber hinaus 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.

445 Absichtserklärung zwischen dem Büro des Information Commissioner und der UK Intelligence Community, siehe Fußnote 165.

446 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).

447 Gemäß Paragraf 227 Absätze 7 und 8 IPA 2016 ist der Investigatory Powers Commissioner ein Judicial Commissioner, und der Investigatory Powers Commissioner und die übrigen Judicial Commissioners werden gemeinsam als die Judicial Commissioners bezeichnet. Derzeit gibt es 15 Judicial Commissioners.

www.parlament.gv.at

hohes richterliches Amt bekleiden oder bekleidet haben[448] (d. h. sie müssen einem der höchsten Gerichte angehören oder angehört haben) und sind, wie alle Angehörigen des Justizwesens, von der Regierung unabhängig[449]. Nach Paragraf 227 IPA 2016 ernennt der Premierminister den IPC und so viele Judicial Commissioners, wie er es für erforderlich hält. Alle Commissioners, unabhängig davon, ob sie Angehörige des Justizwesens sind oder waren, können nur auf der Grundlage einer gemeinsamen Empfehlung der drei Obersten Richter für England & Wales, Schottland und Nordirland und des Lord Chancellor ernannt werden[450]. Der Secretary of State muss dem IPC Personal, Räumlichkeiten, Ausrüstung sowie sonstige Einrichtungen und Dienstleistungen zur Verfügung stellen.[451] Die Amtszeit der Judicial Commissioners beträgt drei Jahre; eine Wiederernennung ist möglich.[452] Ihre Unabhängigkeit wird zudem noch dadurch abgesichert, dass für die Amtsenthebung eines Judicial Commissioner strenge Voraussetzungen und hohe Hürden gelten; sie erfolgt entweder durch den Premierminister unter den in Paragraf 228 Absatz 5 IPA 2016 erschöpfend aufgeführten besonderen Umständen (z. B. Konkurs oder Inhaftierung), oder wenn beide Kammern des Parlaments einen entsprechenden Beschluss zur Genehmigung der Amtsenthebung erlassen haben[453].

(251) Der IPC und die Judicial Commissioners werden bei der Erfüllung ihrer Aufgaben durch das Investigatory Powers Commissioner's Office (IPCO) unterstützt. Zum Stab des IPCO zählen ein Team von Inspektoren, interne Rechts- und Technikexperten sowie ein Sachverständigengremium für Beratung in technischen Angelegenheiten. Ebenso wie bei den einzelnen Judicial Commissioners, ist die Unabhängigkeit des IPCO geschützt. Das IPCO ist eine nachgelagerte Behörde („arm's-length body“) des Innenministeriums; das heißt, es erhält Mittel vom Innenministerium, führt seine Aufgaben jedoch unabhängig aus.[454]

---

448 Nach Teil 3 Paragraf 60 Absatz 2 des Gesetzes über die Verfassungsreform von 2005 (Constitutional Reform Act 2005) bezeichnet der Begriff „hohes richterliches Amt“ das Amt eines Richters an einem der folgenden Gerichte: i) Supreme Court, ii) Court of Appeal in England and Wales, iii) High Court of England and Wales, iv) Court of Session, v) Court of Appeal in Northern Ireland, vi) High Court in Northern Ireland, oder das Amt als Lord of Appeal in Ordinary.

449 Die Unabhängigkeit der Justiz beruht auf Konventionen und ist seit dem Gesetz zur Regelung der Thronfolge Englands (Act of Settlement) von 1701 allgemein anerkannt.

450 Paragraf 227 Absatz 3 IPA 2016. Gemäß Paragraf 227 Absatz 4 Buchstabe e IPA 2016 müssen Judicial Commissioners zudem vom Investigatory Powers Commissioner empfohlen werden.

451 Paragraf 238 IPA 2016.

452 Paragraf 227 Absatz 2 IPA 2016.

453 Das Amtsenthebungsverfahren entspricht dem Amtsenthebungsverfahren für andere Richter im Vereinigten Königreich (siehe z. B. Paragraf 11 Absatz 3 des Gesetzes über höhere Gerichte (Senior Courts Act) von 1981 und Paragraf 33 des Gesetzes über die Verfassungsreform (Constitutional Reform Act) von 2005, die ebenfalls einen Beschluss nach Billigung durch beide Kammern des Parlaments erfordern). Bis heute wurde noch kein Judicial Commissioner seines Amtes enthoben.

454 Mit dem Begriff „arm's-length body“ wird eine Einrichtung oder Behörde bezeichnet, die zwar von der Regierung finanziert wird, aber unabhängig handelt (eine Definition und weitere Informationen hierzu enthalten das Handbuch des Kabinettbüros für die Klassifizierung öffentlicher Einrichtungen (Handbook of the Cabinet Office on the classification of Public Bodies), abrufbar unter folgendem Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf, sowie der erste Sitzungsbericht 2014–2015 des Sonderausschusses des Unterhauses für die öffentliche Verwaltung (Public Administration Select Committee), abrufbar unter folgenden Link: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

www.parlament.gv.at

(252) Die wesentlichen Aufgaben der Judicial Commissioners sind in Paragraf 229 IPA 2016[455] festgelegt. Insbesondere besitzen sie weitreichende Befugnisse zur Vorabgenehmigung, die zu den Garantien zählt, die mit dem IPA 2016 in den Rechtsrahmen des Vereinigten Königreichs eingeführt wurden. Anordnungen für gezieltes Abfangen, Gerätezugriffe, personenbezogene Massendatensätze, massenhaftes Abfangen von Kommunikationsdaten sowie Speicherungsanordnungen für Kommunikationsdaten müssen allesamt von den Judicial Commissioners genehmigt werden.[456] Ferner muss der IPC die Beschaffung von Kommunikationsdaten für Strafverfolgungszwecke stets im Voraus genehmigen.[457] Verweigert ein Commissioner die Genehmigung einer Anordnung, so kann der Secretary of State beim Investigatory Powers Commissioner Berufung einlegen, dessen Entscheidung endgültig ist.

(253) Der UN-Sonderberichterstatter über das Recht auf Privatheit hat die Einrichtung des Amts der Judicial Commissioners durch den IPA 2016 nachdrücklich begrüßt, da „alle sensibleren oder mit größeren Eingriffen verbundenen Ersuchen zur Durchführung von Überwachungsmaßnahmen sowohl von einem Kabinettsminister als auch vom Investigatory Powers Commissioner's Office genehmigt werden müssen“. Insbesondere betonte er, dass „dieses Element der gerichtlichen Überprüfung [durch die Rolle der IPC], die nunmehr durch ein besser ausgestattetes Team erfahrener Inspektoren und Technologieexperten unterstützt wird, eine der bedeutendsten neuen Garantien darstellt, die durch den IPA eingeführt wurden; durch den IPA wurde ein bislang zersplittertes System von Aufsichtsbehörden abgelöst und die Rolle des Ausschusses für Nachrichtendienste und Sicherheit (Intelligence and Security Committee) des Parlaments und des Gerichts für Ermittlungsbefugnisse (Investigatory Powers Tribunal) ergänzt.“[458]

(254) Darüber hinaus besitzt der IPC Befugnisse zur Ex-post-Aufsicht[459] über die Wahrnehmung von Ermittlungsbefugnissen gemäß dem IPA 2016, auch im Wege von Überprüfungen, Kontrollen und Untersuchungen, sowie einige andere in einschlägigen Rechtsvorschriften vorgesehene Befugnisse und Aufgaben[460]. Die Ergebnisse dieser

---

455 Nach Paragraf 229 IPA 2016 verfügt der Judicial Commissioner über weitreichende Kontrollbefugnisse, die auch die Überwachung der Speicherung und Offenlegung der von den Nachrichtendiensten erhobenen Daten umfassen.

456 Die Entscheidung darüber, ob eine Entscheidung des Secretary of State zur Erteilung einer Anordnung genehmigt wird, liegt bei den Judicial Commissioners selbst. Verweigert ein Commissioner die Genehmigung einer Anordnung, so kann der Secretary of State beim Investigatory Powers Commissioner Berufung einlegen, dessen Entscheidung endgültig ist.

457 Die Genehmigung des IPC ist immer dann erforderlich, wenn Kommunikationsdaten für Zwecke der Strafverfolgung beschafft werden (Paragraf 60A IPA 2016). Wenn Kommunikationsdaten für Zwecke der nationalen Sicherheit beschafft werden, kann die Genehmigung entweder durch den IPC oder durch einen benannten hohen Beamten der jeweiligen Behörde erteilt werden (siehe Paragrafen 61 und 61A IPA 2016 sowie Erwägungsgrund 203).

458 Erklärung des Sonderberichterstatters über das Recht auf Privatheit zum Abschluss seiner Mission im Vereinigten Königreich von Großbritannien und Nordirland (siehe Fußnote 281).

459 Paragraf 229 IPA 2016. Die Untersuchungs- und Informationsbefugnisse der Judicial Commissioners sind in Paragraf 235 IPA 2016 festgelegt.

460 Hierzu zählen Überwachungsmaßnahmen gemäß dem RIPA 2000, die Wahrnehmung von Aufgaben gemäß Teil 3 des Polizeigesetzes (Police Act) von 1997 (Genehmigung von Maßnahmen in Bezug auf Eigentum) und die Wahrnehmung von Aufgaben durch den Secretary of State gemäß den Paragrafen 5 bis 7 des Intelligence Services Act 1994 (Anordnungen des Zugriffs auf Funktelegrafie, des Betretens und des Zugriffs auf Eigentum) (Paragraf 229 IPA 2016).

www.parlament.gv.at

solchen Ex-post-Aufsicht sind Teil des Berichts, den der IPC jährlich erstellen und dem Premierminister zuleiten muss[461] und der veröffentlicht und dem Parlament vorgelegt werden muss[462]. Der Bericht enthält einschlägige Statistiken und Informationen über die Nutzung der Ermittlungsbefugnisse durch Nachrichtendienste und Strafverfolgungsbehörden sowie über die Anwendung der Garantien in Bezug auf Kommunikationsinhalte, die einem Rechtsprivileg unterliegen, vertrauliches journalistisches Material und Quellen für journalistische Informationen; ferner umfasst er Informationen über die getroffenen Vorkehrungen und die Einsatzzwecke, die im Zusammenhang mit Massenanordnungen geltend gemacht werden. Schließlich wird im Jahresbericht des IPCO erläutert, in welchen Bereichen Empfehlungen an die Behörden ergingen und wie diese umgesetzt wurden.[463]

(255) Gemäß Paragraf 231 IPA 2016 muss der IPC, wenn ihm bekannt wird, dass eine Behörde in der Ausübung ihrer Ermittlungsbefugnisse einen maßgeblichen Fehler begangen hat, die von diesem Fehler betroffene Person informieren, wenn er der Auffassung ist, dass der Fehler schwerwiegend ist und die Unterrichtung der Person im öffentlichen Interesse liegt.[464] Nach Paragraf 231 IPA 2016 muss der IPC bei der Unterrichtung einer Person über einen Fehler die Person insbesondere über ihre Rechte auf Anrufung des Investigatory Powers Tribunal informieren und die Einzelheiten des

---

461 Paragraf 230 IPA 2016. Der IPC kann dem Premierminister auch von sich aus über sämtliche Angelegenheiten berichten, die seine Aufgaben betreffen. Darüber hinaus muss der IPC dem Premierminister auf dessen Ersuchen Bericht erstatten, und der Premierminister kann den IPC anweisen, sämtliche Aufgaben der Nachrichtendienste zu überprüfen.

462 Einige Teile des Berichts können von der Veröffentlichung ausgeschlossen werden, wenn dadurch gegen nationale Sicherheitsinteressen verstoßen würde.

463 Im Jahresbericht 2019 des IPCO (Nummer 6.38) wird beispielsweise angeführt, dass dem MI5 empfohlen wurde, seine Verfahren zur Speicherung von personenbezogenen Massendatensätzen zu ändern; demnach hätte der MI5 einen Ansatz wählen sollen, bei dem für alle Felder solcher Massendatensätze sowie für jeden einzelnen Datensatz die Verhältnismäßigkeit einer Speicherung geprüft wird. Ende 2018 gelangte das IPCO zu dem Schluss, dass diese Empfehlung nicht umgesetzt worden war. Und im Bericht für 2019 wurde erklärt, dass der MI5 nun ein neues Verfahren einführt, um diese Anforderung zu erfüllen. Des Weiteren ist dem Jahresbericht 2019 (Nummer 8.22) zu entnehmen, dass den GHCQ eine Reihe von Empfehlungen bezüglich der Aufzeichnungen über die Verhältnismäßigkeit ihrer Abfragen von Massendaten ausgesprochen wurden. Im Bericht wird bestätigt, dass Ende 2018 Verbesserungen in diesem Bereich erzielt wurden. Jahresbericht 2019 des Investigatory Powers Commissioner Office, abrufbar unter folgendem Link: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Darüber hinaus wird jede IPCO-Kontrolle einer Behörde mit einem Bericht abgeschlossen, der der Behörde vorgelegt wird und alle Empfehlungen enthält, die sich aus dieser Kontrolle ergeben. Bei jeder nachfolgenden Kontrolle beginnt das IPCO dann mit einer Überprüfung etwaiger Empfehlungen der letzten Kontrolle und geht dann in dem neuen Kontrollbericht darauf ein, ob frühere Empfehlungen umgesetzt oder weitergeführt wurden.

464 Ein Fehler gilt als „schwerwiegend“ („serious“), wenn der Commissioner der Ansicht ist, dass die betroffene Person durch ihn einen erheblichen Nachteil oder Schaden erlitten hat (Paragraf 231 Absatz 2 IPA 2016). Im Jahr 2018 wurden 22 Fehler gemeldet, von denen acht als schwerwiegend eingestuft wurden und zu einer Unterrichtung der betroffenen Person führten. Siehe Jahresbericht 2018 des Investigatory Powers Commissioner Office, Anhang C, abrufbar unter folgendem Link: https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf. Im Jahr 2019 wurden 14 Fehler als schwerwiegend eingestuft. Siehe Jahresbericht 2019 des Investigatory Powers Commissioner Office, Anhang C, siehe Fußnote 463.

www.parlament.gv.at

Fehlers offenlegen, die nach Auffassung des Commissioner für die Ausübung dieser Rechte erforderlich sind und deren Offenlegung im öffentlichen Interesse liegt[465].

3.3.3.3 Parlamentarische Aufsicht über die Nachrichtendienste

(256) Die Rechtsgrundlage für die parlamentarische Aufsicht durch den Intelligence and Security Committee (ISC) bildet das Justiz- und Sicherheitsgesetz (Justice and Security Act) von 2013 (im Folgenden „JSA 2013“).[466] Durch das Gesetz wurde der ISC als Ausschuss des britischen Parlaments eingerichtet. 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 auf laufende Operationen beziehen[467]. In der gemeinsamen Absichtserklärung des Premierministers und des ISC[468] ist im Einzelnen dargelegt, welche Elemente zu berücksichtigen sind, wenn geprüft wird, ob eine Tätigkeit Teil einer laufenden Operation ist[469]. Der ISC kann zudem vom Premierminister zur Untersuchung laufender Operationen aufgefordert werden und von den Nachrichtendiensten freiwillig bereitgestellte Informationen überprüfen.

(257) Nach Anhang 1 des JSA 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.[470] Den Erläuterungen der britischen Behörden zufolge werden dem ISC in der Praxis nur sehr selten Informationen vorenthalten[471].

---

465 Nach Paragraf 231 IPA 2016 muss der IPC bei der Unterrichtung einer Person über einen Fehler die Einzelheiten offenlegen, die nach Auffassung des Commissioner für die Ausübung dieser Rechte erforderlich sind; dabei muss er insbesondere berücksichtigen, inwieweit die Offenlegung der Einzelheiten dem öffentlichen Interesse zuwiderlaufen oder die Verhütung oder Aufdeckung schwerer Straftaten, das wirtschaftliche Wohl des Vereinigten Königreichs oder die fortgesetzte Erfüllung der Aufgaben eines der Nachrichtendienste gefährden würde.

466 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 nationalen Interesse.

467 Paragraf 2 JSA 2013.

468 Absichtserklärung zwischen dem Premierminister und dem ISC, abrufbar unter folgendem Link: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

469 Absichtserklärung zwischen dem Premierminister und dem ISC, Nummer 14, siehe Fußnote 468.

470 Der Secretary of State darf der Offenlegung nur aus zwei Gründen widersprechen, nämlich im Falle sensibler Informationen, die gegenüber dem ISC aus Gründen der nationalen Sicherheit nicht offengelegt werden sollten, oder wenn die fraglichen Informationen so beschaffen sind, dass der Secretary of State es (nicht nur aus Gründen der nationalen Sicherheit) nicht für angemessen halten würde, sie bei entsprechender Aufforderung einem fachlichen Sonderausschuss des Unterhauses vorzulegen (Anhang 1 Nummer 4 Ziffer 2 des JSA 2013).

471 The UK Explanatory Framework for Adequacy Discussions, section H: National security, S. 43, siehe Fußnote 31.

www.parlament.gv.at

(258) Der ISC setzt sich aus Mitgliedern beider Kammern des Parlaments zusammen, die vom Premierminister nach Konsultation des Oppositionsführers ernannt werden.[472] Der ISC muss dem Parlament einen jährlichen Tätigkeitsbericht und weitere Berichte vorlegen, die er für angebracht hält.[473] Des Weiteren hat der ISC Anspruch darauf, alle drei Monate die Liste der Einsatzzwecke zu erhalten, anhand derer massenhaft erlangtes Material überprüft wird.[474] Der Premierminister übermittelt dem ISC Kopien der Untersuchungs-, Kontroll- und Überprüfungsberichte des Investigatory Powers Commissioner, wenn der Gegenstand der Berichte für die gesetzlichen Zuständigkeiten des Ausschusses relevant ist[475]. Schließlich kann der ISC den IPC auffordern, eine Untersuchung durchzuführen, und der IPC muss den ISC darüber unterrichten, ob eine solche Untersuchung durchgeführt wird[476].

(259) Des Weiteren lieferte der ISC Beiträge zum Entwurf des IPA 2016 und brachte eine Reihe von Änderung ein, die letztendlich in das Gesetz übernommen wurden.[477] Insbesondere empfahl der Ausschuss die Stärkung des Schutzes der Privatsphäre durch Einführung einer Reihe von Datenschutzbestimmungen, die für das gesamte Spektrum der Ermittlungsbefugnisse gelten.[478] Ferner schlug er Änderungen an den vorgeschlagenen Kapazitäten in Bezug auf Gerätezugriff, personenbezogene Massendatensätze und Kommunikationsdaten vor und forderte weitere spezifische

---

472 Paragraf 1 JSA 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.

473 Die Berichte und Stellungnahmen des Ausschusses sind online unter folgendem Link abrufbar: https://isc.independent.gov.uk/publications/. 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://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf) herausgegeben; darin befasste sich der Ausschuss mit dem Rechtsrahmen für die von den Nachrichtendiensten angewandten Überwachungsmethoden und sprach eine Reihe von Empfehlungen aus, die anschließend erörtert und in den Entwurf des Gesetzes über Ermittlungsbefugnisse aufgenommen wurden, der mit dem IPA 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.

474 Paragrafen 142, 161 und 183 IPA 2016.

475 Paragraf 234 IPA 2016.

476 Paragraf 236 IPA 2016.

477 Intelligence and Security Committee of Parliament, Report on the draft Investigatory Powers Bill, abrufbar unter folgendem Link: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

478 Diese allgemeinen Pflichten in Bezug auf den Schutz der Privatsphäre sind nun in Paragraf 2 Absatz 2 IPA 2016 festgelegt; demnach muss eine Behörde, die im Rahmen des IPA 2016 handelt, Folgendes berücksichtigen: ob das durch die Anordnung, die Genehmigung oder den Bescheid angestrebte Ziel nach vernünftigem Ermessen auch mit anderen, weniger stark eingreifenden Mitteln erreicht werden könnte; ob das Schutzniveau, das in Bezug auf die Beschaffung von Informationen aufgrund der Anordnung, der Genehmigung oder des Bescheids zugrunde zu legen ist, aufgrund der besonderen Sensibilität dieser Informationen höher ist; das öffentliche Interesse an der Integrität und Sicherheit von Telekommunikationssystemen und Postdiensten sowie alle anderen Aspekte des öffentlichen Interesses am Schutz der Privatsphäre.

www.parlament.gv.at

Änderungen, um die Beschränkungen und Garantien für die Nutzung von Ermittlungsbefugnissen zu stärken[479].

3.3.4 Rechtsbehelfe

(260) Im Bereich des staatlichen Zugriffs für Zwecke der nationalen Sicherheit müssen die betroffenen Personen die Möglichkeit haben, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung solcher Daten zu erwirken[480]. Eine solche gerichtliche Instanz muss insbesondere die Befugnis haben, gegenüber den Nachrichtendiensten verbindliche Entscheidungen zu treffen[481]. Wie in den Erwägungsgründen 261 bis 271 erläutert, verfügen betroffenen Personen im Vereinigten Königreich über eine Reihe von Möglichkeiten, um derartige Rechtsbehelfe einzulegen.

3.3.4.1 Rechtsbehelfsverfahren gemäß Teil 4 des DPA

(261) Gemäß Paragraf 165 DPA 2018 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 4 des DPA 2018 vorliegt. Der Information Commissioner hat die Befugnis, die Einhaltung des DPA 2018 durch den Verantwortlichen und den Auftragsverarbeiter zu bewerten und sie aufzufordern, notwendige Maßnahmen zu ergreifen. 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[482], auf Widerspruch gegen die Verarbeitung[483] und auf Berichtigung oder Löschung[484] nachzukommen.

(262) 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[485]. Als Schaden gilt sowohl ein finanzieller als auch ein nichtfinanzieller Schaden, wie z. B. seelisches Leid[486].

3.3.4.2 Rechtsbehelfsverfahren gemäß dem IPA 2016

(263) Natürliche Personen können bei Verstößen gegen den IPA 2016 vor dem Gericht für Ermittlungsbefugnisse (Investigatory Powers Tribunal) Rechtsbehelfe einlegen.

---

479 Beispielsweise wurde auf Antrag des ISC die Anzahl der Tage, die eine „dringende" („urgent") Anordnung bestehen kann, bevor der Judicial Commissioner sie genehmigen muss, von fünf auf drei Arbeitstage verringert, und der ISC erhielt die Befugnis, Angelegenheiten an den Investigatory Powers Commissioner zur Untersuchung zu verweisen.

480 *Schrems II*, Rn. 194.

481 *Schrems II*, Rn. 197.

482 Paragraf 94 Absatz 11 DPA 2018.

483 Paragraf 99 Absatz 4 DPA 2018.

484 Paragraf 100 Absatz 1 DPA 2018.

485 Nach Paragraf 169 DPA 2018 kann „eine Person, die aufgrund eines Verstoßes gegen eine Anforderung der Datenschutzvorschriften einen Schaden erleidet", Ansprüche geltend machen. Nach Angaben der britischen Behörden werden Ansprüche oder Beschwerden gegenüber den Nachrichtendiensten in der Praxis für gewöhnlich beim Investigatory Powers Tribunal eingereicht; dieses verfügt über weitreichende Zuständigkeiten, um Entschädigungen bzw. Schadensersatz zuerkennen, und erhebt keine Gebühren für die Einreichung einer Klage.

486 Paragraf 169 Absatz 5 DPA 2018.

www.parlament.gv.at

(264) Das Investigatory Powers Tribunal wurde durch den RIPA 2000 eingerichtet und ist unabhängig von der Exekutive[487]. Gemäß Paragraf 65 RIPA 2000 werden die Mitglieder des Tribunals von Ihrer Majestät für einen Zeitraum von fünf Jahren ernannt. Ein Mitglied des Tribunals kann von Ihrer Majestät nach einer Meinungsäußerung („Address“)[488] beider Kammern des Parlaments seines Amtes enthoben werden[489].

(265) Nach Paragraf 65 RIPA 2000 ist das Tribunal die zuständige gerichtliche Instanz für Beschwerden von Personen, die durch eine Handlung im Rahmen des IPA 2016 oder des RIPA 2000 oder durch das Verhalten eines Nachrichtendienstes geschädigt wurde[490].

(266) Möchte eine natürliche Person vor dem Investigatory Powers Tribunal Klage erheben („standing requirement“), so muss sie nach Paragraf 65 RIPA 2000 überzeugt sein[491], dass 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 stattgefunden haben[492]. Ferner muss der Beschwerdeführer Überzeugt sein, dass die Handlungen „unter anfechtbaren Umständen“ („challengeable circumstances“)[493] oder „durch oder im Namen der Nachrichtendienste ausgeführt wurden“ („to have been carried out by or on behalf of the intelligence services“)[494]. Da insbesondere dieses Kriterium der „Überzeugung“

---

487 Nach Anhang 3 des RIPA 2000 müssen die Mitglieder über fachspezifische richterliche Erfahrungen verfügen und können wiederernannt werden.

488 Eine „Address“ ist ein dem Parlament vorgelegter Antrag, mit dem dem Monarchen die Ansichten des Parlaments zu einem bestimmten Thema mitgeteilt werden sollen.

489 Anhang 3 Nummer 1 Ziffer 5 RIPA 2000.

490 Paragraf 65 Absatz 5 RIPA 2000.

491 Zum Kriterium der Prüfung der Überzeugung („belief“) siehe die Rechtssache Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH, Rn. 41. Darin 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.

492 Paragraf 65 Absatz 4 Buchstabe a RIPA 2000.

493 „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).

494 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 209 Beschwerden beim Tribunal eingingen; 52 % davon wurden als leichtfertig

www.parlament.gv.at

(„belief“) recht weit ausgelegt worden ist[495], sind die Anforderungen für eine Klageerhebung vor dem Tribunal niedrig.

(267) Prüft das Investigatory Powers 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[496]. Kommt es vor dem Tribunal zu einem Verfahren, so muss es bei seiner Entscheidungsfindung dieselben Grundsätze anwenden, die ein Gericht bei einer Anfechtungsklage zugrunde legen würde[497]. Darüber hinaus sind die Adressaten der Anordnungen oder Bescheide gemäß dem IPA 2016 und jede andere Person, die ein Amt unter der Krone innehat oder bei der Polizei oder dem Police Investigations and Review Commissioner tätig ist, verpflichtet, diesem Tribunal alle Dokumente und Informationen offenzulegen oder zur Verfügung zu stellen, die das Tribunal benötigt, um seine Zuständigkeit ausüben zu können[498].

(268) Das Investigatory Powers Tribunal muss dem Beschwerdeführer mitteilen, ob zu seinen Gunsten entschieden wurde oder nicht.[499] 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. Hierzu zählen unter anderem Beschlüsse zur Aufhebung oder Annullierung einer Anordnung oder einer Genehmigung sowie Beschlüsse zur Vernichtung von Aufzeichnungen über Informationen, die eine Person betreffen und in Ausübung einer durch eine Anordnung, eine Genehmigung oder einen Bescheid übertragenen Befugnis erlangt wurden oder sich anderweitig im Besitz einer Behörde befinden[500]. Nach

---

oder schikanös eingestuft, und bei 25 % wurden keine Feststellungen getroffen („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.

495 Siehe Rechtssache Human Rights Watch/Secretary of State [2016], UKIPTrib15_165-CH. Darin 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).

496 Paragraf 67 Absatz 3 RIPA 2000.

497 Paragraf 67 Absatz 2 RIPA 2000.

498 Paragraf 68 Absätze 6 und 7 RIPA 2000.

499 Paragraf 68 Absatz 4 RIPA 2000.

500 Ein Beispiel für die Anwendung dieser Befugnisse ist die Rechtssache Liberty & Others/the Security Service, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2. Darin entschied das Tribunal zugunsten von zwei Beschwerdeführern: in einem Fall, weil ihre Kommunikation über die vorgegebenen Grenzen hinaus gespeichert wurde, im anderen Fall, weil das in den internen Regeln der GCHQ festgelegte

www.parlament.gv.at

Paragraf 67A RIPA 2000 kann gegen eine Entscheidung des Tribunals Berufung eingelegt werden, sofern das Tribunal oder das zuständige Berufungsgericht seine Erlaubnis erteilt.

(269) Abschließend sei darauf hingewiesen, dass die Rolle des Investigatory Powers Tribunal auch mehrfach im Rahmen von Klagen vor dem Europäischen Gerichtshof für Menschenrechte erörtert wurde, insbesondere in der Rechtssache Kennedy/the United Kingdom[501] und zuletzt in der Rechtssache Big Brother Watch and others/United Kingdom[502]; darin erklärte der Gerichtshof, dass „sich das Investigatory Powers Tribunal als eine robuste Rechtsbehelfsinstanz für jeden erwiesen hat, der den Verdacht hat, dass seine Kommunikation durch Nachrichtendienste abgefangen wird“[503].

3.3.4.3 Sonstige Rechtsbehelfsverfahren

(270) Wie in den Erwägungsgründen 109 bis 111 erläutert, stehen auch im Bereich der nationalen Sicherheit Rechtsbehelfe nach dem Human Rights Act 1998 und vor dem des Europäischen Gerichtshof für Menschenrechte[504] zur Verfügung. Nach Paragraf 65 Absatz 2 RIPA 2000 besitzt das Investigatory Powers Tribunal die ausschließliche Zuständigkeit für alle auf der Grundlage des Human Rights Act gegen Nachrichtendienste erhobenen Klagen.[505] 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 Tribunal selbst bei einem zuständigen Berufungsgericht (in England und Wales wäre das der Court of Appeal) ein Rechtsmittel eingelegt werden kann und dass der Supreme Court unlängst entschieden hat, dass das Tribunal grundsätzlich Gegenstand einer gerichtlichen Überprüfung sein kann: siehe R (Privacy International)/Investigatory Powers Tribunal, [2019] UKSC 22; [2019] 2 WLR 1219“[506].

(271) Aufgrund der vorstehenden Ausführungen lässt sich Folgendes festhalten: Der Zugriff britischer Strafverfolgungsbehörden oder nationaler Sicherheitsbehörden auf personenbezogene Daten, die in den Anwendungsbereich des vorliegenden

---

Überprüfungsverfahren nicht eingehalten wurde. Im ersten Fall wies das Gericht die Nachrichtendienste an, die Kommunikationsvorgänge, die länger als den maßgeblichen Zeitraum gespeichert waren, zu vernichten. Im zweiten Fall wurde keine Vernichtung angeordnet, da die Kommunikation nicht gespeichert worden war.

501 *Kennedy,* siehe Fußnote 129.

502 Europäischer Gerichtshof für Menschenrechte (Große Kammer), Big Brother Watch u. a./Vereinigtes Königreich (siehe oben, Fn. 268), Rn. 413 und 415.

503 Europäischer Gerichtshof für Menschenrecht, Big Brother Watch, Rn. 425.

504 Wie beispielsweise das kürzlich ergangene Urteil der Großen Kammer des Europäischen Gerichtshofs für Menschenrechte in der Rechtssache Big Brother Watch u. a./Vereinigtes Königreich (siehe Fußnote 279) zeigt, ermöglicht dies eine wirksame gerichtliche Kontrolle – ähnlich derjenigen, der EU-Mitgliedstaaten unterliegen – durch ein internationales Gericht in Bezug auf die Einhaltung der Grundrechte durch Behörden beim Zugang zu personenbezogenen Daten. Darüber hinaus unterliegt die Vollstreckung der Urteile des Europäischen Gerichtshofs für Menschenrechte einer besonderen Aufsicht durch den Europarat.

505 In Belhaj & others, [2017] UKSC 3, stützte sich die Feststellung der Rechtswidrigkeit des Abfangens von einem Rechtsprivileg unterliegendem Material direkt auf Artikel 8 EMRK (siehe Feststellung 11).

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

www.parlament.gv.at

Beschlusses fallen, wird durch Gesetze geregelt, mit denen die Bedingungen für den Zugriff festgelegt werden und sichergestellt wird, dass der Zugriff und die weitere Verwendung der Daten auf das beschränkt sind, was im Hinblick auf das verfolgte Ziel im Bereich der Strafverfolgung oder nationalen Sicherheit notwendig und angemessen ist. Darüber hinaus unterliegt ein solcher Zugriff in den meisten Fällen der vorherigen Genehmigung durch ein Justizorgan – und zwar durch Genehmigung einer allgemeinen Anordnung oder einer Herausgabeanordnung – und in jedem Fall einer unabhängigen Aufsicht. Sobald Behörden Zugriff auf Daten haben, unterliegt deren Verarbeitung, darunter auch der weitere Austausch und die Weiterübermittlung dieser Daten, besonderen Datenschutzgarantien gemäß Teil 3 des DPA 2018 (die den Garantien der Richtlinie (EU) 2016/680 entsprechen) für die Verarbeitung durch Strafverfolgungsbehörden und gemäß Teil 4 des DPA 2018 für die Verarbeitung durch Nachrichtendienste. Schließlich stehen betroffenen Personen in diesem Bereich wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung, einschließlich des Rechts auf Auskunft über ihre Daten oder auf deren Berichtigung oder Löschung.

(272) Angesichts der Bedeutung solcher Bedingungen, Einschränkungen und Garantien für die Zwecke dieses Beschlusses wird die Kommission die Anwendung und Auslegung der britischen Vorschriften über den Zugang der Regierung zu Daten genau überwachen. Dazu gehören einschlägige Entwicklungen in den Bereichen Gesetzgebung, Regulierung und Rechtsprechung sowie die Tätigkeiten des ICO und anderer Aufsichtsbehörden in diesem Bereich. Besondere Aufmerksamkeit wird auch der Umsetzung einschlägiger Urteile des Europäischen Gerichtshofs für Menschenrechte durch das Vereinigte Königreich gewidmet, einschließlich der Maßnahmen, die in den „Aktionsplänen“ und „Aktionsberichten“ aufgeführt sind, die dem Ministerkomitee im Rahmen der Überwachung der Einhaltung der Urteile des Gerichtshofs vorgelegt werden.

4. SCHLUSSFOLGERUNG

(273) Die Kommission ist der Ansicht, dass die UK GDPR und der DPA 2018 ein Schutzniveau für aus der Europäischen Union übermittelte personenbezogene Daten gewährleisten, das der Sache nach dem durch die Verordnung (EU) 2016/679 garantierten Schutzniveau gleichwertig ist.

(274) 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.

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

(276) Daher sollte in Anbetracht der Feststellungen dieses Beschlusses beschlossen werden, dass das Vereinigte Königreich ein angemessenes Schutzniveau im Sinne von

www.parlament.gv.at

Artikel 45 der Verordnung (EU) 2016/679 gemäß seiner Auslegung im Lichte der Charta der Grundrechte der Europäischen Union gewährleistet.

(277) 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.

5. AUSWIRKUNGEN DIESES BESCHLUSSES UND MAßNAHMEN DER DATENSCHUTZBEHÖRDEN

(278) 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.

(279) Daher ist ein nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlassener Angemessenheitsbeschluss der Kommission für alle Organe der Mitgliedstaaten, an die er gerichtet ist, einschließlich ihrer unabhängigen Aufsichtsbehörden, verbindlich. Insbesondere können während der Geltungsdauer dieses Beschlusses Übermittlungen von einem Verantwortlichen oder Auftragsverarbeiter in der Europäischen Union an Verantwortliche oder Auftragsverarbeiter im Vereinigten Königreich erfolgen, ohne dass eine weitere Genehmigung eingeholt werden muss.

(280) Es sei daran erinnert, dass gemäß Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 und wie vom Gerichtshof im Urteil in der Rechtssache Schrems erläutert[507] 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.[508]

6. ÜBERWACHUNG, AUSSETZUNG, AUFHEBUNG ODER ÄNDERUNG DIESES BESCHLUSSES

(281) Gemäß Artikel 45 Absatz 4 der Verordnung (EU) 2016/679 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

---

507 *Schrems*, Rn. 65.

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

www.parlament.gv.at

durchsetzen wird, die nicht mehr dem Recht der Europäischen Union unterliegt und sich möglicherweise weiterentwickeln wird. In diesem Zusammenhang gilt die besondere Aufmerksamkeit der praktischen Anwendung der Vorschriften des Vereinigten Königreichs über die Übermittlung personenbezogener Daten an Drittländer und deren möglichen Auswirkungen auf das Schutzniveau für die im Rahmen dieses Beschlusses übermittelten Daten; der Wirksamkeit der Ausübung individueller Rechte, einschließlich einschlägiger rechtlicher und praktischer Entwicklungen in Bezug auf Ausnahmen oder Beschränkungen dieser Rechte (insbesondere im Zusammenhang mit der Aufrechterhaltung einer wirksamen Einwanderungskontrolle); sowie der Einhaltung der Beschränkungen und Garantien in Bezug auf den Zugang der Regierung. Unter anderem wird die Kommission Entwicklungen in der Rechtsprechung sowie die Aufsicht durch das ICO und andere unabhängige Stellen in ihre Überwachung einfließen lassen.

(282) Um diese Überwachung zu erleichtern, sollten die Behörden des Vereinigten Königreichs die Kommission unverzüglich über jede wesentliche Änderung der Rechtsordnung des Vereinigten Königreichs unterrichten, 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, sowohl was die Verarbeitung personenbezogener Daten durch Verantwortliche und Auftragsverarbeiter im Rahmen der DSGVO des Vereinigten Königreichs als auch die Beschränkungen und Garantien für den Zugang der Behörden zu personenbezogenen Daten anbelangt. Dies sollte auch Entwicklungen in Bezug auf die in Erwägungsgrund 281 genannten Elemente einschließen.

(283) Damit die Kommission ihre Kontrollfunktion 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 Verantwortliche oder Auftragsverarbeiter 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 oder für die nationale Sicherheit zuständig sind, einschließlich der Aufsichtsbehörden, nicht das erforderliche Schutzniveau gewährleisten.

(284) Lassen verfügbare Informationen – insbesondere Informationen, die sich aus der Überwachung dieses Beschlusses ergeben oder von den Behörden des Vereinigten Königreichs oder der 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. Dieser Zeitraum kann erforderlichenfalls um einen bestimmten Zeitraum verlängert werden, wobei die Art des Problems und/oder die zu treffenden Maßnahmen zu berücksichtigen sind. Ein solches Verfahren würde beispielsweise in Fällen eingeleitet, in denen Weiterübermittlungen – auch auf der Grundlage neuer, vom Secretary of State erlassener Angemessenheitsvorschriften oder vom Vereinigten Königreich geschlossener internationaler Übereinkünfte – nicht mehr im Rahmen der Garantien erfolgen würden, die die Kontinuität des Schutzes im Sinne des Artikel 44 der Verordnung (EU) 2016/679 gewährleisten.

www.parlament.gv.at

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

(286) 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.

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

7. GELTUNGSDAUER UND VERLÄNGERUNG DIESES BESCHLUSSES

(288) Die Kommission muss 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.

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

(290) 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 93 Absatz 2 der Verordnung (EU) 2016/679 genannten Verfahren zu erlassen.

8. SCHLUSSBEMERKUNGEN

(291) Der Europäische Datenschutzausschuss hat seine Stellungnahme[509] veröffentlicht, der bei der Ausarbeitung dieses Beschlusses Rechnung getragen wurde.

---

509 Stellungnahme 14/2021 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

www.parlament.gv.at

(292) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 93 der Verordnung (EU) 2016/679 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

(1) Für die Zwecke des Artikels 45 der Verordnung (EU) 2016/679 gewährleistet das Vereinigte Königreich ein angemessenes Schutzniveau für personenbezogene Daten, die im Rahmen der Verordnung (EU) 2016/679 aus der Europäischen Union an das Vereinigte Königreich übermittelt werden.

(2) Dieser Beschluss gilt nicht für personenbezogene Daten, die für Zwecke der Einwanderungskontrolle des Vereinigten Königreichs übermittelt werden oder anderweitig in den Geltungsbereich der Ausnahme von bestimmten Rechten betroffener Personen für die Zwecke der Aufrechterhaltung einer wirksamen Einwanderungskontrolle gemäß Anhang 2 Paragraf 4 Absatz 1 DPA 2018 fallen.

Artikel 2

Üben die zuständigen Überwachungsbehörden in den Mitgliedstaaten zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ihre Befugnisse nach Artikel 58 der Verordnung (EU) 2016/679 im Hinblick auf die Übermittlung von Daten 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 werden, individuelle Rechte ausgeübt werden und die Behörden des Vereinigten Königreichs Zugang zu Daten haben, die auf der Grundlage dieses Beschlusses übermittelt 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 Absatz 1 berührt ist.

www.parlament.gv.at

Artikel 4

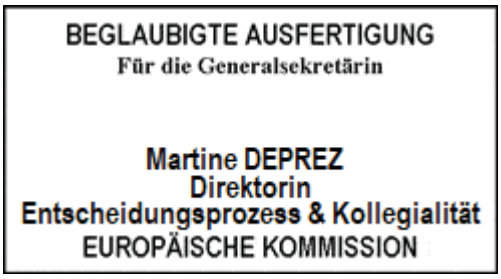
Die Geltungsdauer dieses Beschlusses endet am 27. Juni 2025, sofern sie nicht nach dem in Artikel 93 Absatz 2 der Verordnung (EU) 2016/679 genannten Verfahren verlängert wird.

Artikel 5

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 28.6.2021

Für die Kommission
Didier REYNDERS
Mitglied der Kommission



www.parlament.gv.at