II

(Ikke-lovgivningsmæssige retsakter)

AFGØRELSER

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2021/1772

af 28. juni 2021

i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Det Forenede Kongerige

(meddelt under nummer C(2021) 4800)

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) ([1]), særlig artikel 45, stk. 3, og

ud fra følgende betragtninger:

1. INDLEDNING

(1) I forordning (EU) 2016/679 fastsættes reglerne for overførsel af personoplysninger fra en dataansvarlig eller databehandler i Den Europæiske Union til tredjelande og internationale organisationer, i det omfang overførslen falder inden for forordningens anvendelsesområde. Reglerne om internationale overførsler af oplysninger er fastsat i kapitel V i nævnte forordning, dvs. i artikel 44-50. Strømmen af personoplysninger til og fra lande uden for Den Europæiske Union er afgørende for udvidelsen af det internationale samarbejde og den grænseoverskridende handel, men niveauet for beskyttelse af personoplysninger i Den Europæiske Union må ikke undermineres af overførsler til tredjelande ([2]).

(2) I henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 kan Kommissionen ved hjælp af en gennemførelsesretsakt fastslå, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau. På denne betingelse kan overførsel af personoplysninger til et tredjeland finde sted uden yderligere godkendelse, jf. artikel 45, stk. 1, og betragtning 103 i nævnte forordning.

(3) Som omhandlet i artikel 45, stk. 2, i forordning (EU) 2016/679 skal vedtagelsen af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet finde sted på grundlag af en omfattende analyse af det pågældende tredjelands retsorden, både hvad angår de regler, der finder anvendelse på dataimportøren, og de begrænsninger og garantier, der gælder med hensyn til offentlige myndigheders adgang til personoplysninger. I sin vurdering skal Kommissionen fastslå, om det pågældende tredjeland sikrer et beskyttelsesniveau, som »i det væsentlige svarer« til det, der sikres i Den Europæiske Union (betragtning 104 i forordning (EU) 2016/679). Den standard, som dette væsentlighedskriterium vurderes på grundlag af, er den, der er fastsat i EU-lovgivningen, navnlig forordning (EU) 2016/679, samt Den Europæiske Unions Domstols retspraksis ([3]). Det Europæiske Databeskyttelsesråds reference vedrørende et tilstrækkeligt beskyttelsesniveau er også af betydning i denne henseende ([4]).

([1]) EUT L 119 af 4.5.2016, s. 1.
([2]) Se betragtning 101 i forordning (EU) 2016/679.
([3]) Se senest sag C-311/18, Facebook Ireland og Schrems (»Schrems II«) ECLI:EU:C:2020:559.
([4]) Det Europæiske Databeskyttelsesråd, Adequacy Referential, WP 254 rev. 01. Kan findes på følgende link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Som Den Europæiske Unions Domstol har præciseret, kræves der ikke et identisk beskyttelsesniveau ([5]). Det betyder navnlig, at de midler, som tredjelandet anvender til at beskytte personoplysninger, kan være forskellige fra de midler, som gennemføres inden for Den Europæiske Union, så længe de i praksis viser sig at være effektive med henblik på at sikre et tilstrækkeligt beskyttelsesniveau ([6]). Standarden for tilstrækkelighed er derfor ikke, at EU-reglerne duplikeres punkt for punkt. Testen består snarere i, om det pågældende udenlandske system som helhed sikrer det krævede beskyttelsesniveau gennem kerneindholdet i retten til databeskyttelse og den effektive gennemførelse, overvågning og håndhævelse heraf ([7]).

(5) Kommissionen har gennemgået Det Forenede Kongeriges lovgivning og praksis omhyggeligt. På grundlag af konklusionerne i betragtning 8 til 270 konkluderer Kommissionen, at Det Forenede Kongerige sikrer tilstrækkelig beskyttelse af personoplysninger, som inden for rammerne af forordning (EU) 2016/679 overføres fra Den Europæiske Union til Det Forenede Kongerige.

(6) Denne konklusion vedrører ikke personoplysninger, der videregives med henblik på indvandringskontrol i Det Forenede Kongerige, eller som på anden måde falder ind under anvendelsesområdet for undtagelsen fra visse registreredes rettigheder med henblik på opretholdelse af en effektiv indvandringskontrol (»den indvandringsrelaterede undtagelse«) i henhold til paragraph 4(1) i Schedule 2 til UK Data Protection Act. Gyldigheden og fortolkningen af den indvandringsrelaterede undtagelse i henhold til britisk ret er ikke fastlagt efter en afgørelse truffet af appelretten i England og Wales den 26. maj 2021. Selv om appeldomstolen anerkender, at registreredes rettigheder i princippet kan begrænses i forbindelse med indvandringskontrol af hensyn til vigtige samfundsinteresser, har den konkluderet, at den indvandringsrelaterede undtagelse i sin nuværende form er uforenelig med britisk ret, da den lovgivningsmæssige foranstaltning ikke er knyttet til specifikke bestemmelser, der fastsætter de garantier, der er anført i artikel 23, stk. 2, i Det Forenede Kongeriges generelle forordning om databeskyttelse (UK GDPR) ([8]). Under disse omstændigheder bør overførsel af personoplysninger fra Unionen til Det Forenede Kongerige som underlagt den indvandringsrelaterede undtagelse udelukkes fra denne afgørelses anvendelsesområde ([9]). Når uoverensstemmelsen med britisk ret er afhjulpet, bør den indvandringsrelaterede undtagelse tages op til fornyet vurdering, og det samme gælder behovet for at opretholde begrænsningen af denne afgørelses anvendelsesområde.

(7) Denne afgørelse bør ikke berøre den direkte anvendelse af forordning (EU) 2016/679 på organisationer, der er etableret i Det Forenede Kongerige, hvis betingelserne vedrørende forordningens territoriale anvendelsesområde, jf. forordningens artikel 3, er opfyldt.

2. REGLER FOR BEHANDLING AF PERSONOPLYSNINGER

2.1. De forfatningsmæssige rammer

(8) Det Forenede Kongerige er et parlamentarisk demokrati, der har en konstitutionel monark som statsoverhoved. Det har et suverænt parlament, som rangerer over alle andre statslige institutioner, en udøvende magt, der er udvalgt fra og ansvarlig over for parlamentet og et uafhængigt retsvæsen. Den udøvende magts myndighed bygger på tilliden til den i Underhuset, som er folkevalgt, og den er ansvarlig over for begge kamre i parlamentet, som har ansvaret for at kontrollere regeringen og drøfte og vedtage lovgivning.

([5]) Sag C-362/14, Schrems (»Schrems I«), ECLI:EU:C:2015:650, præmis 73.

([6]) Schrems I-dommen, præmis 74.

([7]) Se meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden, COM (2017)7 af 10.1.2017, afsnit 3.1, s. 6-7, som kan findes på følgende link: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

([8]) Appeldomstolen (Court of Appeal) (afdelingen for civile sager), Open Rights Group mod Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport, [2021] EWCA Civ 800, præmis 53 til 56. Appeldomstolen omstødte afgørelsen truffet af retten i første instans (High Court of Justice), som tidligere havde vurderet undtagelsen i lyset af forordning (EU) 2016/679 (navnlig artikel 23) og Den Europæiske Unions charter om grundlæggende rettigheder, og fastslog, at undtagelsen var lovlig (Open Rights Group & Anor, R (On the Application Of) mod Secretary of State for the Home Department & Anor [2019] EWHC 2562).

([9]) Forudsat at de gældende betingelser er opfyldt, kan videregivelse med henblik på indvandringskontrol i Det Forenede Kongerige foretages på grundlag af de overførselsmekanismer, der er fastsat i artikel 46 til 49 i forordning (EU) 2016/679.

(9) Det Forenede Kongeriges parlament har givet det skotske parlament, det walisiske parlament (Senedd Cymru) og Nordirlands parlament ansvaret for lovgivning om nationale anliggender i henholdsvis Skotland, Wales og Nordirland, som Det Forenede Kongeriges parlament ikke har forbeholdt sig selv. Databeskyttelse er et forbeholdt anliggende, hvilket vil sige, at den samme lovgivning gælder i hele landet, mens andre politikområder af relevans for denne afgørelse er blevet overdraget. Eksempelvis er de strafferetlige systemer, herunder politiarbejdet, i Skotland og Nordirland blevet overdraget til henholdsvis det skotske parlament og Nordirlands forsamling. Det Forenede Kongerige har ikke en kodificeret forfatning i form af en grundfæstet retsakt om oprettelse. Der er med tiden opstået forfatningsmæssige principper, der navnlig er baseret på retspraksis og konventioner. Domstolene har anerkendt den forfatningsmæssige værdi, der ligger i visse love, såsom Magna Carta, Bill of Rights 1689 (lov om rettigheder) og Human Rights Act 1998 (lov om menneskerettigheder). Enkeltpersoners grundlæggende rettigheder er som en del af forfatningen blevet udviklet gennem sædvaneret, ovennævnte love og internationale traktater, navnlig den europæiske menneskerettighedskonvention (EMRK), som Det Forenede Kongerige ratificerede i 1951. I 1987 ratificerede Det Forenede Kongerige desuden Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108) ([10]).

(10) Med menneskerettighedsloven Human Rights Act 1998 blev rettighederne i den europæiske menneskerettighedskonvention indarbejdet i Det Forenede Kongeriges lovgivning. Loven indrømmer enhver person de grundlæggende rettigheder og friheder, der er fastsat i artikel 2-12 og artikel 14 i den europæiske menneskerettighedskonvention, i artikel 1, 2 og 3 i dens første protokol og i artikel 1 i dens trettende protokol, sammenholdt med konventionens artikel 16, 17 og 18. Disse rettigheder omfatter retten til respekt for privatliv og familieliv (og retten til databeskyttelse som en del af denne ret) samt retten til en retfærdig rettergang ([11]). I henhold til konventionens artikel 8 må en offentlig myndighed navnlig kun gribe ind i retten til privatlivets fred i overensstemmelse med loven, hvis det er nødvendigt i et demokratisk samfund af hensyn til statens sikkerhed, den offentlige sikkerhed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelser, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder.

(11) I henhold til Human Rights Act 1998 skal enhver handling fra offentlige myndigheders side være forenelig med en konventionsrettighed ([12]). Desuden skal primær og underordnet lovgivning læses og gennemføres på en måde, der er forenelig med rettighederne i konventionen ([13]).

2.2. **Det Forenede Kongeriges databeskyttelsesramme**

(12) Det Forenede Kongerige udtrådte af Den Europæiske Union den 31. januar 2020. På grundlag af aftalen om Det Forenede Kongerige Storbritannien og Nordirlands udtræden af Den Europæiske Union og Det Europæiske Atomenergifællesskab ([14]) fandt EU-retten fortsat anvendelse i Det Forenede Kongerige i overgangsperioden frem til den 31. december 2020. Forud for udtrædelsen og i overgangsperioden bestod den lovgivningsmæssige ramme for beskyttelse af personoplysninger i Det Forenede Kongerige af den relevante EU-lovgivning (navnlig forordning (EU) 2016/679 og Europa-Parlamentets og Rådets direktiv (EU) 2016/680 ([15])) samt national lovgivning, navnlig Data Protection Act 2018 (DPA 2018) ([16]), som i det omfang, det var tilladt i henhold til forordning (EU) 2016/679, fastsatte nationale regler med præcisering og begrænsning af anvendelsen af bestemmelserne i forordning (EU) 2016/679 og gennemførte direktiv (EU) 2016/680.

([10]) Principperne i konvention 108 blev oprindeligt gennemført i Det Forenede Kongeriges lovgivning ved hjælp af Data Protection Act fra 1984, som blev erstattet af DPA 1998 og derefter af DPA 2018 (sammenholdt med UK GDPR). I 2018 har Det Forenede Kongerige desuden undertegnet protokollen om ændring af konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (kendt som konvention 108+), og landet arbejder i øjeblikket på ratificeringen af konventionen.

([11]) Artikel 6 og 8 i EMRK (se også Schedule 1 til Human Rights Act 1998).

([12]) Section 6 i Human Rights Act 1998.

([13]) Section 3 i Human Rights Act 1998.

([14]) Aftale om Det Forenede Kongerige Storbritannien og Nordirlands udtræden af Den Europæiske Union og Det Europæiske Atomenergifællesskab (2019/C 384 I/01), XT/21054/2019/INIT (EUT C 384I af 12.11.2019, s. 1), der kan findes på følgende link: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=DA.

([15]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89), som kan findes på følgende link: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016L0680&from=DA.

([16]) Data Protection Act 2018, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(13) Som forberedelse på Det Forenede Kongeriges udtræden af Den Europæiske Union har landets regering vedtaget European Union (Withdrawal) Act 2018 ([17]), som indarbejder umiddelbart gældende EU-ret i kongerigets lovgivning ([18]). Denne »bibeholdte EU-ret« omfatter forordning (EU) 2016/679 i sin helhed (herunder betragtningerne) ([19]). I overensstemmelse med denne retsakt skal domstolene i Det Forenede Kongerige fortolke den uændrede bibeholdte EU-ret i overensstemmelse med EU-Domstolens relevante retspraksis og de generelle principper i EU-retten, da de har virkning umiddelbart før overgangsperiodens udløb (henholdsvis »bibeholdt EU-retspraksis« og »bibeholdte generelle principper i EU-retten«) ([20]).

(14) I henhold til European Union (Withdrawal) Act 2018 har Det Forenede Kongeriges ministre beføjelse til at indføre afledt ret gennem retsakter for at foretage de ændringer, der er nødvendige for at bibeholde EU-retten som følge af Det Forenede Kongeriges udtræden af Den Europæiske Union. De udøvede denne beføjelse ved at vedtage Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (bestemmelser om beskyttelse af data, personoplysninger og elektronisk kommunikation i forbindelse med udtræden af EU fra 2019) (DPPEC-bestemmelserne) ([21]). DPPEC-bestemmelserne ændrer forordning (EU) 2016/679 som introduceret i Det Forenede Kongeriges lovgivning gennem European Union (Withdrawal) Act 2018, databeskyttelsesloven (DPA 2018) og anden lovgivning om databeskyttelse af relevans for den indenlandske kontekst ([22]).

(15) Efter overgangsperiodens udløb består de retlige rammer for beskyttelse af personoplysninger i Det Forenede Kongerige derfor af følgende:

— UK GDPR som indarbejdet i Det Forenede Kongeriges lovgivning i henhold til European Union (Withdrawal) Act 2018 og som ændret ved DPPEC-bestemmelserne ([23])

— DPA 2018 ([24]) som ændret ved DPPEC-bestemmelserne.

(16) Da UK GDPR er baseret på EU-ret, afspejler databeskyttelsesreglerne i Det Forenede Kongerige i mange henseender de tilsvarende regler, der gælder i Den Europæiske Union.

(17) Ud over de beføjelser, der er tillagt Secretary of State ved European Union (Withdrawal) Act 2018, giver flere bestemmelser i DPA 2018 ministeriet beføjelse til at vedtage afledt ret med henblik på at ændre visse bestemmelser i loven eller fastsætte supplerende regler ([25]). Secretary of State har hidtil kun udøvet beføjelsen i henhold til Section

([17]) European Union Withdrawal Act 2018, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) Hensigten med European Union (Withdrawal) Act 2018 og dennes virkning er, at al direkte EU-ret, som var indarbejdet i Det Forenede Kongeriges lovgivning ved overgangsperiodens udløb, indarbejdes i Det Forenede Kongeriges lovgivning, da den har virkning i EU-retten umiddelbart inden overgangsperiodens udløb, se Section 3 i European Union (Withdrawal) Act 2018.

([19]) I de forklarende bemærkninger til European Union (Withdrawal) Act 2018 præciseres det, at »når lovgivningen omdannes i henhold til denne artikel, er det selve lovteksten, der vil udgøre en del af den nationale lovgivning. Dette gælder hele teksten i ethvert EU-instrument (herunder betragtningerne)». (Forklarende bemærkninger til European Union (Withdrawal) Act 2018, paragraph 83, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). De britiske myndigheder anfører, at det ikke var nødvendigt at ændre betragtningerne på samme måde, som artiklerne i forordning (EU) 2016/679 er blevet ændret ved DPPEC-bestemmelserne, da betragtningerne ikke har status af bindende retlige regler.

([20]) Section 6 i European Union (Withdrawal) Act 2018.

([21]) Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, som kan findes på følgende link: https://www.legislation.gov.uk/uksi/2019/419/contents/made, som ændret ved DPPEC Regulations 2020, der kan findes på følgende link: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Disse ændringer af UK GDPR og DPA 2018 er hovedsagelig af teknisk art og består bl.a. i at slette henvisningerne til »medlemsstater« og tilpasse terminologien, f.eks. erstatte henvisningerne til forordning (EU) 2016/679 med henvisninger til UK GDPR. I nogle tilfælde har der været behov for ændringer for at afspejle bestemmelsernes rent nationale kontekst, f.eks. med hensyn til, »hvem» der vedtager »bestemmelser om tilstrækkelighed« med henblik på Det Forenede Kongeriges retlige ramme for databeskyttelse (se Section 17A i DPA 2018), dvs. Secretary of State i stedet for Europa-Kommissionen.

([23]) General Data Protection Regulation, Keeling Schedule, som kan findes på følgende 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, som kan findes på følgende 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]) Sådanne beføjelser er f.eks. indeholdt i Section 16 (beføjelse til i særlige snævert afgrænsede situationer at gøre yderligere undtagelser fra specifikke bestemmelser i UK GDPR), 17A (beføjelse til at vedtage bestemmelser om tilstrækkeligheden af beskyttelsesniveauet), 212 og 213 (beføjelser til at iværksætte lovgivning og fastsætte overgangsbestemmelser) og 211 (beføjelse til at foretage mindre ændringer og konsekvensændringer) i DPA 2018.

137 i DPA 2018 til at vedtage Data Protection (Charges and Information) (Amendment) Regulations 2019, som fastsætter de omstændigheder, hvorunder de dataansvarlige skal betale en årlig afgift til Det Forenede Kongeriges uafhængige databeskyttelsesmyndighed, Information Commissioner (ICO).

(18) Endelig findes der yderligere vejledning om Det Forenede Kongeriges databeskyttelseslovgivning i de adfærdskodekser og andre retningslinjer, som Information Commissioner har vedtaget. Selv om denne vejledning rent formelt ikke er juridisk bindende, har den fortolkningsmæssig vægt, og den viser, hvordan databeskyttelseslovgivningen finder anvendelse og håndhæves af Information Commissioner i praksis. Navnlig gælder det, at Information Commissioner i henhold til Section 121 til 125 i DPA 2018 skal udarbejde adfærdskodekser for datadeling, direkte markedsføring, aldersmæssigt passende design samt databeskyttelse og journalistik.

(19) Med hensyn til opbygning og hovedkomponenter svarer Det Forenede Kongeriges retlige ramme, der finder anvendelse på oplysninger, som overføres i henhold til denne afgørelse, således meget til den, der gælder i Den Europæiske Union. For eksempel er rammen ikke kun baseret på forpligtelser, der er fastsat i national ret, og som er formet af EU-retten, men også på forpligtelser, der er nedfældet i folkeretten, navnlig gennem Det Forenede Kongeriges tiltrædelse af EMRK og konvention 108. Desuden anerkendes Den Europæiske Menneskerettighedsdomstols kompetence. De nævnte forpligtelser, der følger af retligt bindende internationale instrumenter, navnlig vedrørende beskyttelse af personoplysninger, er derfor et særligt vigtigt element i de retlige rammer, der vurderes i denne afgørelse.

2.3. **Materielt og territorialt anvendelsesområde**

(20) I lighed med forordning (EU) 2016/679 finder UK GDPR anvendelse på behandling af personoplysninger, der helt eller delvist foretages automatisk, eller på anden behandling, hvis personoplysningerne er en del af et register ([26]). Definitionerne af »personoplysninger«, »den registrerede« og »behandling« i UK GDPR er identiske med definitionerne i forordning (EU) 2016/679 ([27]). Desuden finder UK GDPR anvendelse på manuel behandling af ustrukturerede personoplysninger ([28]), som visse offentlige myndigheder i Det Forenede Kongerige er i besiddelse af ([29]), idet de principper og rettigheder i UK GDPR, der ikke er relevante for sådanne personoplysninger, ikke anvendes i henhold til Section 24 og 25 i DPA 2018. Ligesom det er fastsat i forordning (EU) 2016/679, finder UK GDPR ikke anvendelse på en persons behandling af personoplysninger i forbindelse med rent personlige eller familiemæssige aktiviteter ([30]).

(21) UK GDPR's anvendelsesområde er blevet udvidet, så den også omfatter behandling i forbindelse med en aktivitet, der umiddelbart inden overgangsperiodens udløb faldt uden for EU-rettens anvendelsesområde (f.eks. national sikkerhed) ([31]), eller var omfattet af kapitel 2 i afsnit V i traktaten om Den Europæiske Union (aktiviteter under den fælles udenrigs- og sikkerhedspolitik) ([32]). Ligesom i Den Europæiske Unions system finder UK GDPR ikke anvendelse på en kompetent myndigheds behandling af personoplysninger med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner,

([26]) Artikel 2, stk. 1 og 5, i UK GDPR.

([27]) Artikel 4, stk. 1 og 2, i UK GDPR.

([28]) Manuel ustruktureret behandling af personoplysninger defineres i artikel 2, stk. 5, litra b), som behandling af personoplysninger, der ikke foregår automatisk eller på struktureret vis.

([29]) I artikel 2, stk. 1A, i UK GDPR fastsættes det, at retsakten også finder anvendelse på manuel ustruktureret behandling af personoplysninger, som opbevares af en offentlig myndighed på området for informationsfrihed. Der kan være tale om enhver offentlig myndighed som defineret i Freedom of Information Act 2000 (lov om informationsfrihed) eller enhver skotsk offentlig myndighed som defineret i Freedom of Information (Scotland) Act 2002 (asp 13). Section 21(5) i DPA 2018.

([30]) Artikel 2, stk. 2, litra a), i UK GDPR.

([31]) Aktiviteter, der vedrører statens sikkerhed, er kun omfattet af anvendelsesområdet for UK GDPR, for så vidt som de ikke udføres af en kompetent myndighed med henblik på retshåndhævelse, i hvilket tilfælde Part 3 i DPA 2018 finder anvendelse, eller af eller på vegne af en efterretningstjeneste, hvis aktiviteter er adskilt fra anvendelsesområdet for UK GDPR og er omfattet af Part 4 i DPA 2018 i henhold til artikel 2, stk. 2, litra c), i UK GDPR. For eksempel kan en politistyrke foretage sikkerhedskontrol af en medarbejder for at sikre, at det er forsvarligt at give ham adgang til materiale, der har betydning for statens sikkerhed. Selv om politiet er en kompetent myndighed med hensyn til retshåndhævelse, sker den pågældende behandling ikke med retshåndhævelse for øje, og UK GDPR finder derfor anvendelse. Se UK Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework, s. 8, som kan findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

([32]) Artikel 2, stk. 1, litra a) og b), i UK GDPR.

herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed (de såkaldte »retshåndhævelsesformål«) — en sådan behandling er i stedet reguleret af Part 3 i DPA 2018, som det er tilfældet med direktiv (EU) 2016/680 i henhold til EU-retten — eller behandling af personoplysninger hos efterretningstjenesterne (Security Service (sikkerhedstjenesten), Secret Intelligence Service (efterretningstjenesten) og Government Communications Headquarters (det statslige kommunikationskontor)), som er omfattet af Part 4 i DPA 2018 ([33]).

(22) UK GDPR's geografiske anvendelsesområde er beskrevet i artikel 3 i UK GDPR ([34]) og omfatter behandling af personoplysninger (uanset hvor den finder sted) i forbindelse med aktiviteter, der udføres af en dataansvarligs eller databehandlers virksomhed i Det Forenede Kongerige, samt behandling af personoplysninger om registrerede, der befinder sig i Det Forenede Kongerige, hvor behandlingsaktiviteterne vedrører udbud af varer eller tjenester til sådanne registrerede eller overvågning af deres adfærd ([35]). Dette afspejler tilgangen i artikel 3 i forordning (EU) 2016/679.

2.4. **Definitioner af personoplysninger og begreberne dataansvarlig og databehandler**

(23) Definitionerne af personoplysninger, behandling, dataansvarlig og databehandler samt definitionen af pseudonymisering i forordning (EU) 2016/679 er blevet bibeholdt uden væsentlige ændringer i UK GDPR ([36]). Desuden defineres en række særlige kategorier af oplysninger i artikel 9, stk. 1, i UK GDPR på samme måde som i forordning (EU) 2016/679 (»personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering«). Section 205 i DPA 2018 indeholder definitionen af »biometriske data« ([37]), »helbredsoplysninger« ([38]) og »genetiske data« ([39]).

2.5. **Garantier, rettigheder og forpligtelser**

2.5.1. *Behandlingens lovlighed og rimelighed*

(24) Personoplysninger bør behandles på lovlig og retfærdig vis.

(25) Principperne om lovlighed, rimelighed og gennemsigtighed samt grundlaget for lovlig behandling er sikret i Det Forenede Kongeriges lovgivning ved artikel 5, stk. 1, litra a), og artikel 6, stk. 1, i UK GDPR, som er identiske med de respektive bestemmelser i forordning (EU) 2016/679 ([40]). Section 8 i DPA 2018 supplerer artikel 6, stk. 1, litra e), ved at fastsætte, at behandling af personoplysninger i henhold til artikel 6, stk. 1, litra e), i UK GDPR (som er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller som led i den dataansvarliges udøvelse

([33]) Artikel 2, stk. 2, litra b) og c), i UK GDPR.

([34]) Det samme geografiske anvendelsesområde gælder for behandling af personoplysninger i henhold til Part 2 i DPA 2018, som supplerer UK GDPR (Section 207(1A)).

([35]) Dette betyder navnlig, at DPA 2018 og således nærværende afgørelse ikke finder anvendelse på britiske kronbesiddelser (Jersey, Guernsey og Isle of Man) og Det Forenede Kongeriges oversøiske territorier, herunder Falklandsøerne og Gibraltars territorium.

([36]) Artikel 4, stk. 1, 2, 5, 7 og 8, i UK GDPR.

([37]) »Biometriske data«: personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger.

([38]) »Helbredsoplysninger«: personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand.

([39]) »Genetiske data«: personoplysninger vedrørende en fysisk persons arvede eller erhvervede genetiske karakteristika, som giver entydig information om den fysiske persons fysiologi eller helbred, og som navnlig foreligger efter en analyse af en biologisk prøve fra den pågældende fysiske person.

([40]) I henhold til artikel 6, stk. 1, i UK GDPR er behandling kun lovlig, hvis og i det omfang: a) den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål, b) behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt, c) behandling er nødvendig for at overholde en retlig forpligtelse, som gælder for den dataansvarlige, d) behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser, e) behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, eller f) behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

af offentlig myndighed) omfatter behandling af personoplysninger, der er nødvendig for retsplejen, udøvelsen af en funktion i et af parlamentets kamre, udøvelsen af en funktion, der er tillagt en person ved en retsakt eller retsudøvelse, udøvelsen af en funktion, som varetages af Kronen, en minister under Kronen eller en offentlig instans, eller en aktivitet, der understøtter eller fremmer demokratisk engagement.

(26) Med hensyn til samtykke (en af de legitime grunde til behandling) bibeholdes betingelserne i artikel 7 i forordning (EU) 2016/679 også uændret i UK GDPR, dvs. at den dataansvarlige skal kunne påvise, at den registrerede har givet sit samtykke, der skal indgives en skriftlig anmodning om samtykke i et klart og forståeligt sprog, den registrerede skal have ret til at trække sit samtykke tilbage til enhver tid, og når det vurderes, om samtykke gives frivilligt, bør der tages hensyn til, om opfyldelsen af en kontrakt er betinget af samtykke til den pågældende behandling af personoplysninger, som ikke er nødvendig for opfyldelsen af den pågældende kontrakt. I henhold til artikel 8 i UK GDPR er et barns samtykke i forbindelse med levering af informationssamfundstjenester desuden kun lovligt, når barnet er mindst 13 år gammelt. Dette falder inden for den aldersgruppe, der er fastsat i artikel 8 i forordning (EU) 2016/679.

2.5.2. *Behandling af særlige kategorier af personoplysninger*

(27) Der bør være særlige garantier, når »særlige kategorier« af oplysninger behandles.

(28) Både UK GDPR og DPA 2018 indeholder specifikke regler for behandling af særlige kategorier af personoplysninger, som er defineret i artikel 9, stk. 1, i UK GDPR på samme måde som i forordning (EU) 2016/679 (se betragtning 23 ovenfor). I henhold til artikel 9 i UK GDPR er behandling af særlige kategorier af oplysninger i princippet forbudt, medmindre der gælder en specifik undtagelse.

(29) Disse undtagelser (som er anført i artikel 9, stk. 2 og 3, i UK GDPR) medfører ingen substansændringer i forhold til dem, der er omhandlet i artikel 9, stk. 2 og 3), i forordning (EU) 2016/679. Medmindre den registrerede udtrykkeligt har givet sit samtykke til behandlingen af disse personoplysninger, er behandling af særlige kategorier af personoplysninger kun tilladt under særlige og begrænsede omstændigheder. I de fleste tilfælde skal behandlingen af følsomme oplysninger være nødvendig til et specifikt formål, der er defineret i den relevante bestemmelse (se artikel 9, stk. 2, litra b), c), f), g), h), i) og j)).

(30) Når en undtagelse i henhold til artikel 9, stk. 2, i UK GDPR kræver tilladelse ved lov, eller der henvises til den offentlige interesse, præciseres de betingelser, der skal være opfyldt, for at undtagelserne kan påberåbes, desuden i Section 10 i DPA 2018 sammen med Schedule 1 til samme lov. I tilfælde af behandling af følsomme oplysninger med det formål at beskytte »folkesundheden« (artikel 9, stk. 2, litra i), i UK GDPR) kræves det f.eks. i paragraph 3(b) i Part 1 i Schedule 1, at en sådan behandling ud over nødvendighedstesten foretages »af en sundhedsperson eller under dennes ansvar« eller »af en anden person, der har tavshedspligt i henhold til en retsakt eller retsudøvelse«, herunder i kraft af den veletablerede tavshedspligt i henhold til gældende sædvaneret.

(31) I det tilfælde, at følsomme oplysninger behandles af hensyn til væsentlige samfundsinteresser (artikel 9, stk. 2, litra g), i UK GDPR), indeholder Part 2 i Schedule 1 til DPA 2018 en udtømmende liste over formål, der kan anses for at være væsentlige samfundsinteresser, ligesom der fastsættes yderligere specifikke betingelser for hvert af disse formål. For eksempel anerkendes fremme af racemæssig og etnisk mangfoldighed på ledelsesniveau i organisationer som en væsentlig samfundsinteresse. Behandling af følsomme oplysninger til dette specifikke formål er underlagt detaljerede krav, herunder at behandlingen skal foretages som led i en procedure for udpegelse af personer, der er egnede til at bestride ledende stillinger, at den er nødvendig for at fremme racemæssig og etnisk mangfoldighed, og at den sandsynligvis ikke vil forårsage væsentlig skade eller alvorlige problemer for den registrerede.

(32) I Section 11(1) i DPA 2018 fastsættes betingelserne for behandling af personoplysninger under de omstændigheder, der er beskrevet i artikel 9, stk. 3, i UK GDPR vedrørende tavshedspligt. Der kan f.eks. være tale om omstændigheder, hvor behandlingen udføres af en sundhedsperson, en socialarbejder eller en anden person, der under omstændighederne har tavshedspligt i henhold til en retsakt eller retsudøvelse, eller på dennes ansvar.

(33) Desuden kræver mange af de undtagelser, der er anført i artikel 9, stk. 2, i UK GDPR, at der træffes passende og specifikke beskyttelsesforanstaltninger, for at kunne anvendes. Afhængigt af behandlingens art og risikoniveauet for de registreredes rettigheder og frihedsrettigheder fastsættes der forskellige beskyttelsesforanstaltninger i betingelserne for behandling i Schedule 1 til DPA 2018. I Schedule 1 fastsættes betingelserne for hver enkelt behandlingssituation.

(34) I nogle tilfælde regulerer og begrænser DPA 2018 de former for følsomme oplysninger, der kan behandles, for at overholde et bestemt retsgrundlag. Eksempelvis gives der i paragraph 8 i Schedule 1 mulighed for behandling af følsomme oplysninger med henblik på at fremme lige muligheder eller ligebehandling. Denne betingelse for behandling kan kun anvendes, hvis oplysningerne viser racemæssig eller etnisk oprindelse, religiøs eller filosofisk overbevisning eller seksuel orientering, eller hvis der er tale om helbredsoplysninger.

(35) I nogle tilfælde begrænser DPA 2018 den type dataansvarlig, der kan anvende betingelsen for behandling. For eksempel indeholder paragraph 23 i Schedule 1 bestemmelser om behandling af følsomme oplysninger i forbindelse med valgte repræsentanters svar til offentligheden. Denne betingelse kan kun anvendes, hvis den dataansvarlige er den valgte repræsentant eller handler under deres myndighed.

(36) I visse andre tilfælde fastsætter DPA 2018 grænser for, hvilke kategorier af registrerede betingelsen kan anvendes for. For eksempel regulerer paragraph 21 i Schedule 1 behandlingen af følsomme oplysninger i forbindelse med erhvervstilknyttede pensionsordninger. Denne betingelse kan kun anvendes, hvis den pågældende registrerede er søskende, forælder, bedsteforælder eller oldeforælder til brugeren af ordningen.

(37) Desuden gælder det, at den dataansvarlige i de fleste tilfælde skal udarbejde et »Appropriate Policy Document«, når vedkommende påberåber sig de undtagelser i artikel 9, stk. 2, i UK GDPR, som er nærmere præciseret i Section 10 i DPA 2018 sammen med Schedule 1 til samme lov. Dette dokument skal beskrive den dataansvarliges procedurer for sikring af overholdelse af principperne i artikel 5 i UK GDPR. Desuden skal det fastlægge politikker for opbevaring og sletning, og den sandsynlige opbevaringsperiode skal angives. Den dataansvarlige skal gennemgå og ajourføre dette dokument, når det er relevant. Den dataansvarlige skal opbevare dokumentet i seks måneder efter behandlingens afslutning og efter anmodning stille det til rådighed for Information Commissioner ([41]).

(38) I henhold til paragraph 41 i Schedule 1 til DPA 2018 skal ovennævnte »Appropriate Policy Document« altid ledsages af en udvidet fortegnelse over behandlingsaktiviteterne. Denne fortegnelse skal spore opfyldelsen af forpligtelserne i dokumentet, dvs. at det skal registreres, om oplysningerne slettes eller opbevares i overensstemmelse med politikkerne. Hvis politikkerne ikke er blevet fulgt, skal årsagerne hertil registreres i fortegnelsen. I fortegnelsen skal det også beskrives, hvordan behandlingen opfylder artikel 6 i UK GDPR (lovlig behandling) og den specifikke betingelse i Schedule 1 til DPA 2018, der lægges til grund.

(39) Endelig indeholder UK GDPR ligesom forordning (EU) 2016/679 også en række generelle garantier for visse former for behandling af særlige kategorier af oplysninger. Artikel 35 i UK GDPR kræver en konsekvensanalyse vedrørende databeskyttelse, hvis særlige kategorier af oplysninger behandles i stort omfang. I henhold til artikel 37 i UK GDPR skal den dataansvarlige eller databehandleren udpege en databeskyttelsesrådgiver, hvis deres kerneaktiviteter består i at behandle særlige kategorier af oplysninger i stort omfang.

(40) Med hensyn til personoplysninger vedrørende straffedomme og lovovertrædelser er artikel 10 i UK GDPR identisk med artikel 10 i forordning (EU) 2016/679. Artiklen giver kun mulighed for behandling af personoplysninger vedrørende straffedomme og lovovertrædelser under en offentlig myndigheds kontrol, eller hvis behandlingen er tilladt i henhold til national lovgivning, der giver passende garantier for de registreredes rettigheder og frihedsrettigheder.

(41) Hvis behandlingen af oplysninger vedrørende straffedomme og lovovertrædelser ikke foretages under en offentlig myndigheds kontrol, fastsættes det i Section 10(5) i DPA 2018, at en sådan behandling kun må finde sted til de specifikke formål/i de specifikke situationer, der er fastsat i Part 1, 2 og 3 i Schedule 1 til DPA 2018, og at behandlingen er underlagt de specifikke krav, som er fastlagt for hvert/hver af disse formål/situationer. Oplysninger vedrørende straffedomme kan f.eks. behandles af nonprofitorganisationer, hvis behandlingen foretages a) som led i deres legitime aktiviteter, idet de fornødne garantier stilles af en fond, forening eller en anden nonprofitorganisation med et politisk, filosofisk, religiøst eller fagforeningsmæssigt formål, og b) på betingelse af i) at behandlingen udelukkende vedrører medlemmerne eller tidligere medlemmer af organisationen eller personer, der har regelmæssig kontakt med den i forbindelse med dens formål, og ii) at oplysningerne ikke videregives uden for organisationen uden de registreredes samtykke.

([41]) Paragraph 38-40 i Schedule 1 til DPA 2018.

(42) Desuden er der i Part 3 i Schedule 1 til DPA 2018 fastsat en række yderligere omstændigheder, hvor der kan anvendes oplysninger vedrørende straffedomme, som svarer til det retlige grundlag for behandling af følsomme oplysninger i artikel 9, stk. 2, i forordning (EU) 2016/679 og i UK GDPR (f.eks. den registreredes samtykke, en persons vitale interesser, hvis den registrerede retligt eller fysisk er ude af stand til at give sit samtykke, hvis oplysningerne allerede tydeligvis er blevet offentliggjort af den registrerede, hvis behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares osv.).

2.5.3. *Formålsbegrænsning, rigtighed, dataminimering, opbevaringsbegrænsning og datasikkerhed*

(43) Personoplysninger skal behandles til et specifikt formål og efterfølgende udelukkende anvendes, såfremt anvendelsen ikke er uforenelig med behandlingsformålet.

(44) Dette princip er fastsat i artikel 5, stk. 1, litra b), i forordning (EU) 2016/679 og er bibeholdt uden ændringer i artikel 5, stk. 1, litra b), i UK GDPR. Betingelserne for yderligere forenelig behandling i henhold til artikel 6, stk. 4, i forordning (EU) 2016/679 er også bibeholdt uden væsentlige ændringer i artikel 6, stk. 4, litra a)-e), i UK GDPR.

(45) Endvidere skal personoplysninger være korrekte og om nødvendigt ajourførte. De bør også være tilstrækkelige, relevante og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de behandles, og de bør i princippet ikke opbevares i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de behandles.

(46) Disse principper om dataminimering, rigtighed og opbevaringsbegrænsning er fastsat i artikel 5, stk. 1, litra c)-e), i forordning (EU) 2016/679 og bibeholdes uden ændringer i artikel 5, stk. 1, litra c)-e), i UK GDPR.

(47) Personoplysninger bør også behandles på en måde, der værner om deres sikkerhed, idet de bl.a. beskyttes mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse. Med henblik herpå bør virksomhedsledere træffe passende tekniske eller organisatoriske foranstaltninger for at beskytte personoplysninger mod mulige trusler. Disse foranstaltninger bør vurderes under hensyntagen til det aktuelle tekniske niveau og de relaterede omkostninger.

(48) Datasikkerhed er forankret i Det Forenede Kongeriges lovgivning i kraft af princippet om integritet og fortrolighed i artikel 5, stk. 1, litra f), i UK GDPR og i samme retsakts artikel 32 om behandlingssikkerhed. Disse bestemmelser er identiske med de respektive bestemmelser i forordning (EU) 2016/679. Desuden kræver UK GDPR på samme betingelser som dem, der er fastsat i artikel 33 og 34 i forordning (EU) 2016/679, at både tilsynsmyndigheden og den registrerede underrettes om et brud på persondatasikkerheden (henholdsvis artikel 33 og 34 i UK GDPR).

2.5.4. *Gennemsigtighed*

(49) Registrerede bør underrettes om de vigtigste dele af behandlingen af deres personoplysninger.

(50) Dette sikres ved artikel 13 og 14 i UK GDPR, som ud over et generelt princip om gennemsigtighed fastsætter regler om de oplysninger, der skal gives til den registrerede ([42]). I UK GDPR er der ikke foretaget nogen væsentlige ændringer af disse regler i forhold til de tilsvarende artikler i forordning (EU) 2016/679. Ligesom i forordning (EU) 2016/679 er gennemsigtighedskravene i disse artikler imidlertid omfattet af en række undtagelser, der er fastsat i DPA 2018 (se betragtning 55 til 72).

([42]) I artikel 13, stk. 1, litra f), og artikel 14, stk. 1, litra f), er henvisningerne til Kommissionens afgørelser om tilstrækkeligheden af beskyttelsesniveauet blevet erstattet af henvisninger til tilsvarende instrumenter i Det Forenede Kongerige, dvs. bestemmelser om tilstrækkelighed i henhold til DPA 2018. Desuden er henvisningerne til EU-retten eller medlemsstaternes lovgivning i artikel 14, stk. 5, litra c)-d), blevet erstattet med en henvisning til national ret (som eksempler på national lovgivning, der kan falde ind under artikel 14, stk. 5, litra c), har Det Forenede Kongerige anført Section 7 i Scrap Metal Dealers Act 2013, der fastsætter regler for registrering af licenser vedrørende metalskrot, og Part 35 i Companies Act 2006, der indeholder regler om selskabsregistrering). Ligeledes kan et eksempel på national lovgivning, der kan falde ind under artikel 14, stk. 5, litra d), omfatte lovgivning, som fastsætter regler om tavshedspligt, eller forpligtelser, der afspejles i ansættelseskontrakter eller den tavshedspligt, der gælder i henhold til sædvaneretten (f.eks. hvad angår personoplysninger, der behandles af sundhedspersonale, HR-medarbejdere, socialarbejdere osv.).

2.5.5. *Individuelle rettigheder*

(51) Registrerede bør have visse rettigheder, som kan gøres gældende over for den dataansvarlige eller databehandleren, navnlig retten til indsigt i oplysninger, retten til at gøre indsigelse mod behandlingen og retten til at få oplysninger berigtiget og slettet. Samtidig kan sådanne rettigheder være underlagt begrænsninger, for så vidt som disse begrænsninger er nødvendige og forholdsmæssige for at beskytte den offentlige sikkerhed eller andre vigtige mål af almen interesse.

2.5.5.1 Materielle rettigheder

(52) UK GDPR giver enkeltpersoner de samme rettigheder, der kan håndhæves, som forordning (EU) 2016/679. Bestemmelserne om enkeltpersoners rettigheder er blevet bibeholdt i UK GDPR uden væsentlige ændringer.

(53) Disse rettigheder omfatter den registreredes ret til indsigt (artikel 15 i UK GDPR), retten til berigtigelse (artikel 16 i UK GDPR), retten til sletning (artikel 17 i UK GDPR), retten til begrænsning af behandling (artikel 18 i UK GDPR), en underretningspligt vedrørende berigtigelse eller sletning af personoplysninger eller begrænsning af behandling (artikel 19 i UK GDPR), retten til dataportabilitet (artikel 20 i UK GDPR) og retten til at gøre indsigelse (artikel 21 i UK GDPR) ([43]). Sidstnævnte omfatter også den registreredes ret til at gøre indsigelse mod behandling af personoplysninger med henblik på direkte markedsføring, jf. artikel 21, stk. 2 og 3, i forordning (EU) 2016/679. I henhold til Section 122 i DPA 2018 skal Information Commissioner desuden udarbejde en adfærdskodeks for direkte markedsføring i overensstemmelse med kravene i databeskyttelseslovgivningen (og bestemmelserne om databeskyttelse og elektronisk kommunikation i Privacy and Electronic Communications (EC Directive) Regulations 2003 samt andre retningslinjer til fremme af god praksis i forbindelse med direkte markedsføring, som Information Commissioner finder passende. Information Commissioners kontor er i færd med at udvikle kodeksen for direkte markedsføring ([44]).

(54) Den registreredes ret til ikke at være genstand for en afgørelse, der udelukkende er baseret på automatisk behandling, og som har retsvirkning eller på tilsvarende vis påvirker den pågældende væsentligt, jf. artikel 22 i GDPR, er også blevet bevaret i UK GDPR uden væsentlige ændringer. Der er imidlertid tilføjet et nyt stk. 3A for at henvise til, at Section 14 i DPA 2018 fastsætter garantier for registreredes rettigheder, frihedsrettigheder og legitime interesser, når behandlingen foretages i henhold til artikel 22, stk. 2, litra b), i UK GDPR. Dette gælder kun, når grundlaget for en sådan afgørelse er en godkendelse eller et krav i henhold til Det Forenede Kongeriges lovgivning, og ikke hvis afgørelsen er nødvendig i henhold til en kontrakt eller er truffet med den registreredes udtrykkelige samtykke. Hvis Section 14 i DPA 2018 finder anvendelse, skal den dataansvarlige, så snart det er praktisk muligt, skriftligt underrette den registrerede om, at der er truffet en afgørelse udelukkende på grundlag af automatisk behandling. Den registrerede har ret til — senest en måned efter modtagelsen af underretningen — at anmode den dataansvarlige om at tage afgørelsen op til fornyet overvejelse eller træffe en ny afgørelse, der ikke udelukkende er baseret på automatisk behandling. Secretary of State har beføjelse til at vedtage yderligere sikkerhedsforanstaltninger med hensyn til automatisk beslutningstagning. Denne beføjelse er endnu ikke blevet udøvet.

2.5.5.2 Begrænsninger i individuelle rettigheder og andre bestemmelser

(55) DPA 2018 fastsætter en række begrænsninger for individuelle rettigheder i overensstemmelse med artikel 23 i UK GDPR. I denne artikel indføres der ingen begrænsninger vedrørende den ret til at gøre indsigelse mod direkte markedsføring, som er fastsat i artikel 21, stk. 2 og 3, i UK GDPR eller retten til ikke at være underlagt automatisk beslutningstagning som fastsat i artikel 22 i UK GDPR.

(56) Begrænsningerne er nærmere beskrevet i Schedule 2-4 til DPA 2018. Myndigheder i Det Forenede Kongerige har forklaret, at de følger to principper, nemlig specialitetsprincippet (ved at anlægge en detaljeret tilgang, opdele overordnede begrænsninger i flere og mere specifikke bestemmelser) og konditionalitetsprincippet (hver bestemmelse suppleres af sikkerhedsforanstaltninger i form af begrænsninger eller betingelser for at forhindre misbrug) ([45]).

([43]) I artikel 17, stk. 1, litra e), og artikel 17, stk. 3, litra 17 b), er henvisningerne til EU-retten og medlemsstaternes lovgivning blevet erstattet med en henvisning til national ret (som eksempler på en sådan national lovgivning i henhold til artikel 17, stk. 1, litra e), har Det Forenede Kongerige nævnt Education (Pupil Information) (England) Regulations 2006, der kræver, at elevernes navne slettes fra skoleregistrene, efter at de har forladt skolen, og Medical Act 1983, Section 34F, som fastsætter reglerne om sletning af navne fra General Practitioner Register og Specialist Register.

([44]) Udkastet til adfærdskodeksen kan findes på følgende link: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

([45]) UK Explanatory Framework for Adequacy Discussions, section E: Restrictions, s. 1, som kan findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

(57) Ved formuleringen af de begrænsninger, der er beskrevet i artikel 23, stk. 1, i UK GDPR, sikres det, at de kun finder anvendelse under nærmere angivne omstændigheder, hvor det er nødvendigt i et demokratisk samfund og står i et rimeligt forhold til det legitime mål, de forfølger. I overensstemmelse med fast retspraksis om fortolkning af begrænsninger kan en undtagelse fra databeskyttelsesordningen desuden kun anvendes i særlige tilfælde, hvis det er nødvendigt og rimeligt at gøre det ([46]). Vurderingen af nødvendigheden skal være »streng, idet ethvert indgreb i den registreredes rettigheder skal stå i et rimeligt forhold til, hvor alvorlig truslen mod offentlighedens interesser er. Der er derfor tale om en klassisk proportionalitetsanalyse ([47]).«

(58) Formålet med disse begrænsninger svarer til formålet med dem, der er anført i artikel 23 i forordning (EU) 2016/679, bortset fra begrænsningerne med hensyn til statens sikkerhed og forsvar, som i stedet er reguleret af Section 26 i DPA 2018, men som er underlagt de samme krav om nødvendighed og proportionalitet (se betragtning 63 til 66).

(59) Nogle af begrænsningerne, f.eks. dem, der vedrører forebyggelse eller afsløring af kriminalitet, pågribelse eller retsforfølgning af lovovertrædere og fastsættelse eller opkrævning af skatter eller afgifter ([48]), gør det muligt at begrænse alle individuelle rettigheder og gennemsigtighedsforpligtelser (bortset fra rettigheder i henhold til artikel 21, stk. 2, og artikel 22). Andre begrænsninger finder kun anvendelse på gennemsigtighedsforpligtelser og adgangsrettigheder, såsom de begrænsninger, der vedrører fortroligheden mellem advokat og klient ([49]), retten til fritagelse fra et krav om at give oplysninger, som ville føre til selvinkriminering ([50]), og virksomhedsfinansiering, navnlig forebyggelse af insiderhandel ([51]). Kun få af begrænsningerne gør det muligt at begrænse den dataansvarliges forpligtelse til at underrette en registreret om et brud på datasikkerheden og principperne om formålsbegrænsning samt lovlighed, rimelighed og gennemsigtighed i behandlingen ([52]).

(60) Nogle af begrænsningerne gælder automatisk »fuldt ud« for en bestemt slags behandling af personoplysninger (f.eks. er anvendelsen af gennemsigtighedsforpligtelser og individuelle rettigheder udelukket, når personoplysninger behandles med henblik på at vurdere en persons egnethed til et retligt embede, eller når personoplysninger behandles af en domstol eller en person, der handler som en domstol).

(61) For de fleste tilfældes vedkommende præciseres det imidlertid i den relevante paragraph i Schedule 2 til DPA 2018, at begrænsningen kun finder anvendelse, når (og i det omfang) anvendelsen af bestemmelserne »sandsynligvis vil skade« det legitime formål, der forfølges med begrænsningen. For eksempel finder bestemmelserne i UK GDPR ikke anvendelse på personoplysninger, der behandles med henblik på forebyggelse eller afsløring af kriminalitet, pågribelse eller retsforfølgning af lovovertrædere eller ansættelse eller opkrævning af en skat eller afgift, »i det omfang anvendelsen af disse bestemmelser sandsynligvis vil skade« et af disse forhold ([53]).

(62) De britiske domstole har fortolket ordlyden »sandsynligvis vil skade« som »en meget betydelig og tungtvejende risiko for at skade de udpegede offentlige interesser« ([54]). En begrænsning, som er omfattet af vurderingen af, om der forvoldes skade, kan derfor kun påberåbes, hvis og i det omfang der er en meget betydelig og tungtvejende chance for, at tildelingen af en bestemt rettighed vil skade den offentlige interesse. Den dataansvarlige er ansvarlig for fra sag til sag at vurdere, om disse betingelser er opfyldt ([55]).

(63) Ud over begrænsningerne i Schedule 2 til DPA 2018 indeholder Section 26 i samme lov en undtagelse, der kan finde anvendelse på visse bestemmelser i UK GDPR og DPA 2018, hvis denne undtagelse er nødvendig af hensyn til beskyttelsen af statens sikkerhed eller det nationale forsvar. Denne undtagelse finder anvendelse på databeskyttelsesprincipperne (bortset fra princippet om lovlighed), gennemsigtighedsforpligtelserne, den registreredes rettigheder, forpligtelsen til at anmelde et brud på datasikkerheden, reglerne om internationale overførsler, nogle af de pligter og

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

([47]) Guriev mod Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), præmis 43. Se i denne henseende også Lin mod Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB), præmis 80.

([48]) Paragraph 2 i Schedule 2 til DPA 2018.

([49]) Paragraph 19 i Schedule 2 til DPA 2018.

([50]) Paragraph 20 i Schedule 2 til DPA 2018.

([51]) Paragraph 21 i Schedule 2 til DPA 2018.

([52]) Begrænsninger i retten til underretning om brud på datasikkerheden er f.eks. kun tilladt i forbindelse med kriminalitet og beskatning (paragraph 2 i Schedule 2 til DPA 2018), parlamentarisk privilegium (paragraph 13 i Schedule 2 til DPA 2018) og behandling til journalistiske, akademiske, kunstneriske og litterære formål (paragraph 26 i Schedule 2 til DPA 2018).

([53]) Paragraph 2 i Schedule 2 til DPA 2018.

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

([55]) Open Rights Group & Anor, R (On the Application Of) mod Secretary of State for the Home Department & Anor, præmis 31.

beføjelser, der påhviler Information Commissioner, og reglerne om retsmidler, ansvar og sanktioner, bortset fra bestemmelsen om de generelle betingelser for pålæggelse af administrative bøder i artikel 83 i UK GDPR og bestemmelsen om sanktioner i artikel 84 i UK GDPR. Desuden ændrer Section 28 i DPA 2018 anvendelsen af artikel 9, stk. 1, for at muliggøre behandling af særlige kategorier af oplysninger i artikel 9, stk. 1, i UK GDPR, i det omfang behandlingen foretages af hensyn til statens sikkerhed eller til forsvarsformål, og idet de fornødne garantier stilles med hensyn til registreredes rettigheder og frihedsrettigheder ([56]).

(64) Undtagelsen kan kun anvendes i det omfang, den er nødvendig for at beskytte statens sikkerhed eller det nationale forsvar. Ligesom det gælder for de øvrige undtagelser, der er fastsat i DPA 2018, skal den dataansvarlige overveje og påberåbe sig den i hvert enkelt tilfælde. Desuden skal enhver anvendelse af undtagelsen være i overensstemmelse med standarderne for menneskerettigheder (understøttet af Human Rights Act 1998), ifølge hvilken ethvert indgreb i retten til privatlivets fred skal være nødvendig og forholdsmæssig i et demokratisk samfund ([57]).

(65) Denne fortolkning af undtagelsen bekræftes af den ICO, der har udstedt detaljerede retningslinjer for anvendelsen af undtagelsen for national sikkerhed og forsvar, idet den gør det klart, at den skal overvejes og anvendes af den dataansvarlige fra sag til sag ([58]). Det understreges navnlig i vejledningen, at det ikke er »en generel undtagelse«, og at det for at kunne påberåbe sig den »ikke er tilstrækkeligt, at oplysningerne behandles af hensyn til den nationale sikkerhed«. Derimod skal den dataansvarlige, der påberåber sig den, »påvise, at der er en reel mulighed for at skade den nationale sikkerhed«, og den dataansvarlige forventes om nødvendigt at »forelægge [ICO] dokumentation for, hvorfor [den] har anvendt denne undtagelse«. Vejledningen indeholder en tjekliste og en række eksempler for yderligere at præcisere, under hvilke betingelser denne undtagelse kan påberåbes.

(66) Den omstændighed, at oplysningerne behandles til nationale sikkerheds- eller forsvarsformål, er derfor ikke i sig selv tilstrækkelig til, at undtagelsen kan finde anvendelse. Den dataansvarlige skal overveje de faktiske konsekvenser for statens sikkerhed, hvis den pågældende databeskyttelsesbestemmelse skal overholdes. Undtagelsen kan kun anvendes på netop de bestemmelser, der anses for at udgøre risikoen, og skal anvendes så restriktivt som muligt ([59]).

(67) Denne tilgang er blevet bekræftet af Information Tribunal ([60]). I sagen *Baker* mod *Secretary of State for the Home Department* (»*Baker mod Secretary of State*«) fastslog retten, at det var ulovligt at anvende undtagelsen vedrørende statens sikkerhed som en generel undtagelse for anmodninger om adgang, som efterretningstjenesterne modtager. I stedet skulle undtagelsen anvendes fra sag til sag under hensyntagen til den enkelte anmodnings berettigelse og i lyset af enkeltpersoners ret til respekt for deres privatliv ([61]).

([56]) Ifølge oplysningerne fra de britiske myndigheder vil de dataansvarlige, når behandlingen vedrører statens sikkerhed, typisk anvende skærpede garantier og sikkerhedsforanstaltninger for behandlingen, som afspejler behandlingens følsomme karakter. Hvilke sikkerhedsforanstaltninger der er passende, afhænger af de risici, som er forbundet med den behandling, der foretages. Der kan f.eks. være tale om begrænsninger i adgangen til dataene, således at autoriserede personer kun kan få adgang til dem med en passende sikkerhedsgodkendelse, strenge restriktioner for udveksling af data og den høje sikkerhedsstandard, der gælder for opbevarings- og håndteringsprocedurer.

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

([58]) Jf. ICO's retningslinjer om undtagelsen for national sikkerhed og forsvar, som kan findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([59]) Et eksempel fra de britiske myndigheder viser, at hvis en formodet terrorist, som efterforskes af sikkerhedstjenesten MI5, indgiver en anmodning om adgang til indenrigsministeriet (f.eks. fordi han er involveret i en tvist med indenrigsministeriet om immigrationsspørgsmål), vil det være nødvendigt at forebygge videregivelse til den registrerede af oplysninger, som MI5 måtte have delt med indenrigsministeriet vedrørende igangværende efterforskninger, der kunne skade følsomme kilder, metoder eller teknikker og/eller føre til en forøgelse af den trussel, som den pågældende udgør. Under sådanne omstændigheder er det sandsynligt, at betingelserne for anvendelse af den i Section 26 omhandlede undtagelse ville være opfyldt, og at der af hensyn til statens sikkerhed ville være behov for en undtagelse fra at offentliggøre oplysningerne. Hvis indenrigsministeriet imidlertid også var i besiddelse af personoplysninger om den fysiske person, som ikke vedrørte MI5-undersøgelsen, og disse oplysninger kunne videregives uden risiko for skade på statens sikkerhed, ville undtagelsen vedrørende statens sikkerhed ikke finde anvendelse, når det skulle overvejes at videregive oplysninger til den pågældende. ICO er i færd med at udarbejde retningslinjer for, hvordan de dataansvarlige bør anvende undtagelsen i Section 26. Disse retningslinjer forventes offentliggjort inden udgangen af marts 2021.

([60]) Information Tribunal blev oprettet for at behandle klager vedrørende databeskyttelse i henhold til databeskyttelsesloven Data Protection Act 1984. I 2010 blev Information Tribunal en del af General Regulatory Chamber of the First Tier Tribunal (afdelingen for sager om statsligt tilsyn under førsteinstansretten) som led i ændringen af det britiske domstolssystems opbygning.

([61]) Se Baker mod Secretary of State for the Home Department [2001] UKIT NSA2 (»Baker mod Secretary of State«).

2.5.6. *Begrænsninger for personoplysninger, der behandles til journalistiske, kunstneriske, akademiske og litterære formål samt med henblik på arkivering og forskning*

(68) Artikel 85, stk. 2, i UK GDPR giver mulighed for, at personoplysninger, der behandles til journalistiske, kunstneriske, akademiske og litterære formål, undtages fra flere bestemmelser i UK GDPR. I Part 5 i Schedule 2 til DPA 2018 fastsættes de undtagelser, der gælder for behandling til disse formål. Den indeholder undtagelser fra databeskyttelsesprincipperne (bortset fra princippet om integritet og fortrolighed), retsgrundlaget for behandlingen (herunder særlige kategorier af oplysninger om bl.a. straffedomme), betingelserne for samtykke, gennemsigtighedsforpligtelserne, de registreredes rettigheder, forpligtelsen til at anmelde brud på datasikkerheden og kravet om at høre Information Commissioner forud for behandling, der indebærer stor risiko, og reglerne om internationale overførsler ([62]). I denne henseende afviger UK GDPR rent indholdsmæssigt ikke væsentligt fra forordning (EU) 2016/679, som i artikel 85 også giver mulighed for at undtage behandling, der foretages i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed, fra en række krav i forordning (EU) 2016/679. Bestemmelserne i DPA 2018, navnlig Schedule 2, Part 5, er forenelige med UK GDPR.

(69) Den centrale afvejning, der skal foretages i henhold til artikel 85 i UK GDPR, vedrører spørgsmålet om, hvorvidt en undtagelse fra de databeskyttelsesregler, der er nævnt i betragtning 68, er »nødvendig for at forene retten til beskyttelse af personoplysninger med ytrings- og informationsfriheden« ([63]). I henhold til paragraph 26(2) og (3) i Schedule 2 til DPA 2018 foretager Det Forenede Kongerige ved denne afvejning en vurdering baseret på en »rimelig antagelse«. For at en undtagelse kan begrundes, skal den dataansvarlige med rimelighed antage, i) at offentliggørelse er i offentlighedens interesse, og ii) at anvendelsen af den relevante bestemmelse i GDPR ville være uforenelig med journalistiske, akademiske, kunstneriske eller litterære formål. Som bekræftet i retspraksis ([64]) har vurderingen baseret på en »rimelig antagelse« både et subjektivt og et objektivt element: Det er ikke tilstrækkeligt, at den dataansvarlige kan påvise, at han selv mente, at overholdelsen var uforenelig med formålet. Hans antagelse skal også være rimelig, hvilket vil sige, at en fornuftig person, som havde kendskab til de relevante forhold, ville være enig i den. Den dataansvarlige skal derfor udvise rettidig omhu i forbindelse med sin antagelse for at kunne påvise, at den er rimelig. Ifølge de britiske myndigheders forklaringer skal vurderingen baseret på en »rimelig antagelse« foretages for hver enkelt undtagelse ([65]). Hvis betingelserne er opfyldt, anses undtagelsen for at være nødvendig og forholdsmæssig i henhold til Det Forenede Kongeriges lovgivning.

(70) I henhold til Section 124 i DPA 2018 skal ICO udarbejde en adfærdskodeks for databeskyttelse og journalistik. Arbejdet med at udarbejde denne kodeks er i gang. I henhold til Data Protection Act 1998 er der udsendt retningslinjer på området, hvori det navnlig understreges, at det for at kunne påberåbe sig denne undtagelse ikke er tilstrækkeligt blot at anføre, at overholdelse ville være en ulempe for journalisters aktiviteter. Der skal

([62]) Se artikel 85 i UK GDPR og Schedule 2, Part 5, paragraph 26(9), i DPA 2018.

([63]) I overensstemmelse med Schedule 2, Part 5, paragraph 26(2) i DPA 2018 finder undtagelsen anvendelse på behandling af personoplysninger til særlige formål (journalistiske, akademiske, kunstneriske og litterære formål), hvis behandlingen foretages med henblik på en persons offentliggørelse af journalistisk, akademisk, kunstnerisk eller litterært materiale, og den dataansvarlige med rimelighed antager, at offentliggørelsen af dette materiale vil være i offentlighedens interesse. Ved vurderingen af, om offentliggørelse er i offentlighedens interesse, skal den dataansvarlige tage hensyn til den særlige rolle, som offentlighedens interesse spiller med hensyn til ytrings- og informationsfriheden. Desuden skal den dataansvarlige tage hensyn til adfærdskodekser og retningslinjer, der er relevante for den pågældende offentliggørelse (BBC's redaktionelle retningslinjer og kodekserne Ofcom Broadcasting Code og Editors' Code of Practice). For at en undtagelse kan finde anvendelse, skal den dataansvarlige desuden med rimelighed antage, at overholdelse af den relevante bestemmelse ville være uforenelig med de særlige formål (paragraph 26(3) i Schedule 2 til DPA 2018).

([64]) Dommen i NT1 mod Google [2018] EWHC 799 (QB), præmis 102, behandlede bl.a. spørgsmålet om, hvorvidt den dataansvarlige med rimelighed kunne antage, at offentliggørelse var i offentlighedens interesse, og at overholdelsen af de relevante bestemmelser var uforenelig med de særlige formål. Retten anførte, at Section 32(1) (b) og (c) i Data Protection Act 1998 har et subjektivt og et objektivt element: Den dataansvarlige skal påvise, at han antog, at offentliggørelse ville være i samfundets interesse, og at denne antagelse objektivt set var rimelig. Han/hun skal påvise den subjektive antagelse, at overholdelse af den bestemmelse, som vedkommende ønsker undtagelse fra, ville være uforenelig med det særlige formål, der er tale om.

([65]) ICO's beslutning om i henhold til Data Protection Act 1998 at pålægge True Visions Productions en bøde er et eksempel på, hvordan kriteriet om en »rimelig antagelse» anvendes. ICO accepterede, at mediekontrolorganet subjektivt antog, at overholdelsen af det første databeskyttelsesprincip (retfærdighed og lovlighed) var uforeneligt med journalistiske formål. ICO accepterede imidlertid ikke, at denne antagelse objektivt set var rimelig. ICO's afgørelse kan findes på følgende link: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

også være et klart argument for, at den pågældende bestemmelse udgør en hindring for ansvarlig journalistik ([66]). Retningslinjer for anvendelsen af kriteriet om offentlig interesse og afvejningen af offentlighedens interesse med den enkeltes ret til privatlivets fred er også blevet offentliggjort af Det Forenede Kongeriges tilsynsmyndighed for telekommunikation OFCOM og af BBC i selskabets redaktionelle retningslinjer ([67]). I retningslinjerne gives der navnlig eksempler på oplysninger, der kan betragtes som værende i offentlighedens interesse, og samtidig anføres behovet for at kunne påvise, at offentlighedens interesse vejer tungere end retten til privatlivets fred under de særlige omstændigheder i sagen.

(71) I lighed med hvad der er fastsat i artikel 89 i databeskyttelsesforordningen, kan personoplysninger, som behandles med henblik på arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål, også undtages fra en række af bestemmelserne i UK GDPR ([68]). For så vidt angår forskning og statistik er der mulighed for undtagelser fra de bestemmelser i UK GDPR, der vedrører bekræftelse af behandling, og adgang til data og garantier i forbindelse med overførsler fra tredjelande, ret til berigtigelse, begrænsning af behandling og indsigelse mod behandling. Med hensyn til arkivering i samfundets interesse er der også mulighed for undtagelser fra underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling og i forbindelse med retten til dataportabilitet.

(72) I henhold til paragraph 27(1) og 28(1) i Schedule 2 til DPA 2018 er der mulighed for at gøre brug af undtagelserne fra de anførte bestemmelser i UK GDPR, hvis anvendelsen af bestemmelserne ville »forhindre eller i alvorlig grad hæmme opfyldelsen« af de pågældende formål ([69]).

(73) I betragtning af deres relevans for en effektiv udøvelse af individuelle rettigheder vil der blive taget behørigt hensyn til enhver relevant udvikling med hensyn til fortolkningen og den praktiske anvendelse af ovennævnte undtagelser (foruden den, der vedrører opretholdelse af en effektiv indvandringskontrol, jf. betragtning 6), herunder enhver yderligere udvikling af retspraksis og ICO's retningslinjer og håndhævelsesforanstaltninger i forbindelse med den løbende overvågning af denne afgørelse ([70]).

2.5.7. *Begrænsninger for videreoverførsel*

(74) Beskyttelsesniveauet for personoplysninger, der overføres fra Den Europæiske Union til dataansvarlige eller databehandlere i Det Forenede Kongerige, må ikke undergraves af videreoverførsel af sådanne oplysninger til modtagere i et tredjeland. Sådanne »videreoverførsler«, som set fra den britiske dataansvarliges eller databehandlers synspunkt udgør internationale overførsler fra Det Forenede Kongerige, bør kun tillades, hvis den efterfølgende modtager uden for Det Forenede Kongerige selv er underlagt regler, der sikrer et beskyttelsesniveau svarende til det, som sikres i Det Forenede Kongeriges retsorden. Derfor er anvendelsen af reglerne i UK GDPR og DPA 2018 om internationale overførsler af personoplysninger en vigtig faktor for at sikre kontinuitet i beskyttelsen af personoplysninger, der overføres fra Den Europæiske Union til Det Forenede Kongerige i henhold til denne afgørelse.

([66]) Ifølge retningslinjerne skal de pågældende organisationer kunne redegøre for, hvorfor overholdelse af den relevante bestemmelse i Data Protection Act 1998 er uforenelig med opnåelsen af journalistiske formål. De dataansvarlige skal navnlig afveje den skadelige virkning, som overholdelse af reglerne ville have på journalistikken, og den skadelige virkning, som manglende overholdelse ville have på den registreredes rettigheder. Hvis en journalist med rimelighed kan nå sine redaktionelle mål på en måde, der er i overensstemmelse med databeskyttelseslovens standardbestemmelser, skal vedkommende gøre det. Organisationerne skal kunne begrunde deres anvendelse af begrænsningen med hensyn til enhver bestemmelse, som de ikke har overholdt. »Data protection and journalism: a guide for the media« kan findes på følgende link: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Blandt eksempler på offentlig interesse kan nævnes afsløring eller opklaring af kriminalitet, beskyttelse af den offentlige sundhed eller sikkerhed, afsløring af vildledende påstande fra enkeltpersoner eller organisationer eller afsløring af inkompetence, der har konsekvenser for offentligheden. Se OFCOM's retningslinjer, som kan findes på følgende link: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf, og BBC's redaktionelle retningslinjer, som kan findes på følgende link: https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Se artikel 89 i UK GDPR samt paragraph 27(2) og paragraph 28(2) i Part 6 i Schedule 2 til DPA 2018.

([69]) Det er dog en betingelse, at personoplysninger behandles i overensstemmelse med artikel 89, stk. 1, i UK GDPR som suppleret ved Section 19 i DPA 2018.

([70]) Jf. betragtning 281 til 287.

(75) Ordningen for internationale overførsler af personoplysninger fra Det Forenede Kongerige er fastsat i artikel 44-49 i UK GDPR suppleret med DPA 2018 og er grundlæggende identisk med de regler, der er fastsat i kapitel V i forordning (EU) 2016/679 ([71]). Overførsel af personoplysninger til et tredjeland eller en international organisation kan kun finde sted på grundlag af bestemmelser om beskyttelsesniveauets tilstrækkelighed (Det Forenede Kongeriges pendant til en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til forordning (EU) 2016/679), eller uden brug af sådanne bestemmelser, hvis den dataansvarlige eller databehandleren har givet de fornødne garantier i overensstemmelse med artikel 46 i UK GDPR. I mangel af bestemmelser om tilstrækkeligheden af beskyttelsesniveauet eller passende garantier kan en overførsel kun finde sted på grundlag af undtagelser, der er fastsat i artikel 49 i UK GDPR.

(76) Det kan i Secretary of States bestemmelser om tilstrækkeligheden fastsættes, at et tredjeland (eller et område eller en sektor i et tredjeland), en international organisation eller en beskrivelse ([72]) af et sådant land eller område eller en sådan sektor eller organisation sikrer et tilstrækkeligt niveau for beskyttelse af personoplysninger. Ved vurderingen af beskyttelsesniveauets tilstrækkelighed skal Secretary of State tage hensyn til nøjagtig de samme elementer, som Kommissionen skal vurdere i henhold til artikel 45, stk. 2, litra a)-c), i forordning (EU) 2016/679, fortolket sammen med betragtning 104 i samme forordning og den bibeholdte EU-retspraksis. Det betyder, at den relevante standard i forbindelse med vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, vil være, om det pågældende tredjeland sikrer et beskyttelsesniveau, der »i det væsentlige svarer til« det, der sikres i Det Forenede Kongerige.

(77) Med hensyn til procedurer er bestemmelserne om tilstrækkeligheden af beskyttelsesniveauet underlagt de »generelle« proceduremæssige krav, der er fastsat i Section 182 i DPA 2018. I henhold til denne procedure skal Secretary of State rådføre sig med Information Commissioner, når førstnævnte foreslår at vedtage britiske bestemmelser om tilstrækkelighed ([73]). Når Secretary of State har vedtaget disse bestemmelser, forelægges de for parlamentet, idet de er underlagt »den negative beslutningsprocedure«, i henhold til hvilken begge parlamentets kamre kan granske bestemmelserne og har mulighed for at vedtage et forslag om annullering af dem inden for en frist på 40 dage ([74]).

(78) I henhold til Section 17B(1) i DPA 2018 skal bestemmelserne om tilstrækkelighed revideres med højst fire års mellemrum, og Secretary of State skal løbende overvåge udviklingen i tredjelande og internationale organisationer, der kan påvirke beslutninger om at fastsætte bestemmelser om tilstrækkelighed eller om at ændre eller tilbagekalde sådanne bestemmelser. Hvis Secretary of State bliver opmærksom på, at et sådant land eller en sådan organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, skal Secretary of State i det omfang, det er nødvendigt, ændre eller tilbagekalde bestemmelserne og indlede konsultationer med det pågældende tredjeland eller den pågældende organisation for at afhjælpe manglen på et tilstrækkeligt beskyttelsesniveau. Disse proceduremæssige aspekter afspejler også de tilsvarende krav i forordning (EU) 2016/679.

([71]) Med undtagelse af artikel 48 i forordning (EU) 2016/679, som Det Forenede Kongerige har valgt ikke at medtage i UK GDPR. I denne forbindelse bør det først og fremmest bemærkes, at den standard, der skal anses for at sikre et tilstrækkeligt beskyttelsesniveau, er en standard for »væsentlig ækvivalens» snarere end for identitet, som præciseret af EU-Domstolen (Schrems I-sagen, præmis 73-74) og anerkendt af Det Europæiske Databeskyttelsesråd (Adequacy Referential, s. 3). Som Det Europæiske Databeskyttelsesråd forklarede i Adequacy Referential (sin henvisning til tilstrækkelighed), er målet derfor ikke at afspejle den europæiske lovgivning punkt for punkt, men at fastlægge de væsentlige — centrale krav i denne lovgivning. I denne forbindelse er det vigtigt at bemærke, at selv om Det Forenede Kongeriges retsorden ikke formelt indeholder en bestemmelse, der er identisk med artikel 48, er den samme virkning sikret ved andre retlige bestemmelser og principper, dvs. at personoplysninger som svar på en anmodning om personoplysninger fra en domstol eller en administrativ myndighed i et tredjeland kun kan overføres til det pågældende tredjeland, hvis der er indgået en international aftale — på grundlag af hvilken den pågældende retsafgørelse eller administrative afgørelse i tredjelandet anerkendes eller fuldbyrdes i Det Forenede Kongerige — eller hvis den er baseret på en af de mekanismer, der er fastsat i kapitel V i UK GDPR. Mere specifikt skal domstolene i Det Forenede Kongerige for at fuldbyrde en udenlandsk retsafgørelse kunne henvise til sædvaneret eller til en lov, der tillader, at den fuldbyrdes. Hverken sædvaneret (jf. Adams and Others mod Cape Industries Plc., [1990] 2 W.L.R. 657) eller vedtægterne indeholder bestemmelser om fuldbyrdelse af udenlandske retsafgørelser, der kræver overførsel af oplysninger, uden at der er indgået en international aftale. Som følge heraf kan anmodninger om oplysninger ikke håndhæves i henhold til Det Forenede Kongeriges lovgivning, såfremt der ikke findes en sådan international aftale. Desuden er enhver overførsel af personoplysninger til tredjelande — herunder efter anmodning herom fra en udenlandsk domstol eller administrativ myndighed — fortsat underlagt begrænsningerne i kapitel V i UK GDPR, som er identiske med de tilsvarende bestemmelser i forordning (EU) 2016/679, og skal derfor bunde i en af de overførselsårsager, der er omtalt i kapitel V under de gældende specifikke betingelser i henhold til det pågældende kapitel.

([72]) De britiske myndigheder har forklaret, at det ved beskrivelsen af et land eller en international organisation vil være nødvendigt at foretage en specifik og delvis fastlæggelse af tilstrækkeligheden med målrettede begrænsninger (f.eks. bestemmelser om tilstrækkelighed, der kun vedrører bestemte former for dataoverførsler).

([73]) Jf. aftalememorandum mellem Secretary of State for the Department for Digital, Culture, Media and Sport (ministeren for digitale og andre medier, kultur og idræt) og Information Commissioner's Office om ICO's rolle med hensyn til de nye vurderinger af tilstrækkeligheden i Det Forenede Kongerige, som kan findes på følgende link: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) Hvis et sådant forslag vedtages, vil bestemmelserne i sidste ende ikke længere have retsvirkning.

(79) I mangel af bestemmelser om beskyttelsesniveauets tilstrækkelighed kan internationale overførsler finde sted, hvis den dataansvarlige eller databehandleren har givet de fornødne garantier i overensstemmelse med artikel 46 i UK GDPR. Disse garantier svarer til dem, der er fastsat i artikel 46 i forordning (EU) 2016/679. De omfatter juridisk bindende instrumenter, der kan håndhæves blandt offentlige myndigheder eller organer, bindende virksomhedsregler ([75]), standardbestemmelser om databeskyttelse, godkendte adfærdskodekser, godkendte certificeringsmekanismer og — med tilladelse fra Information Commissioner — kontraktlige aftaler mellem dataansvarlige (eller databehandlere) eller administrative ordninger mellem offentlige myndigheder. Ud fra et proceduremæssigt synspunkt er reglerne dog blevet ændret for at fungere i den britiske kontekst. Navnlig kan standardbestemmelserne om databeskyttelse vedtages af Secretary of State (Section 17C) eller Information Commissioner (Section 119A) i medfør af DPA 2018.

(80) I mangel af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller passende garantier kan en overførsel kun finde sted på grundlag af undtagelser, der er fastsat i artikel 49 i UK GDPR ([76]). I UK GDPR er der ikke foretaget nogen væsentlige ændringer af undtagelserne i forhold til de tilsvarende bestemmelser i forordning (EU) 2016/679. I henhold til UK GDPR kan der — som i henhold til forordning (EU) 2016/679 — kun gøres brug af visse undtagelser, hvis overførslen er lejlighedsvis ([77]). Endvidere præciserer ICO i sine retningslinjer for internationale overførsler, at undtagelserne kun bør bruges som egentlige »undtagelser« fra den generelle regel om, at der ikke må foretages en begrænset overførsel, medmindre den er omfattet af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, eller der er stillet passende garantier ([78]). Med hensyn til overførsler, der er nødvendige af hensyn til vigtige samfundsinteresser (artikel 49, stk. 1, litra d)), kan Secretary of State fastsætte bestemmelser for at præcisere, under hvilke omstændigheder overførsel af personoplysninger til et tredjeland eller en international organisation ikke er nødvendig af hensyn til vigtige samfundsinteresser. Secretary of State kan desuden fastsætte bestemmelser, der begrænser overførslen af en kategori af personoplysninger til et tredjeland eller en international organisation, hvis overførslen ikke kan finde sted på grundlag af bestemmelser om tilstrækkeligheden af beskyttelsesniveauet, og Secretary of State anser begrænsningen for nødvendig af hensyn til vigtige samfundsinteresser. Der er endnu ikke vedtaget sådanne bestemmelser.

(81) Disse rammer for internationale overførsler finder anvendelse fra og med overgangsperiodens udløb ([79]). Paragraph 4 i Schedule 21 til DPA 2018 (indført ved DPPEC-bestemmelserne) fastsætter imidlertid, at visse overførsler af personoplysninger fra overgangsperiodens udløb behandles, som om de er baseret på bestemmelser om tilstrækkelighed. Disse overførsler omfatter overførsler til en EØS-stat, Gibraltars territorium, en EU-institution, et organ, kontor eller agentur, der er oprettet af eller på grundlag af EU-traktaten, og tredjelande, der var genstand for en EU-afgørelse om beskyttelsesniveauets tilstrækkelighed ved overgangsperiodens udløb. Overførslerne til disse lande kan derfor fortsætte som før Det Forenede

([75]) I UK GDPR bibeholdes reglerne i artikel 47 i forordning (EU) 2016/679, idet der udelukkende foretages ændringer for at tilpasse dem til den nationale sammenhæng, f.eks. ved at henvise til Information Commissioner i stedet for den kompetente tilsynsmyndighed, fjerne henvisningen til sammenhængsmekanismen fra stk. 1 og slette hele stk. 3.

([76]) I henhold til artikel 49 i UK GDPR er overførsel mulig, hvis en af følgende betingelser er opfyldt: a) den registrerede udtrykkelig har givet samtykke til den foreslåede overførsel efter at være blevet informeret om de mulige risici, som sådanne overførsler kan medføre for den registrerede på grund af den manglende afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller fornødne garantier, b) overførslen er nødvendig af hensyn til opfyldelse af en kontrakt mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en sådan kontrakt, c) overførslen er nødvendig af hensyn til indgåelsen eller opfyldelsen af en kontrakt, der i den registreredes interesse er indgået mellem den dataansvarlige og en anden fysisk eller juridisk person, d) overførslen er nødvendig af hensyn til vigtige samfundsinteresser, e) overførslen er nødvendig for, at et retskrav kan fastslås, gøres gældende eller forsvares, f) overførslen er nødvendig for at beskytte den registreredes eller andre personers vitale interesser, hvis den registrerede ikke fysisk eller juridisk er i stand til at give samtykke, g) overførslen finder sted fra et register, der ifølge national lovgivning er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri, men kun i det omfang de ved national lovgivning fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde. Når ingen af ovennævnte betingelser finder anvendelse, kan en overførsel desuden kun finde sted, hvis den ikke gentages, kun vedrører et begrænset antal registrerede, er nødvendig for, at den dataansvarlige kan forfølge vægtige legitime interesser, som ikke tilsidesættes af den registreredes interesser eller rettigheder og frihedsrettigheder, og den dataansvarlige har vurderet alle omstændighederne i forbindelse med overførslen og på grundlag af denne vurdering har givet passende garantier med hensyn til beskyttelsen af personoplysninger.

([77]) I betragtning 111 i UK GDPR præciseres det, at overførsler i forbindelse med en kontrakt eller et retskrav kun kan finde sted, hvis de er lejlighedsvise.

([78]) ICO's retningslinjer vedrørende internationale overførsler kan findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) I en periode på højst seks måneder, der udløber senest den 30. juni 2021, skal bestemmelserne i denne nye ramme læses i lyset af artikel 782 i handels- og samarbejdsaftalen mellem Den Europæiske Union og Det Europæiske Atomenergifællesskab på den ene side og Det Forenede Kongerige Storbritannien og Nordirland på den anden side (L 444/14 af 31.12.2020), som kan findes på følgende link: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:22020A1231(01)&from=DA.

Kongeriges udtræden af EU. Efter overgangsperiodens udløb skal Secretary of State foretage en gennemgang af disse konklusioner om tilstrækkeligheden inden for en periode på fire år, dvs. senest ved udgangen af december 2024. Selv om Secretary of State skal foretage denne gennemgang inden udgangen af december 2024, indeholder overgangsbestemmelserne ifølge myndighederne i Det Forenede Kongerige ikke en »udløbsklausul«, og de relevante overgangsbestemmelser vil ikke automatisk ophøre med at have virkning, hvis en gennemgang ikke er afsluttet ved udgangen af december 2024.

(82) Endelig vil Kommissionen med hensyn til den fremtidige udvikling af Det Forenede Kongeriges internationale overførselsordning — gennem vedtagelse af nye bestemmelser om tilstrækkelighed, indgåelse af internationale aftaler eller udvikling af andre overførselsmekanismer — nøje overvåge situationen, vurdere, om de forskellige overførselsmekanismer anvendes på en måde, der sikrer kontinuitet i beskyttelsen, og om nødvendigt træffe passende foranstaltninger til at imødegå eventuelle negative virkninger for en sådan kontinuitet (se betragtning 278 til 287). Da EU og Det Forenede Kongerige har lignende regler om internationale overførsler, forventes det, at problematiske forskelle også kan undgås gennem samarbejde, udveksling af oplysninger og udveksling af erfaringer, herunder mellem ICO og Det Europæiske Databeskyttelsesråd.

2.5.8. *Ansvarlighed*

(83) I henhold til princippet om ansvarlighed skal enheder, der behandler oplysninger, træffe passende organisatoriske foranstaltninger med henblik på effektiv overholdelse af deres databeskyttelsesforpligtelser, og de skal være i stand til at dokumentere denne overholdelse, navnlig over for den kompetente tilsynsmyndighed.

(84) Princippet om ansvarlighed i forordning (EU) 2016/679 er bibeholdt i artikel 5, stk. 2, i UK GDPR uden væsentlige ændringer, og det samme gælder artikel 24 om den dataansvarliges ansvar, artikel 25 om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger og artikel 30 om fortegnelser over behandlingsaktiviteter. Artikel 35 og 36 om konsekvensanalyse vedrørende databeskyttelse og forudgående høring af tilsynsmyndigheden er også blevet bibeholdt. Artikel 37-39 i forordning (EU) 2016/679 om udpegelse af en databeskyttelsesrådgiver og dennes opgaver er blevet bibeholdt i UK GDPR uden væsentlige ændringer. Desuden er bestemmelserne i artikel 40 og 42 i forordning (EU) 2016/679 om adfærdskodekser og certificering bibeholdt i UK GDPR. ([80])

2.6 **Tilsyn og håndhævelse**

2.6.1. *Uafhængigt tilsyn*

(85) For at sikre, at et tilstrækkeligt databeskyttelsesniveau garanteres i praksis, bør der være oprettet en uafhængig tilsynsmyndighed med beføjelser til at overvåge og sikre, at databeskyttelsesreglerne overholdes. Denne myndighed bør være fuldstændig uafhængig og upartisk i udførelsen af sine opgaver og udøvelsen af sine beføjelser.

(86) I Det Forenede Kongerige varetages tilsynet med og håndhævelsen af UK GDPR og DPA 2018 af Information Commissioner. Information Commissioner er en »Corporation Sole«, dvs. en særskilt juridisk enhed, der består af en enkelt person. I sit arbejde bistås Information Commissioner af et kontor. Den 31. marts 2020 havde Information Commissioners kontor 768 fastansatte medarbejdere ([81]). Information Commissioner er underlagt Department for Digital, Culture, Media and Sport ([82]).

(87) Information Commissioners uafhængighed er udtrykkeligt fastsat i artikel 52 i UK GDPR, hvor der ikke foretages væsentlige ændringer af databeskyttelsesforordningens artikel 52, stk. 1-3. Information Commissioner skal handle helt uafhængigt i forbindelse med varetagelsen af sine opgaver og udøvelsen af sine beføjelser i overensstemmelse med UK GDPR, være fri for udefrakommende indflydelse, hvad enten den er direkte eller indirekte, i forbindelse

([80]) Om nødvendigt erstattes disse henvisninger med henvisninger til Det Forenede Kongeriges myndigheder. I henhold til Section 17 i DPA 2018 kan Information Commissioner eller Det Forenede Kongeriges nationale akkrediteringsorgan f.eks. akkreditere en person, der opfylder kravene i artikel 43 i UK GDPR, med henblik på at overvåge overholdelsen af en certificering.

([81]) Information Commissionerens årsberetning og årsregnskab for 2019- 2020 kan findes på følgende link: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

([82]) Forholdet mellem de to er fastlagt i en forvaltningsaftale. Som overordnet administrativ myndighed består Department for Digital, Culture, Media and Sports centrale ansvarsområder navnlig i at sikre, at Information Commissioner har tilstrækkelige midler og ressourcer, varetage Information Commissioners interesser over for parlamentet og andre offentlige instanser, sikre, at der findes solide nationale databeskyttelsesrammer, og yde vejledning og støtte til Information Commissioners kontor om erhvervsrelaterede spørgsmål vedrørende bl.a. ejendomme, lejemål og offentlige indkøb (forvaltningsaftalen for 2018-2021, som kan findes på følgende link: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf .

med disse opgaver og beføjelser og hverken søge eller modtage instrukser fra nogen. Desuden skal Information Commissioner afholde sig fra enhver handling, der er uforenelig med karakteren af dennes hverv, ligesom vedkommende under udøvelsen af sit hverv ikke må udøve nogen uforenelig lønnet eller ulønnet erhvervsmæssig virksomhed.

(88) Betingelserne for udpegelse og afskedigelse af Information Commissioner er fastsat i Schedule 12 til DPA 2018. Information Commissioner udnævnes af Storbritanniens dronning efter indstilling fra regeringen i henhold til en fair og åben udvælgelsesprøve. Ansøgerne til stillingen skal have relevante kvalifikationer, færdigheder og kompetencer. I overensstemmelse med Governance Code on Public Appointments (forvaltningsloven om offentlige udnævnelser) ([83]) udarbejder et rådgivende vurderingsudvalg en liste over kandidater, der kan udnævnes. Inden Secretary of State at the Department for Digital, Culture, Media and Sport træffer sin endelige afgørelse, skal det relevante særlige udvalg i parlamentet foretage en kontrol forud for udnævnelsen. Udvalgets holdning offentliggøres ([84]).

(89) Information Commissioner har en mandatperiode på op til syv år. Den samme person kan ikke udpeges til Information Commissioner mere end én gang. Information Commissioner kan afskediges af dronningen efter forslag (»Address«) fra begge parlamentets kamre ([85]). En anmodning om afskedigelse af Information Commissioner kan ikke indgives til nogen af parlamentets kamre, medmindre en minister har forelagt en rapport, hvoraf det fremgår, at han eller hun finder det godtgjort, at Information Commissioner har begået en alvorlig forseelse, og/eller at vedkommende ikke længere opfylder de betingelser, der er nødvendige for varetagelsen af vedkommendes opgaver ([86]).

(90) Finansieringen af Information Commissioner kommer fra tre kilder, nemlig i) databeskyttelsesafgifter, der betales af dataansvarlige, og som er fastsatSecretary of States bestemmelser ([87]) (Data Protection (Charges and Information) Regulations 2018) og udgør 85-90 % af kontorets årlige budget ([88]), ii) tilskud i form af støtte, som regeringen yder til Information Commissioner, og som hovedsagelig anvendes til at finansiere Information Commissioners driftsomkostninger i forbindelse med opgaver, der ikke vedrører databeskyttelse ([89]), og iii) gebyrer for tjenesteydelser ([90]). På nuværende tidspunkt opkræves der ikke sådanne gebyrer.

(91) Information Commissioners generelle opgaver i forbindelse med behandling af personoplysninger, som UK GDPR finder anvendelse på, er fastsat i artikel 57 i UK GDPR, som i høj grad afspejler de tilsvarende regler i forordning (EU) 2016/679. Disse opgaver omfatter overvågning og håndhævelse af UK GDPR, fremme af offentlighedens bevidsthed, behandling af klager indgivet af de registrerede, gennemførelse af undersøgelser osv. Derudover pålægger Section 115 i DPA 2018 Information Commissioner en række andre generelle opgaver, herunder en pligt til at rådgive parlamentet, regeringen og andre institutioner og organer om lovgivningsmæssige og administrative foranstaltninger vedrørende beskyttelse af fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger og beføjelse til på Information Commissioners eget initiativ eller efter anmodning at afgive udtalelser til parlamentet,

([83]) Governance Code on Public Appointments findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) Second Report of Session 2015- 2016 of the Culture, Media and Sports Committee at the House of Commons kan findes på følgende link: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) Et »Address« er et forslag, der forelægges Parlamentet, og som har til formål at gøre Kronen opmærksom på Parlamentets udtalelser om et bestemt emne.

([86]) Paragraph 3(3) i Schedule 12 til DPA 2018.

([87]) Section 137 i DPA 2018, se betragtning 17.

([88]) Section 137 og 138 i DPA 2018 indeholder en række sikkerhedsforanstaltninger, der skal sikre, at gebyrerne fastsættes på et passende niveau. Navnlig anføres i Section 137(4) de forhold, som Secretary of State skal tage hensyn til ved fastsættelsen af det beløb, som forskellige organisationer skal betale. For det andet indeholder Section 138(1) og Section 182 i DPA 2018 også et lovkrav om, at Secretary of State skal rådføre sig med Information Commissioner og andre repræsentanter for personer, der kan blive berørt af bestemmelserne, inden de fastsættes, således at der kan tages hensyn til deres synspunkter. I henhold til Section 138(2) i DPA 2018 skal ICO desuden føre tilsyn med, hvordan bestemmelserne om afgifter fungerer, og Information Commissioner kan forelægge Secretary of State forslag til ændringer af bestemmelserne. Endelig gælder det, at undtagen i de tilfælde, hvor der kun er fastsat bestemmelser for at tage hensyn til en stigning i detailprisindekset (i hvilke tilfælde de vil være omfattet af den negative beslutningsprocedure), er bestemmelserne underlagt den positive beslutningsprocedure og kan først vedtages, når de er blevet godkendt ved beslutning truffet af hvert af parlamentets kamre.

([89]) I forvaltningsaftalen præciseres det, at » Secretary of State kan betale ICO midler, som parlamentet har stillet til rådighed i henhold til paragraph 9 i Schedule 12 til DPA 2018. Efter høring af ICO udbetaler DCMS passende beløb (tilskud) til ICO's administrationsomkostninger og udøvelsen af ICO's funktioner i forbindelse med en række specifikke funktioner, herunder informationsfrihed (Management Agreement 2018-2021, paragraph 1.12, jf. fodnote 82).

([90]) Se Section 134 i DPA 2018.

regeringen eller andre institutioner og organer samt til offentligheden om ethvert spørgsmål vedrørende beskyttelse af personoplysninger. Af hensyn til opretholdelsen af retsvæsenets uafhængighed har Information Commissioner ikke bemyndigelse til at udøve sine funktioner i forbindelse med behandling af personoplysninger, som foretages af en person, der handler i egenskab af domstol, eller en ret, som handler i sin egenskab af domstol. Tilsynet med retsvæsenet varetages imidlertid af specialiserede organer (se betragtning 99 til 103.

2.6.2. *Håndhævelse, herunder sanktioner*

(92) Information Commissioners beføjelser er fastsat i artikel 58 i UK GDPR, som ikke indfører væsentlige ændringer af den tilsvarende artikel i forordning (EU) 2016/679. I DPA 2018 er der fastsat supplerende regler for, hvordan disse beføjelser kan udøves. Information Commissioner har navnlig beføjelse til at a) pålægge den dataansvarlige og databehandleren (og under visse omstændigheder enhver anden person) at fremlægge nødvendige oplysninger ved at sende en anmodning om oplysninger (»information notice«) ([91]), b) gennemføre undersøgelser og revisioner ved at sende et vurderingsvarsel (»assessment notice«) ([92]), hvori det kan kræves, at den dataansvarlige eller databehandleren giver Information Commissioner tilladelse til at få adgang til bestemte lokaler, inspicere eller undersøge dokumenter eller udstyr, interviewe personer, der behandler personoplysninger på vegne af den dataansvarlige, osv.), c) på anden måde få adgang til dataansvarliges og databehandleres dokumenter m.v. og deres lokaler i overensstemmelse med Section 154 i DPA 2018 (»powers of entry and inspection« — adgangs- og undersøgelsesbeføjelser), d) udøve korrigerende beføjelser, bl.a. ved brug af advarsler og irettesættelser, eller udstede påbud ved hjælp af en »enforcement notice« (håndhævelsesmeddelelse), der pålægger dataansvarlige/databehandlere at tage eller undlade at tage bestemte skridt, herunder at gøre alt, hvad der er angivet i artikel 58, stk. 2, litra c)-g) og litra j), i UK GDPR (»enforcement notice«) ([93]), og e) udstede administrative bøder i form af en »penalty notice« ([94]) (bødeforlæg). Sidstnævnte kan også udstedes, hvis en offentlig myndighed ikke har overholdt bestemmelserne i UK GDPR ([95]).

(93) I ICO's Regulatory Action Policy (politik for reguleringsmæssige foranstaltninger) fastsættes de omstændigheder, hvorunder organet vil udstede en »information notice«, »assessment notice«, »enforcement notice« eller »penalty notice« ([96]). Et »enforcement notice«, der gives som følge af en dataansvarligs eller databehandlers manglende overholdelse, må kun stille krav, som Information Commissioner finder passende med henblik på at afhjælpe fejlen. Der kan udstedes en »enforcement notice« og en »penalty notice« til en dataansvarlig eller databehandler vedrørende overtrædelser af kapitel II i UK GDPR (principper for behandling), artikel 12-22 (den registreredes rettigheder), artikel 25-39 (dataansvarliges og databehandleres forpligtelser) og artikel 44-49 (internationale overførsler) i UK GDPR. Der kan også gives en »enforcement notice«, hvis en dataansvarlig ikke har overholdt kravet om betaling af en afgift i henhold til Section 137 i DPA 2018. Desuden kan et kontrolorgan i henhold til artikel 41 eller et certificeringsorgan få en »enforcement notice«, hvis det ikke opfylder sine forpligtelser i henhold til UK GDPR. Der kan også gives en »penalty notice« til en person, der ikke har efterkommet en »information notice«, en »assessment notice« eller en »enforcement notice«.

(94) I en »penalty notice« pålægges modtageren at betale Information Commissioner et beløb, der er anført i bødeforlægget. Når Information Commissioner vurderer, om der skal gives en »penalty notice« til en person, og fastsætter sanktionens størrelse, skal vedkommende tage hensyn til de forhold, der er anført i artikel 83, stk. 1 og 2, i UK GDPR, som er identiske med de tilsvarende regler i forordning (EU) 2016/679 ([97]). I henhold til artikel 83, stk. 4 og 5, kan de administrative bøder i tilfælde af manglende overholdelse af de forpligtelser, der er omhandlet i disse

([91]) Section 142 i DPA 2018 (med forbehold af begrænsningerne i Section 143 i samme retsakt).
([92]) Section 146 i DPA 2018 (med forbehold af begrænsningerne i Section 147 i samme retsakt).
([93]) Section 149 til 151 i DPA 2018 (med forbehold af begrænsningerne i Section 152 i samme retsakt).
([94]) Section 155 i DPA 2018 og artikel 83 i UK GDPR.
([95]) Dette følger af Section 155(1) i DPA 2018, sammenholdt med Section 149(2) og (5) i DPA 2018, og af Section 156(4) i DPA 2018, som begrænser udstedelsen af bødepålæg til Crown Estate Commissioners og dataansvarlige for Royal Household i henhold til Section 209(4) i DPA 2018.
([96]) Regulatory Action Policy kan findes på følgende link: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([97]) Herunder overtrædelsens art og grovhed (under hensyntagen til den pågældende behandlings karakter, omfang og formål samt antallet af berørte registrerede og omfanget af den skade, de har lidt), overtrædelsens forsætlige eller uagtsomme karakter, enhver foranstaltning, som den dataansvarlige har truffet for at begrænse den skade, som de registrerede har lidt, graden af den dataansvarliges eller databehandlerens ansvar (under hensyntagen til tekniske og organisatoriske foranstaltninger, som den dataansvarlige eller databehandleren har gennemført), samt enhver relevant tidligere overtrædelse, som den dataansvarlige eller databehandleren har begået, graden af samarbejde med Information Commissioner, de kategorier af personoplysninger, der er berørt af den manglende overholdelse, enhver anden skærpende eller formildende omstændighed, der finder anvendelse på sagens omstændigheder, såsom opnåede økonomiske fordele eller direkte eller indirekte undgåede tab som følge af overtrædelsen.

bestemmelser, højst udgøre henholdsvis 8 700 000 GBP og 17 500 000 GBP. Hvis der er tale om en virksomhed, kan Information Commissioner dog også pålægge bøder i procent af den årlige omsætning på verdensplan, hvis dette beløb er højere. Som i de tilsvarende bestemmelser i forordning (EU) 2016/679 er disse beløb fastsat til henholdsvis 2 % og 4 % i henholdsvis artikel 83, stk. 4 og 5. I tilfælde af manglende efterkommelse af en »information notice«, en »assessment notice« eller en »enforcement notice« er maksimumsbeløbet for den sanktion, der kan pålægges ved en »penalty notice«, 17 500 000 GBP eller for en virksomheds vedkommende 4 % af den årlige omsætning på verdensplan, afhængigt af hvilket beløb der er højest.

(95) UK GDPR har sammen med DPA 2018 også styrket en række andre af Information Commissioners beføjelser. For eksempel kan Information Commissioner nu gennemføre obligatoriske revisioner af alle dataansvarlige og databehandlere ved hjælp af »assessment notices«, mens Information Commissioner i henhold til den tidligere lovgivning, Data Protection Act 1998, kun havde denne beføjelse med hensyn til centrale statslige organisationer, herunder sundhedsorganisationer, idet andre skulle acceptere en revision.

(96) Siden indførelsen af forordning (EU) 2016/679 har ICO behandlet ca. 40 000 klager fra registrerede om året, ([98]) og desuden foretager ICO ca. 2 000 undersøgelser på *eget initiativ* ([99]). Størstedelen af klagerne vedrører retten til indsigt i og videregivelse af oplysninger. På baggrund af sine undersøgelser træffer Information Commissioner håndhævelsesforanstaltninger i en bred vifte af sektorer. Mere specifikt har Information Commissioner ifølge sin seneste årsberetning (2019-2020) ([100]) udsendt 54 »information notices«, otte »assessment notices«, syv »enforcement notices«, fire advarsler, otte meddelelser om retsforfølgning og 15 bøder i rapporteringsperioden ([101]).

(97) Der er bl.a. tale om adskillige betydelige økonomiske sanktioner, som er pålagt i henhold til forordning (EU) 2016/679 og DPA 2018. Navnlig pålagde Information Commissioner i oktober 2020 et britisk luftfartsselskab en bøde på 20 mio. GBP for brud på datasikkerheden, der berørte mere end 400 000 kunder. Ved udgangen af oktober 2020 blev en international hotelkæde pålagt at betale en bøde på 18,4 mio. GBP for manglende sikker opbevaring af millioner af kunders personoplysninger, og i november 2020 blev en britisk forhandler af billetter til arrangementer online idømt en bøde på 1,25 mio. GBP for manglende beskyttelse af kundernes betalingsoplysninger ([102]).

(98) Information Commissioner har en række håndhævelsesbeføjelser, som er beskrevet i betragtning 92. Derudover findes der visse overtrædelser af databeskyttelseslovgivningen, som udgør strafbare handlinger og derfor kan gøres til genstand for strafferetlige sanktioner (Section 196 i DPA 2018). Der kan f.eks. være tale om bevidst eller letsindig indhentning eller videregivelse af personoplysninger uden den dataansvarliges samtykke, videregivelse af personoplysninger til en anden person uden den dataansvarliges samtykke ([103]), fornyet identificering af anonymiserede personoplysninger uden samtykke fra den dataansvarlige, der er ansvarlig for at anonymisere oplysningerne ([104]), bevidst hindring af, at Information Commissioner udøver sine beføjelser med hensyn til gennemgang af personoplysninger i overensstemmelse med internationale forpligtelser ([105]), afgivelse af falske erklæringer som svar på en »information notice« eller tilintetgørelse af oplysninger i forbindelse med »information notices« eller »assessment notices« ([106]).

([98]) Ifølge oplysningerne fra de britiske myndigheder blev der i den periode, der er omfattet af Information Commissioners årsberetning for 2019-2020, ikke konstateret nogen overtrædelse i ca. 25 % af tilfældene. I omkring 29 % af tilfældene blev den registrerede enten bedt om at rette sin første henvendelse til den dataansvarlige, om at afvente den dataansvarliges svar eller om at fortsætte en løbende dialog med denne. I ca. 17 % af tilfældene blev der ikke konstateret nogen overtrædelse, men der blev givet rådgivning til den dataansvarlige. I omkring 25 % af sagerne konstaterede Information Commissioner en overtrædelse, hvorefter kontoret enten rådgav den dataansvarlige, eller denne blev pålagt at træffe visse foranstaltninger. I ca. 3 % af sagerne blev det vurderet, at klagen ikke faldt ind under forordning (EU) 2016/679, mens ca. 1 % af sagerne blev henvist til en anden databeskyttelsesmyndighed inden for rammerne af Det Europæiske Databeskyttelsesråd.

([99]) ICO kan indlede disse undersøgelser på grundlag af oplysninger, som kontoret modtager fra en lang række kilder, herunder anmeldelser om brud på persondatasikkerheden, indberetninger fra andre offentlige myndigheder i Det Forenede Kongerige eller udenlandske databeskyttelsesmyndigheder og klager fra enkeltpersoner eller civilsamfundsorganisationer.

([100]) Information Commissionerens årsberetning og årsregnskab 2019- 2020 (jf. fodnote 81).

([101]) Ifølge den foregående årsberetning for perioden 2018-2019 udstedte Information Commissioner 22 »penalty notices» i henhold til DPA 1998 i rapporteringsperioden. Bøderne beløb sig til i alt 3 010 610 GBP, og der var bl.a. to bøder på 500 000 GBP (det maksimalt tilladte i henhold til DPA 1998). I 2018 gennemførte Information Commissioner navnlig en undersøgelse af anvendelsen af dataanalyser til politiske formål efter afsløringerne i Cambridge Analytica-sagen. Undersøgelsen resulterede i en politikrelateret rapport, en række anbefalinger, en bøde på 500 000 GBP til Facebook og en »enforcement notice« til den canadiske dataformidler Aggregate IQ, hvori sidstnævnte pålægges at slette personoplysninger, som den var i besiddelse af om britiske statsborgere og indbyggere (se Information Commissioners årsrapport og årsregnskab 2018-2019, som kan findes på følgende link: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf) .

([102]) En oversigt over de håndhævelsesforanstaltninger, der er truffet, findes på ICO's websted på følgende link: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) Section 170 i DPA 2018.

([104]) Section 171 i DPA 2018.

([105]) Section 119 i DPA 2018.

([106]) Section 144 og 148 i DPA 2018.

2.6.3. *Tilsyn med retsvæsenet*

(99) Tilsynet med domstolenes og retsvæsenets behandling af personoplysninger er dobbelt. Hvis en indehaver af et retsligt embede eller en ret ikke udøver retslig myndighed, fører ICO tilsyn. Hvis den dataansvarlige udøver retslig myndighed, kan ICO ikke udøve sine kontrolfunktioner ([107]), og kontrollen udføres af særlige organer. Dette afspejler tilgangen i forordning (EU) 2016/679 (artikel 55, stk. 3).

(100) For så vidt angår det andet tilfælde vedrørende retterne i England og Wales og First Tier (ret i første instans) og Upper Tribunals (appeldomstole) i England og Wales udøves denne kontrol navnlig af Judicial Data Protection Panel ([108]). Desuden har Lord Chief Justice og Senior President of Tribunals udstedt en Privacy Notice ([109]), som beskriver, hvordan domstolene i England og Wales behandler personoplysninger med henblik på en judiciel funktion. En lignende notice er blevet udstedt af de nordirske ([110]) og skotske domstole ([111]).

(101) I Nordirland har Lord Chief Justice i Nordirland desuden udnævnt en dommer ved High Court til Data Supervisory Judge (datatilsynsdommer, DSJ) ([112]). Der er også udsendt vejledninger til det nordirske retsvæsen om, hvad de skal gøre i tilfælde af tab eller potentielt tab af data, og om processen for håndtering af eventuelle problemer, der måtte opstå som følge heraf ([113]).

(102) I Skotland har Lord President udnævnt en dommer med ansvar for datatilsyn, som skal undersøge eventuelle klager vedrørende databeskyttelse. Dette er fastsat i de judicielle klageregler, der svarer til reglerne for England og Wales ([114]).

(103) Endelig bør det nævnes, at en af præsidenterne ved den øverste domstol udpeges til at føre tilsyn med databeskyttelsen.

2.6.4. *Klageadgang*

(104) Med henblik på at sikre tilstrækkelig beskyttelse og navnlig håndhævelse af individuelle rettigheder bør den registrerede have effektive muligheder for administrativ og retslig prøvelse, herunder skadeserstatning.

([107]) Section 117 i DPA 2018.

([108]) Panelet er ansvarligt for at yde vejledning og uddannelse til retsvæsenet. Desuden behandler det klager fra registrerede vedrørende den måde, som domstolene og enkeltpersoner, der handler i egenskab af domstol, behandler personoplysninger på. Panelet bestræber sig på at sikre behandling af enhver klage. Hvis en klager ikke er tilfreds med en afgørelse, som panelet har truffet, og fremlægger yderligere beviser, kan panelet tage sin afgørelse op til fornyet overvejelse. Panelet pålægger ikke selv økonomiske sanktioner, men hvis det mener, at der foreligger en tilstrækkelig alvorlig overtrædelse af DPA 2018, kan det henvise sagen til Judicial Conduct Investigation Office (JCIO — kontoret for retlig efterforskning af adfærd), som vil undersøge klagen. Hvis klagen anses for berettiget, er det op til Lord Chancellor (lordkansleren) og Lord Chief Justice (eller en højtstående dommer, der er bemyndiget til at handle på hans vegne) at afgøre, hvilke foranstaltninger der skal træffes over for den person eller instans, som der klages over. Der kan afhængigt af sagens alvor være tale om bl.a. en formel henstilling, en formel advarsel, en irettesættelse og i sidste ende afskedigelse. Hvis en person er utilfreds med den måde, som har JCIO undersøgt klagen på, kan vedkommende sende sin klage videre til Judicial Appointments and Conduct Ombudsman (ombudsmanden for udpegelser og adfærd) (se https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Denne ombudsmand har beføjelse til at anmode JCIO om at undersøge en klage igen og kan foreslå, at klageren får erstatning, hvis den mener, at klageren har lidt skade som følge af fejl eller forsømmelser.

([109]) Denne Privacy Notice fra Lord Chief Justice og Senior President of Tribunals findes på følgende link: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([110]) Meddelelsen om beskyttelse af privatlivets fred, der er udsendt af Lord Chief Justice i Nordirland, findes på følgende link: https://judiciaryni.uk/data-privacy

([111]) »Privacy Notice« for skotske domstole og retter kan findes på følgende link: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([112]) DSJ vejleder retsvæsenet og undersøger overtrædelser og/eller klager i forbindelse med domstolenes eller enkeltpersoners behandling af personoplysninger.

([113]) Hvis klagen eller overtrædelsen anses for at være alvorlig, henvises den til Judicial Complaints Officer (en klageinstans) med henblik på yderligere efterforskning i overensstemmelse med Lord Chief Justice of Northern Ireland's Code of Practice on Complaints (kodeks om klager). En sådan klage kan bl.a. få følgende resultater: ingen yderligere foranstaltninger, rådgivning, uddannelse eller mentorhjælp, uformel advarsel, formel advarsel, endelig advarsel, begrænsning af praksis eller henvisning til et lovpligtigt nævn. Code of Practice on Complaints fra Lord Chief Justice of Northern Ireland kan findes på følgende link: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.

([114]) Enhver begrundet klage undersøges af Data Supervisory Judge og henvises til Lord President, som har beføjelse til at yde rådgivning eller udstede en formel advarsel eller en irettesættelse, hvis han finder det nødvendigt (der findes tilsvarende regler for medlemmer af retterne, som findes på følgende link: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) For det første har den registrerede ret til at indgive en klage til Information Commissioner, hvis han eller hun mener, at der i forbindelse med personoplysninger om vedkommende er tale om en overtrædelse af UK GDPR ([115]). UK GDPR bibeholder bestemmelserne i artikel 77 i forordning (EU) 2016/679 om denne ret uden væsentlige ændringer. Det samme gælder artikel 57, stk. 1, litra f), og stk. 2, der fastsætter Information Commissioners opgaver i forbindelse med behandling af klager. Som beskrevet i betragtning 92 til 98 ovenfor har Information Commissioner beføjelse til at vurdere den dataansvarliges og databehandlerens overholdelse af UK GDPR og DPA 2018, pålægge dem at træffe eller undlade at træffe bestemte foranstaltninger i tilfælde af manglende overholdelse og pålægge bøder.

(106) For det andet sikrer UK GDPR og DPA 2018 adgang til retsmidler over for Information Commissioner. I henhold til artikel 78, stk. 1, i UK GDPR har en person ret til effektive retsmidler mod en juridisk bindende afgørelse truffet af Information Commissioner vedrørende vedkommende. I forbindelse med domstolsprøvelsen undersøger dommeren den afgørelse, der anfægtes i klagen, og undersøger, om Information Commissioner har handlet lovligt. Desuden har ([116]) klageren i henhold til artikel 78, stk. 2, i UK GDPR adgang til retsmidler, hvis Information Commissioner ikke behandler vedkommendes klage korrekt. Klageren kan anmode en First Tier Tribunal (førsteinstansret) om at pålægge Information Commissioner at træffe passende foranstaltninger til at besvare klagen eller underrette klageren om de fremskridt, der gøres i behandlingen af klagen ([117]). Desuden kan enhver person, som Information Commissioner forkynder en af ovennævnte meddelelser (»information notice«, »assessment notice«, »enforcement notice« eller »penalty notice«) over for, indbringe sagen for en First Tier Tribunal ([118]). Hvis denne First Tier Tribunal finder, at Information Commissioners afgørelse ikke er i overensstemmelse med loven, eller hvis Information Commissioner burde have udøvet sin skønsbeføjelse anderledes, skal retten tage appellen til følge eller erstatte en anden meddelelse eller afgørelse, som Information Commissioner måtte have forkyndt eller truffet.

(107) For det tredje kan enkeltpersoner anlægge sag direkte mod dataansvarlige og databehandlere ved domstolene i henhold til artikel 79 i UK GDPR og Section 167 i DPA 2018. Hvis en domstol efter anmodning fra en registreret finder det godtgjort, at der er sket en krænkelse af den registreredes rettigheder i henhold til databeskyttelseslovgivningen, kan domstolen pålægge den dataansvarlige for så vidt angår behandlingen eller en databehandler, der handler på vegne af den dataansvarlige, at træffe de foranstaltninger, der er angivet i kendelsen, eller at undlade at træffe de foranstaltninger, der er angivet i kendelsen.

(108) I henhold til artikel 82 i UK GDPR og Section 168 i DPA 2018 har enhver person, der har lidt materiel eller immateriel skade som følge af en overtrædelse af UK GDPR, desuden ret til erstatning for den lidte skade fra den dataansvarlige eller databehandleren. Reglerne om erstatning og ansvar i artikel 82, stk. 1-5, i UK GDPR er identiske med de tilsvarende regler i forordning (EU) 2016/679. I henhold til Section 168 i DPA 2018 omfatter ikkemateriel skade også overlast. I henhold til artikel 80 i UK GDPR har den registrerede også ret til at bemyndige et repræsentativt organ eller en organisation til at indgive klagen til Information Commissioner på dennes vegne (i henhold til artikel 77 i UK GDPR) og til at udøve de rettigheder, der er omhandlet i artikel 78 (ret til adgang til effektive retsmidler mod Information Commissioner), artikel 79 (ret til effektive retsmidler mod en dataansvarlig eller databehandler) og artikel 82 (ret til erstatning og ansvar) i UK GDPR på hans eller hendes vegne.

(109) Ud over disse klagemuligheder kan enhver person, der mener, at vedkommendes rettigheder, herunder retten til privatlivets fred og beskrevet ovenfor databeskyttelse, er blevet krænket af offentlige myndigheder, indbringe sagen for domstolene i Det Forenede Kongerige i henhold til Human Rights Act 1998 ([119]). En person, der hævder, at en offentlig myndighed har handlet (eller agter at handle) på en måde, der er uforenelig med en konventionsbaseret rettighed og dermed ulovlig i henhold til Section 6(1) i Human Rights Act 1998, kan anlægge sag mod myndigheden ved den relevante domstol eller påberåbe sig de pågældende rettigheder i en retssag, hvis vedkommende er (eller ville være) offer for den ulovlige handling.

(110) Hvis retten fastslår, at en handling fra en offentlig myndigheds side er ulovlig, kan den træffe en sådan foranstaltning, anvende et sådant retsmiddel eller træffe en sådan afgørelse inden for rammerne af sine beføjelser, som den finder passende ([120]). Retten kan også erklære en bestemmelse i den primære lovgivning uforenelig med en ret i henhold til en konvention.

([115]) Artikel 77 i UK GDPR.

([116]) Section 166 i DPA 2018 omhandler specifikt følgende situationer: a) Information Commissioner undlader at træffe passende foranstaltninger for at reagere på klagen, b) Information Commissioner undlader at give klageren oplysninger om forløbet af klagen eller om resultatet af klagen inden udløbet af den periode på 3 måneder, der begynder på det tidspunkt, hvor Information Commissioner modtager klagen, eller c) hvis Information Commissioners behandling af klagen ikke er afsluttet i løbet af denne periode, undlader at give klageren sådanne oplysninger i en efterfølgende periode på 3 måneder.

([117]) Artikel 78, stk. 2, i UK GDPR og Section 166 i DPA 2018.

([118]) Artikel 78, stk. 1, i UK GDPR og Section 162 i DPA 2018.

([119]) Section 7(1) i Human Rights Act 1998. I henhold til Section 7(7) er en person kun offer for en ulovlig handling, hvis han ville være offer som omhandlet i artikel 34 i den europæiske menneskerettighedskonvention, hvis der blev anlagt sag ved Den Europæiske Menneskerettighedsdomstol vedrørende denne handling.

([120]) Section 8(1) i Human Rights Act 1998.

(111) Endelig kan en person efter at have udtømt mulighederne i de nationale retsmidler indbringe en klage for Den Europæiske Menneskerettighedsdomstol over krænkelser af de rettigheder, der er garanteret i henhold til den europæiske menneskerettighedskonvention.

3. DET FORENEDE KONGERIGES MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER OVERFØRT FRA DEN EUROPÆISKE UNION

(112) Kommissionen har også vurderet Det Forenede Kongeriges retlige ramme for Det Forenede Kongeriges offentlige myndigheders indsamling og efterfølgende anvendelse af personoplysninger, der overføres til erhvervsdrivende i Det Forenede Kongerige, i offentlighedens interesse, navnlig med henblik på retshåndhævelse og national sikkerhed (i det følgende benævnt »myndighedsadgang«). Ved vurderingen af, om de betingelser, hvorunder myndighedsadgangen til oplysninger, der overføres til Det Forenede Kongerige i medfør af denne afgørelse, opfylder væsentlighedskriteriet i henhold til artikel 45, stk. 1, i forordning (EU) 2016/679, som fortolket af Den Europæiske Unions Domstol i lyset af chartret om grundlæggende rettigheder, har Kommissionen navnlig taget hensyn til følgende kriterier.

(113) For det første skal enhver begrænsning af retten til beskyttelse af personoplysninger være fastsat ved lov, og det retsgrundlag, der gør det muligt at gribe ind i en sådan ret, skal selv fastlægge omfanget af begrænsningen af udøvelsen af den pågældende rettighed ([121]).

(114) For at opfylde kravet om proportionalitet, som indebærer, at undtagelser fra og begrænsninger af beskyttelsen af personoplysninger kun finder anvendelse i det omfang, det er strengt nødvendigt i et demokratisk samfund for at opfylde specifikke mål af almen interesse svarende til dem, der er anerkendt af Unionen, skal den lovgivning i det pågældende tredjeland, der tillader dette indgreb, for det andet fastsætte klare og præcise regler for omfanget og anvendelsen af de pågældende foranstaltninger og fastsætte minimumsgarantier, således at de personer, hvis oplysninger er blevet videregivet, har tilstrækkelige garantier til effektivt at beskytte deres personoplysninger mod risikoen for misbrug ([122]). Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan vedtages ([123]) en foranstaltning om behandling af sådanne oplysninger. Desuden skal den sikre et uafhængigt tilsyn med, at disse krav opfyldes ([124]).

(115) For det tredje skal den pågældende lovgivning være retligt bindende i henhold til national ret, og disse retlige krav skal ikke blot være bindende for myndighederne, men også kunne håndhæves ved domstolene over for myndighederne i det pågældende tredjeland ([125]). De registrerede skal navnlig have mulighed for at anlægge sag ved en uafhængig og upartisk domstol for at få adgang til deres personoplysninger eller for at få dem berigtiget eller slettet ([126]).

3.1. Den overordnede retlige ramme

(116) Hvis offentlige myndigheder opnår adgang til oplysninger i forbindelse med udøvelse af beføjelser i Det Forenede Kongerige, skal det ske under fuld overholdelse af loven. Det Forenede Kongerige har ratificeret den europæiske menneskerettighedskonvention (se betragtning 9), og alle offentlige myndigheder i Det Forenede Kongerige skal handle i overensstemmelse med konventionen ([127]). Konventionens artikel 8 bestemmer, at ethvert indgreb i privatlivets fred skal være i overensstemmelse med loven, tjene et af formålene i artikel 8, stk. 2, og stå i rimeligt forhold til dette formål. Artikel 8 kræver også, at indgrebet skal være »forudsigeligt«, dvs. at det har et klart og tilgængeligt retsgrundlag, og at loven indeholder passende garantier til at forhindre misbrug.

(117) Desuden har Den Europæiske Menneskerettighedsdomstol i sin retspraksis præciseret, at ethvert indgreb i retten til privatlivets fred og databeskyttelse bør være underlagt et effektivt, uafhængigt og upartisk tilsynssystem, som enten en dommer eller et andet uafhængigt organ ([128]) (f.eks. en administrativ myndighed eller et parlamentarisk organ) stiller til rådighed.

([121]) Se Schrems II, præmis 174-175 og den nævnte retspraksis. Se også sag C-623/17 Privacy International ECLI:EU:C:2020:790, præmis 65, for så vidt angår adgang for medlemsstaternes offentlige myndigheder og forenede sager C-511/18, C-512/18 og C-520/18, La Quadrature du Net m.fl., ECLI:EU:C:2020:791, præmis 175.

([122]) Se Schrems II-sagen, præmis 176 og 181, og den nævnte retspraksis. Se også Privacy International, præmis 68, for så vidt angår adgang for offentlige myndigheder i medlemsstaterne og La Quadrature du Net m.fl., præmis 132.

([123]) Se Schrems II-sagen, præmis 176. Se også Privacy International, præmis 68, for så vidt angår adgang for offentlige myndigheder i medlemsstaterne og La Quadrature du Net m.fl., præmis 132.

([124]) Se Schrems II-sagen, præmis 179.

([125]) Se Schrems II-sagen, præmis 181-182.

([126]) Se Schrems I-sagen, præmis 95, og Schrems II-sagen, præmis 194. I den forbindelse har EU-Domstolen navnlig understreget, at overholdelsen af artikel 47 i chartret om grundlæggende rettigheder, der garanterer retten til effektive retsmidler ved en uafhængig og upartisk domstol, »bidrager til det krævede beskyttelsesniveau i Den Europæiske Union […], som Kommissionen skal fastslå er overholdt, før den vedtager en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til databeskyttelsesforordningens artikel 45, stk. 1«, i forordning (EU) 2016/679 (Schrems II, præmis 186).

([127]) Section 6 i Human Rights Act 1998.

([128]) Den Europæiske Menneskerettighedsdomstol, Klass m.fl. mod Tyskland, ansøgning nr. 5029/71, præmis 17- 51.

(118) Desuden skal enkeltpersoner have adgang til effektive retsmidler, og Den Europæiske Menneskerettighedsdomstol har præciseret, at disse retsmidler skal tilbydes af et uafhængigt og upartisk organ, der har vedtaget sin egen forretningsorden, og som består af medlemmer, der skal have eller have haft et højt dommerembede, eller erfarne advokater, og at der ikke må være nogen bevisbyrde, der skal overvindes for at indgive en ansøgning til den. Når det uafhængige og upartiske organ foretager sin undersøgelse af klager fra enkeltpersoner, bør det have adgang til alle relevante oplysninger, herunder fortrolige oplysninger. Endelig bør organet have beføjelse til at afhjælpe manglende overholdelse ([129]).

(119) Det Forenede Kongerige har også ratificeret Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108) og undertegnet protokollen om ændring af konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108+) i 2018 ([130]). Artikel 9 i konvention nr. 108 bestemmer, at undtagelser fra de generelle databeskyttelsesprincipper (artikel 5 om oplysningernes kvalitet), reglerne for særlige kategorier af oplysninger (artikel 6) og den registreredes rettigheder (artikel 8 om yderligere garantier for den registrerede) kun kan indrømmes, hvis en sådan undtagelse er fastsat i det pågældende lands lovgivning og udgør en nødvendig foranstaltning i et demokratisk samfund af hensyn til statens sikkerhed, den offentlige sikkerhed, statens monetære interesser eller bekæmpelsen af strafbare handlinger eller beskyttelsen af den registrerede eller andres rettigheder og frihedsrettigheder ([131]).

(120) Som følge af medlemskabet af Europarådet, tilslutningen til den europæiske menneskerettighedskonvention og anerkendelse af Den Europæiske Menneskerettighedsdomstols kompetence er Det Forenede Kongerige derfor underlagt en række forpligtelser, der er fastsat i folkeretten, og som fastlægger landets system for myndighedsadgang på grundlag af principper, garantier og individuelle rettigheder svarende til dem, der er garanteret i henhold til EU-retten og finder anvendelse på medlemsstaterne. Som understreget i betragtning 19 er fortsat overholdelse af sådanne instrumenter derfor et særligt vigtigt element i den vurdering, som denne afgørelse er baseret på.

(121) Endvidere sikrer DPA 2018 en række specifikke databeskyttelsesgarantier og -rettigheder, når data behandles af offentlige myndigheder, herunder retshåndhævende organer og organer med ansvar for statens sikkerhed.

(122) Navnlig er ordningen for behandling af personoplysninger i forbindelse med strafferetlig håndhævelse fastsat i Part 3 i DPA 2018, som blev vedtaget for at gennemføre direktiv (EU) 2016/680. Part 3 i DPA 2018 finder anvendelse på kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed ([132]).

(123) Begrebet »kompetent myndighed« er fastsat i Section 30, DPA, som en person, der er opført på fortegnelsen i DPA 2018, Schedule 7, samt enhver anden person, i det omfang personen har lovbestemte funktioner i forbindelse med et hvilket som helst retshåndhævelsesformål ([133]). Som forklaret nedenfor (se betragtning 139) kan visse kompetente myndigheder (f.eks. National Crime Agency (det nationale kontor for kriminalitet)) på visse betingelser gøre brug af de beføjelser, der er fastsat i Investigatory Power Act 2016 (IPA 2016). I dette tilfælde vil de garantier, der er fastsat i IPA 2016, finde anvendelse ud over dem, der er fastsat i Part 3 i DPA 2018. Efterretningstjenesterne (Secret Intelligence Service, Security Service og Government Communications Headquarters) er ikke »kompetente myndigheder« ([134]) henhørende under Part 3 i DPA 2018, og derfor finder reglerne ikke anvendelse på deres aktiviteter. En specifik del af DPA 2018 (Part 4) omhandler efterretningstjenesternes behandling af personoplysninger (se betragtning 125 for yderligere oplysninger).

([129]) Den Europæiske Menneskerettighedsdomstol, Kennedy mod Det Forenede Kongerige, ansøgning nr. 26839/05 (»Kennedy«), præmis 167 og 190.

([130]) Se betragtning 9 ovenfor for yderligere oplysninger om den europæiske menneskerettighedskonvention og indarbejdelsen af den i Det Forenede Kongeriges lovgivning gennem Human Rights Act 1998 samt konvention 108.

([131]) I henhold til artikel 11 i konvention 108+ er begrænsning af visse specifikke rettigheder og forpligtelser i konventionen af hensyn til den nationale sikkerhed eller forebyggelse, efterforskning og retsforfølgning af straffelovsovertrædelser og fuldbyrdelse af strafferetlige sanktioner ligeledes kun tilladt, når en sådan begrænsning er fastsat ved lov, respekterer kernen i de grundlæggende rettigheder og frihedsrettigheder og udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund. Behandlingsaktiviteter til formål, der vedrører statens sikkerhed og forsvar, skal også være underlagt uafhængig og effektiv kontrol og tilsyn i henhold til den nationale lovgivning i den pågældende part i konventionen.

([132]) Section 31 i DPA 2018.

([133]) De kompetente myndigheder, der er anført i Schedule 7, omfatter ikke kun politistyrker, men også alle ministerielle forvaltningsgrene i Det Forenede Kongerige samt andre myndigheder med undersøgelsesfunktioner (f.eks. Commissioner for Her Majesty's Revenue and Customs (toldvæsenet), National Crime Agency (det nationale kontor for kriminalitet), Welsh Revenue Authority (Wales' afgiftsmyndighed), Competition and Markets Authority (konkurrence- og markedsmyndigheden) eller Her Majesty's Land Register (ejendomsregistret)), anklagemyndigheder, andre strafferetlige myndigheder og tilsvarende eller organisationer, der udfører retshåndhævelsesaktiviteter (blandt disse findes der i Schedule 7 til DPA 2018 en fortegnelse over Directors of Public Prosecutors, Director of Public Prosecutors for Northern Ireland eller Information Commission).

([134]) Section 30(2) i DPA 2018.

(124) Ligesom direktiv (EU) 2016/680 fastsætter Part 3 i DPA 2018 principperne om lovlighed og rimelighed ([135]), formålsbegrænsning ([136]), dataminimering ([137]), nøjagtighed ([138]), opbevaringsbegrænsning ([139]) og sikkerhed ([140]). Lovgivningen pålægger specifikke gennemsigtighedsforpligtelser ([141]) og giver enkeltpersoner ret til indsigt ([142]), berigtigelse og sletning ([143]) og ret til ikke at være genstand for automatisk beslutningstagning ([144]). De kompetente myndigheder skal også gennemføre databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, føre fortegnelser over behandlingsaktiviteter og, i forbindelse med visse behandlingsaktiviteter, foretage konsekvensanalyser vedrørende databeskyttelse og på forhånd rådføre sig med Information Commissioner ([145]). I henhold til Section i DPA 2018 skal de påvise overensstemmelse. De er desuden forpligtet til at træffe passende foranstaltninger til at garantere behandlingssikkerheden ([146]), ligesom de er underlagt særlige forpligtelser i tilfælde af brud på datasikkerheden, bl.a. med hensyn til anmeldelse af sådanne brud til Information Commissioner og registrerede ([147]). Som det er tilfældet i direktiv (EU) 2016/680, er der også et krav om, at en dataansvarlig (medmindre der er tale om en domstol eller en anden retsmyndighed, der handler i sin egenskab af domstol) skal udpege en databeskyttelsesrådgiver ([148]), som bistår den dataansvarlige med at opfylde sine forpligtelser og overvåge ovennævnte overensstemmelse ([149]). Desuden indeholder lovgivningen særlige krav til internationale overførsler af personoplysninger til tredjelande eller internationale organisationer med henblik på retshåndhævelse for at sikre kontinuitet i beskyttelsen ([150]). På datoen for vedtagelse af denne afgørelse har Kommissionen vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet på grundlag af artikel 36, stk. 3, i direktiv (EU) 2016/680, hvori det fastslås, at den databeskyttelsesordning, der gælder for Det Forenede Kongeriges strafferetshåndhævende myndigheders behandling af oplysninger, sikrer et beskyttelsesniveau, som i det væsentlige svarer til det, der sikres ved direktiv (EU) 2016/680.

(125) Part 4 i DPA 2018 finder anvendelse på al behandling, der foretages af eller på vegne af efterretningstjenesterne. Navnlig fastsætter denne del de vigtigste databeskyttelsesprincipper (lovlighed, rimelighed og gennemsigtighed ([151]), formålsbegrænsning ([152]), dataminimering ([153]), nøjagtighed ([154]), opbevaringsbegrænsning ([155]) og sikkerhed ([156])). Derudover fastsætter den en række betingelser for behandling af særlige kategorier af oplysninger ([157]), ligesom den fastlægger de registreredes rettigheder ([158]), kræver

([135]) Section 35 i DPA 2018.
([136]) Section 36 i DPA 2018.
([137]) Section 37 i DPA 2018.
([138]) Section 38 i DPA 2018.
([139]) Section 39 i DPA 2018.
([140]) Section 40 i DPA 2018.
([141]) Section 44 i DPA 2018.
([142]) Section 45 i DPA 2018.
([143]) Section 46 og 47 i DPA 2018.
([144]) Section 49 og 50 i DPA 2018.
([145]) Section 56-65 i DPA 2018.
([146]) Section 66 i DPA 2018.
([147]) Section 67(-68) i DPA 2018.
([148]) Section 69-71 i DPA 2018.
([149]) Section 67(-68) i DPA 2018.
([150]) Chapter 5 i Part 3 i DPA 2018.
([151]) Med henblik på at fastslå databehandlingens rimelighed og gennemsigtighed skal der i henhold til Section 86(6) i DPA 2018 tages hensyn til den metode, der anvendes til at indhente oplysningerne. I den henseende opfyldes kravet om rimelighed og gennemsigtighed, hvis oplysningerne indhentes fra en person, der er lovligt bemyndiget eller forpligtet til at fremlægge dem.
([152]) I henhold til Section 87 i DPA 2018 skal formålet med behandlingen være udtrykkeligt angivet og legitimt. Oplysningerne må ikke behandles på en måde, der er uforenelig med de formål, hvortil de indsamles. I henhold til Section 87(3) i DPA 2018 kan forenelig behandling af personoplysninger til et andet formål kun tillades, hvis den dataansvarlige ved lov er bemyndiget til at behandle oplysningerne til dette formål, og behandlingen er nødvendig og står i rimeligt forhold til det oprindelige formål. Behandlingen bør anses for at være forenelig, hvis den består i behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål og er underlagt de fornødne garantier (Section 87(4) i DPA 2018).
([153]) Personoplysninger skal være tilstrækkelige, relevante og ikke uforholdsmæssigt omfattende (Section 88 i DPA 2018).
([154]) Personoplysninger skal være korrekte og ajourførte (Section 89 i DPA 2018).
([155]) Personoplysninger må ikke opbevares længere end nødvendigt (Section 90 i DPA 2018).
([156]) Det sjette databeskyttelsesprincip er, at personoplysninger skal behandles på en måde, der omfatter passende sikkerhedsforanstaltninger for så vidt angår risici, der opstår som følge af behandling af personoplysninger. Disse risici omfatter (men er ikke begrænset til) utilsigtet eller uautoriseret adgang til eller tilintetgørelse, tab, brug, ændring eller videregivelse af personoplysninger (Section 91 i DPA 2018). Section 107 kræver også, at 1) hver dataansvarlig skal træffe sikkerhedsforanstaltninger, som er passende i forhold til de risici, der opstår som følge af behandling af personoplysninger, og at 2) hver dataansvarlig og hver databehandler i tilfælde af automatisk behandling gennemfører forebyggende eller afhjælpende foranstaltninger baseret på en risikovurdering.
([157]) Section 86(2)(b) i og Schedule 10 til DPA 2018.
([158]) Chapter 3 i Part 4 i DPA 2018, navnlig rettighederne til: indsigt, berigtigelse og sletning, retten til at gøre indsigelse mod behandlingen, retten til ikke at blive underlagt automatisk beslutningstagning og til at gribe ind over for denne samt retten til at blive informeret om beslutningstagningen. Desuden skal den dataansvarlige give den registrerede oplysninger om behandlingen af vedkommendes personoplysninger. Som forklaret i ICO's retningslinjer om efterretningstjenesternes behandling kan enkeltpersoner udøve alle deres rettigheder (herunder en anmodning om berigtigelse) ved at indgive en klage til ICO eller indbringe sager for retten (se ICO's retningslinjer om efterretningstjenesters behandling, som findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

databeskyttelse gennem design ([159]) og regulerer internationale overførsler af personoplysninger ([160]). ICO har for nylig udsendt detaljerede retningslinjer for efterretningstjenesternes behandling i henhold til Part 4 i DPA 2018 ([161]).

(126) Samtidig indeholder Section 110 i DPA 2018 en undtagelse fra bestemte bestemmelser i Part 4 i DPA 2018 ([162]), når en sådan undtagelse er nødvendig af hensyn til statens sikkerhed. Denne undtagelse kan gøres gældende på grundlag af en vurdering af den konkrete sag ([163]). Som forklaret af Det Forenede Kongeriges myndigheder og bekræftet af retspraksis skal en »dataansvarlig overveje de faktiske konsekvenser for statens sikkerhed eller det nationale forsvar, hvis vedkommende skal overholde den særlige databeskyttelsesbestemmelse, og vurdere, om vedkommende med rimelighed kan overholde den sædvanlige regel uden at påvirke statens sikkerhed eller det nationale forsvar« ([164]). ICO fører tilsyn med, om undtagelser er blevet anvendt korrekt ([165]).

(127) Hvad angår muligheden for at begrænse anvendelsen af ovenstående specifikke bestemmelser i henhold til Section 111 i DPA 2018 med henblik på beskyttelse af »statens sikkerhed«, gælder det desuden, at en dataansvarlig kan anmode om et certifikat underskrevet af en minister eller Attorney General (regeringens og statens øverste juridiske rådgiver), der bekræfter, at en begrænsning af sådanne rettigheder er en nødvendig og forholdsmæssig foranstaltning til beskyttelse af statens sikkerhed ([166]).

(128) Det Forenede Kongeriges regering har udstedt retningslinjer for at hjælpe dataansvarlige, når de overvejer, om de skal ansøge om et certifikat vedrørende statens sikkerhed i henhold til DPA 2018. Heri fremhæves det navnlig, at enhver begrænsning af registreredes ret til beskyttelse af hensyn til statens sikkerhed skal være forholdsmæssig og nødvendig ([167]). Alle nationale sikkerhedscertifikater skal offentliggøres på ICO's websted ([168]).

([159]) Section 103 i DPA 2018.

([160]) Section 109 i DPA 2018. Videregivelse af personoplysninger til internationale organisationer eller lande uden for Det Forenede Kongerige er mulig, hvis videregivelsen er en nødvendig og forholdsmæssig foranstaltning, der gennemføres med henblik på den dataansvarliges lovbestemte funktioner eller til andre formål, der er fastsat i specifikke afsnit i Security Service Act 1989 (lov om sikkerhedstjenesten) og Intelligence Services Act 1994 (lov om efterretningstjenesten).

([161]) ICO's retningslinjer, jf. fodnote 158.
Section 30 i DPA 2018 og Schedule 7 til DPA 2018.

([162]) I Section 110(2), i DPA 2018 opregnes de bestemmelser, som det er tilladt at gøre en undtagelse fra. Disse vedrører bl.a. databeskyttelsesprincipperne (bortset fra princippet om lovlighed), de registreredes rettigheder, forpligtelsen til at underrette Information Commissioner om et brud på datasikkerheden, Information Commissioners undersøgelsesbeføjelser i overensstemmelse med internationale forpligtelser, visse af Information Commissioners håndhævelsesbeføjelser, de bestemmelser, der gør visse overtrædelser af databeskyttelsesreglerne til en strafbar handling, og bestemmelserne vedrørende særlige formål med behandlingen, såsom journalistiske, akademiske eller kunstneriske formål.

([163]) Se Baker mod Secretary of State, jf. fodnote 61.

([164]) UK Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework, s. 15-16 (jf. fodnote 31). Se også dommen i sagen Baker mod Secretary of State (jf. fodnote 61), hvori retten annullerede et nationalt sikkerhedscertifikat udstedt af Home Secretary (indenrigsministeren) og bekræftede anvendelsen af undtagelsen begrundet med statens sikkerhed, idet den fandt, at der ikke var nogen grund til at fastsætte en generel undtagelse for forpligtelsen til at besvare anmodninger om aktindsigt, og at indrømmelse af en sådan undtagelse under alle omstændigheder uden en analyse fra sag til sag oversteg, hvad der var nødvendigt og forholdsmæssigt for beskyttelsen af statens sikkerhed.

([165]) Se aftalememorandummet mellem ICO og UKIC (UK Intelligence Community — den britiske efterretningstjeneste), hvoraf det fremgår, at ICO efter at have modtaget en klage fra en registreret ønsker at sikre sig, at spørgsmålet er blevet behandlet korrekt, og, hvor det er relevant, at en eventuel undtagelse er blevet anvendt korrekt. Aftalememorandum mellem Information Commissioner's Office og Det Forenede Kongeriges efterretningstjeneste, paragraph 16, der kan findes på følgende link: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) Med DPA 2018 blev muligheden for at udstede certifikater i henhold til Section 28(2) i Data Protection Act 1998 ophævet. Der er dog stadig mulighed for at udstede »gamle certifikater« i det omfang, der er en historisk udfordring i henhold til 1998-loven (se paragraph 17 i Part 5 i Schedule 20 til DPA 2018). Denne mulighed forekommer imidlertid meget sjælden og vil kun gælde i begrænsede tilfælde, f.eks. hvor en registreret anfægter anvendelsen af undtagelsen for national sikkerhed i forbindelse med en behandling foretaget af en offentlig myndighed, der har foretaget sin behandling i henhold til 1998-loven. Det skal bemærkes, at Section 28 i DPA 1998 i disse tilfælde finder anvendelse i sin helhed, og at den registrerede derfor har mulighed for at anfægte certifikatet ved domstolen.

([167]) Den britiske regerings Guidance on National Security Certificates (vejledning om nationale sikkerhedscertifikater) i henhold til Data Protection Act 2018, som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Det fremgår af de britiske myndigheders forklaring, at selv om et certifikat er et afgørende bevis for, at undtagelsen for så vidt angår data eller behandling, der er beskrevet i certifikatet, finder anvendelse, fjerner det ikke kravet om, at den dataansvarlige skal overveje, om der er behov for at påberåbe sig undtagelsen i den enkelte sag.

([168]) I henhold til Section 130 i DPA 2018 kan ICO beslutte ikke at offentliggøre teksten eller dele af teksten til certifikatet, hvis det ville stride mod hensynet til den nationale sikkerhed eller være i strid med samfundsinteresserne eller kunne bringe en persons sikkerhed i fare. I sådanne tilfælde vil ICO imidlertid offentliggøre, at certifikatet er udstedt.

(129) Certifikatet bør have en fast gyldighedsperiode på højst fem år, så det regelmæssigt tages op til revision af den udøvende magt ([169]). Certifikatet skal identificere de personoplysninger eller kategorier af personoplysninger, der er omfattet af undtagelsen, samt bestemmelserne i DPA 2018, som undtagelsen finder anvendelse på ([170]).

(130) Det er vigtigt at bemærke, at de nationale sikkerhedscertifikater ikke giver yderligere grund til at begrænse databeskyttelsesrettighederne af hensyn til den nationale sikkerhed. Med andre ord kan den dataansvarlige eller databehandleren kun gøre brug af et certifikat, hvis vedkommende har konkluderet, at det er nødvendigt at påberåbe sig undtagelsen af hensyn til statens sikkerhed, der som forklaret ovenfor skal anvendes fra sag til sag ([171]). Selv om et nationalt sikkerhedscertifikat finder anvendelse på den pågældende sag, kan ICO undersøge, hvorvidt det i et konkret tilfælde var berettiget at påberåbe sig undtagelsen vedrørende statens sikkerhed ([172]).

(131) Enhver person, der berøres direkte af udstedelsen af certifikatet, kan appellere udstedelsen til Upper Tribunal ([173]) eller, hvis certifikatet ([174]) identificerer data ved brug af en generel beskrivelse, anfægte certifikatets anvendelse på specifikke data ([175]). Domstolen tager afgørelsen om at udstede et certifikat op til fornyet overvejelse og afgør, om der var rimelige grunde til at udstede certifikatet ([176]). Den kan tage stilling til en lang række spørgsmål om bl.a. nødvendighed, proportionalitet og lovlighed under hensyntagen til indvirkningen på de registreredes rettigheder og afvejningen af behovet for at beskytte statens sikkerhed. Som følge heraf kan domstolen fastslå, at certifikatet ikke finder anvendelse på specifikke personoplysninger, der er genstand for klagen ([177]).

(132) Der findes en anden gruppe af mulige begrænsninger, som i henhold til Schedule 11 til DPA 2018 ([178]) finder anvendelse på visse bestemmelser i Part 4 i DPA 2018 for at beskytte andre vigtige mål af almen interesse eller beskyttede interesser såsom f.eks. parlamentarisk privilegium, beskyttelse af fortroligheden mellem advokat og klient, gennemførelse af retslige procedurer og sikring af de væbnede styrkers kampeffektivitet ([179]). Der findes undtagelser for anvendelsen af disse bestemmelser enten for visse kategorier af oplysninger (»klassebaseret«) eller i det omfang, at anvendelsen af disse bestemmelser vil kunne skade den beskyttede interesse (»forudsætningsbaseret«) ([180]). Skadebaserede undtagelser kan kun påberåbes, for så vidt anvendelsen af den

([169]) Den britiske regerings Guidance on National Security Certificates, paragraph 15, jf. fodnote 167.

([170]) UK Government Guidance on National Security Certificates, paragraph 5, jf. fodnote 167.

([171]) Jf. fodnote 164.

([172]) I henhold til Section 102 i DPA 2018 skal den dataansvarlige være i stand til at påvise, at den har overholdt DPA 2018. Dette indebærer, at en efterretningstjeneste skal påvise over for ICO, at den, når den påberåber sig undtagelsen, har taget hensyn til sagens særlige omstændigheder. I øvrigt offentliggør ICO en fortegnelse over de nationale sikkerhedscertifikater, som kan findes på følgende link: findes på følgende link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([173]) Upper Tribunal er den domstol, der har kompetence til at behandle klager over afgørelser truffet af lavere forvaltningsdomstole, og har særlig kompetence til at behandle appeller af afgørelser truffet af visse statslige organer.

([174]) Section 111(3) i DPA 2018.

([175]) Section 111(5) i DPA 2018.

([176]) I sagen Baker mod Secretary of State (jf. fodnote 61) ophævede Information Tribunal et nationalt sikkerhedscertifikat udstedt af indenrigsministeriet, idet retten fandt, at der ikke var nogen grund til at fastsætte en generel undtagelse for forpligtelsen til at besvare anmodninger om aktindsigt, og at en sådan undtagelse uden en analyse af den enkelte sag under alle omstændigheder oversteg, hvad der var nødvendigt og forholdsmæssigt af hensyn til beskyttelsen af statens sikkerhed.

([177]) Den britiske regerings Guidance on National Security Certificates, paragraph 25, jf. fodnote 167.

([178]) Der er bl.a. tale om i) databeskyttelsesprincipperne i Part 4, bortset fra kravet om lovlig behandling i henhold til det første princip og det forhold, at behandlingen skal opfylde en af de relevante betingelser i Schedule 9 og 10, ii) de registreredes rettigheder og iii) forpligtelserne vedrørende indberetning af overtrædelser til ICO.

([179]) I Part 4 i DPA 2018 fastsættes den retlige ramme, der gælder for alle former for behandling af personoplysninger, der foretages af efterretningstjenester (og ikke kun for udførelsen af deres nationale sikkerhedsopgaver). Part 4 finder derfor også anvendelse, når efterretningstjenester behandler oplysninger, f.eks. med henblik på forvaltning af menneskelige ressourcer, i forbindelse med retssager eller i forbindelse med offentlige indkøb. De begrænsninger, der er anført i Schedule 11, skal hovedsagelig anvendes i disse andre sammenhænge. I forbindelse med tvister med en ansat kan begrænsningen i forbindelse med »retssager« eksempelvis påberåbes, eller i forbindelse med offentlige indkøb kan begrænsningen i forbindelse med »forhandling« påberåbes osv. Dette afspejles i ICO's retningslinjer om efterretningstjenesters behandling, som nævner forhandling af et forlig mellem en efterretningstjeneste og en tidligere medarbejder, der forfølger et krav om ansættelse, som et eksempel på anvendelsen af begrænsninger i Schedule 11 (jf. fodnote 161) Det bør også bemærkes, at de samme begrænsninger er tilgængelige for andre offentlige myndigheder i henhold til Schedule 2 til Part 2 i DPA 2018.

([180]) Ifølge UK Explanatory Framework er undtagelser, der er »klassebaserede«: i) oplysninger om tildeling af »Crown honours and dignities« (Kronens hædersbevisninger o.lign.), ii) beskyttelse af fortroligheden i korrespondancen mellem advokater og klienter, iii) fortrolige referencer vedrørende beskæftigelse, uddannelse eller erhvervsuddannelse samt iv) prøvebesvarelser og -karakterer. De »skadebaserede« undtagelser vedrører i) forebyggelse eller afsløring af kriminalitet og pågribelse og retsforfølgning af lovovertrædere, ii) parlamentarisk privilegium, iii) retssager, iv) de nationale væbnede styrkers kampeffektivitet, v) Det Forenede Kongeriges økonomiske velfærd, vi) forhandlinger med den registrerede, vii) videnskabelig eller historisk forskning eller statistiske formål samt viii) arkivering i almenhedens interesse. UK Explanatory Framework for Adequacy Discussions, section H: National Security, s. 13, jf. fodnote 31.

pågældende databeskyttelsesbestemmelse sandsynligvis vil skade den pågældende specifikke interesse. Anvendelsen af en undtagelse skal derfor altid begrundes med henvisning til den relevante skade, der sandsynligvis vil forekomme i det enkelte tilfælde. En klassebaseret undtagelse kan kun påberåbes i forbindelse med den specifikke, snævert definerede kategori af oplysninger, for hvilken undtagelsen indrømmes. Med hensyn til formål og virkning svarer disse til flere af undtagelserne fra UK GDPR (i henhold til Schedule 2 til DPA 2018), som igen afspejler undtagelserne i artikel 23 i GDPR.

(133) Det følger af ovenstående, at der er indført begrænsninger og betingelser i henhold til de gældende britiske lovbestemmelser, som også fortolket af domstolene og Information Commission, for at sikre, at disse undtagelser og restriktioner holdes inden for grænserne af, hvad der er nødvendigt og rimeligt for at beskytte statens sikkerhed.

3.2 **Det Forenede Kongeriges myndigheders adgang til og brug af personoplysninger med henblik på retshåndhævelse på det strafferetlige område**

(134) Det Forenede Kongeriges lovgivning pålægger en række begrænsninger af adgangen til og brugen af personoplysninger til retshåndhævelsesformål på det strafferetlige område og indeholder en række kontrol- og klagemekanismer på dette område, som er i overensstemmelse med de krav, der er omhandlet i betragtning 113 til 115 i denne afgørelse. De betingelser, hvorunder en sådan adgang kan finde sted, og de garantier, der gælder for udøvelsen af disse beføjelser, vurderes nærmere i de følgende afsnit.

3.2.1. *Retsgrundlag og gældende begrænsninger/garantier*

(135) I henhold til det princip om lovlighed, der er sikret ved Section 35 i DPA 2018, er behandling af personoplysninger til et hvilket som helst retshåndhævelsesformål kun lovlig, hvis den er baseret på loven, og enten den registrerede har givet samtykke til behandlingen med henblik på dette formål ([181]), eller behandlingen er nødvendig for, at en kompetent myndighed kan udføre en opgave med henblik på formålet.

3.2.1.1 Ransagningskendelser og editionskendelser

(136) Det Forenede Kongeriges retlige ramme tillader indsamling af personoplysninger fra erhvervsdrivende med henblik på strafferetlig håndhævelse på grundlag af ransagningskendelser ([182]) og editionskendelser ([183]). Dette gælder også erhvervsdrivende, der behandler oplysninger, som overføres fra EU i henhold til denne afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

(137) Ransagningskendelser udstedes af en domstol, normalt efter anmodning fra efterforskeren. De gør det muligt for efterforskeren at få adgang til lokaler for at søge efter materiale eller personer, der er relevante for deres efterforskning, og tilbageholde alt, hvad der er tilladt at søge efter, herunder alle relevante dokumenter og materiale, der indeholder personoplysninger ([184]). En editionskendelse, som også skal udstedes af en domstol, pålægger den person, der er anført i den, at fremlægge eller give adgang til materiale, som vedkommende er i besiddelse af eller har kontrol over. Vedkommende, som ansøger om en ransagningskendelse eller editionskendelse, skal over for retten begrunde, hvorfor den er nødvendig, og hvorfor brugen

([181]) Anvendelsen af samtykke forekommer ikke relevant i et scenarie vedrørende tilstrækkelighed, da oplysningerne i en overførselssituation ikke vil være blevet indsamlet direkte fra en registreret i EU af en retshåndhævende myndighed i Det Forenede Kongerige på grundlag af samtykke.

([182]) Med hensyn til det relevante retsgrundlag henvises til Section 8 ff. i PACE 1984 (Police and Criminal Evidence Act — lov om politimyndigheden og bevismateriale i strafferetlige sager) (for England og Wales) og Section 10 ff. i Police and Criminal Evidence Order (Northern Ireland) 1989 (strafferetsplejeloven for Nordirland). For så vidt angår Skotland er retsgrundlaget dannet i henhold til sædvaneretten (se Section 46 i Criminal Justice (Scotland) Act 2016 (strafferetsplejeloven for Skotland)) og Section 23B i Criminal Law (Consolidation) (Scotland) (den konsoliderede straffelov for Skotland). For ransagningskendelser udstedt efter anholdelsen er retsgrundlaget Section 18 i PACE 1984 (for England og Wales) og Section 20 ff. i Police and Criminal Evidence Order (Northern Ireland) 1989. For så vidt angår Skotland er retsgrundlaget dannet i henhold til sædvaneretten (se Section 46 i Criminal Justice (Scotland) Act 2016). De britiske myndigheder har præciseret, at ransagningskendelser udstedes af en domstol efter anmodning fra efterforskeren. Disse kendelser gør det muligt for efterforskeren at få adgang til lokaler for at søge efter materiale eller enkeltpersoner, der er relevante for deres undersøgelser. Fuldbyrdelsen af kendelserne vil ofte kræve politiets bistand.

([183]) Når efterforskningen vedrører hvidvaskning af penge (herunder konfiskation og civile inddrivelsesprocedurer), er det relevante retsgrundlag for anvendelse af en editionskendelse Section 345 ff. for England, Wales og Nordirland og Section 380 ff. i Proceeds of Crime Act 2002 (lov om udbytte fra strafbare forhold) for Skotland. Hvis efterforskningen vedrører andre spørgsmål end hvidvaskning af penge, kan der indgives en anmodning om en editionskendelse i henhold til Section 9 i og Schedule 1 til PACE 1984 for England og Wales og Section 10 ff. i Police and Criminal Evidence Order (Northern Ireland) 1989 for Nordirland. For så vidt angår Skotland er retsgrundlaget dannet i henhold til sædvaneretten (se Section 46 i Criminal Justice (Scotland) Act 2016) og Section 23B i Criminal Law (Consolidation) (Scotland). De britiske myndigheder har præciseret, at en editionskendelse pålægger den person, der er anført i den, at fremlægge eller give adgang til det materiale, som vedkommende er i besiddelse af eller har kontrol over (se paragraph 4 i Schedule 1 til PACE 1984).

([184]) I Section 8 og 18 indeholder PACE 1984 f.eks. beføjelser til at beslaglægge og tilbageholde alt, hvad ransagningen er godkendt til.

af den er i almenhedens interesse. Der er flere lovfæstede beføjelser, der gør det muligt at udstede ransagningskendelser og editionskendelser. Hver bestemmelse har sine egne lovbestemte betingelser, som skal være opfyldt, for at der kan udstedes en ransagningskendelse ([185]) eller en editionskendelse ([186]).

(138) Editionskendelser og ransagningskendelser kan anfægtes ved domstolsprøvelse ([187]). Af beskyttelseshensyn må strafferetshåndhævende myndigheder i henhold til Part 3 i DPA 2018 kun få adgang til personoplysninger — hvilket er en form for behandling — i overensstemmelse med principperne og kravene i DPA 2018 (se betragtning 122 og 124 ovenfor). En anmodning fra en retshåndhævende

([185]) Eksempelvis indeholder Section 8 og18 i PACE bestemmelser om henholdsvis fredsdommeres beføjelse til at udstede en kendelse og politibetjentes beføjelse til at ransage en ejendom. I det første tilfælde (Section 8) skal en fredsdommer, inden vedkommende udsteder en kendelse, først sikre sig, at der er rimelig grund til at antage, at i) der er begået en strafbar handling, ii) der er materiale på stedet, som sandsynligvis vil være af væsentlig værdi (enten i sig selv eller sammen med andet materiale) i forbindelse med efterforskningen af handlingen, iii) materialet kan forventes at være relevant bevismateriale, iv) i materialet indgår der ikke elementer, der er omfattet af en ret til fortrolighed, udelukket materiale eller materiale, for hvilket der gælder en særlig procedure, og v) det ikke ville være muligt at få adgang uden brug af en kendelse. I det andet tilfælde giver Section 18 en politibetjent mulighed for at ransage en ejendom, der bebos af en person, som er anholdt for en strafbar handling, for at finde andet materiale end materiale, der er omfattet af retten til fortrolighed, hvis vedkommende har rimelig grund til at antage, at der i ejendommen er bevismateriale, der vedrører den pågældende lovovertrædelse eller en anden lignende eller forbundet strafbar handling. En sådan ransagning skal begrænses til at afdække dette materiale og være godkendt på skrift af en politibetjent, der som minimum har rang af inspektør, medmindre ransagningen er nødvendig for efterforskningen af den strafbare handling. I så fald skal en inspektør eller en politibetjent med højere rang underrettes så hurtigt som praktisk muligt, efter at ransagningen er foretaget. Begrundelsen for ransagningen og arten af det bevismateriale, der søges efter, skal registreres. Desuden indeholder Section 15 og 16 i PACE 1984 en række lovfæstede garantier, som skal følges, når der anmodes om en ransagningskendelse. I Section 15 præciseres de krav, der gælder for at indhente en ransagningskendelse (herunder indholdet af den begæring, som betjenten skal indgive, og det forhold, at kendelsen bl.a. skal angive den lovbestemmelse, i henhold til hvilken den er udstedt, og så vidt muligt identificere de genstande og personer, der skal eftersøges, og de lokaler, der skal ransages). I Section 16 er det bestemt, hvordan en ransagning i henhold til en kendelse skal foretages. (Eksempelvis er det i Section 16(5) fastlagt, at den betjent, der fuldbyrder kendelsen, skal give beboeren en kopi af den. I henhold til Section 16(11) skal kendelsen, når den er fuldbyrdet, opbevares i en periode på 12 måneder. Section 16(12) giver beboeren ret til at få indsigt i kendelsen i denne periode, hvis vedkommende ønsker det). Disse bestemmelser bidrager til at sikre overholdelse af artikel 8 i EMRK (se f.eks. Kent Pharmaceuticals mod Director of the Serious Fraud Office [2002] EWHC 3023 (QB), paragraph [30], af Lord Woolf CJ). Manglende overholdelse af disse garantier kan føre til, at ransagningen erklæres ulovlig (f.eks. R (Brook) mod Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95, R (Superior Import / Export Ltd) mod Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115 og R (F) mod Blackfriars Crown Court [2014] EWHC 1541 (Admin)). Section 15 og 16 i PACE 1984 suppleres af Code B of PACE, som er en adfærdskodeks, der regulerer udøvelsen af politimæssige beføjelser til at ransage ejendomme.

([186]) Eksempelvis bør der, når der udstedes en editionskendelse i henhold til Proceeds of Crime Act 2002 (lov om udbytte fra strafbare handlinger), ud over behovet for at have en rimelig grund til at opfylde betingelserne i Section 346(2) i Proceeds of Crime Act, være en rimelig grund til, at personen er i besiddelse af eller kontrollerer det specificerede materiale, og at materialet sandsynligvis har en væsentlig værdi. En anden forudsætning for at udstede en editionskendelse er, at der skal være en rimelig grund til at antage, at det er i offentlighedens interesse, at materialet fremlægges, eller adgangen til det gives, i betragtning af a) den fordel, der kan forventes opnået ved efterforskningen, hvis materialet fremlægges, og b) de omstændigheder, hvorunder den person, der i ansøgningen angives at være i besiddelse af eller kontrollere det materiale, som indeholder oplysninger om vedkommende. På samme måde skal en ret, der behandler en anmodning om en editionskendelse i henhold til Schedule 1 til PACE 1984, finde det godtgjort, at visse betingelser er opfyldt. Navnlig indeholder Schedule 1 til PACE to forskellige alternative sæt af betingelser, hvoraf det ene skal være opfyldt, før en dommer kan udstede en editionskendelse. Det første sæt kræver, at dommeren har en rimelig grund til at antage i), at der er begået en strafbar handling, ii) at det materiale, der eftersøges på stedet, består af eller omfatter materiale, for hvilket der gælder særlige procedurer, men ikke udelukket materiale, iii) at materialet enten i sig selv eller sammen med andet materiale sandsynligvis har væsentlig betydning for efterforskningen, iv) at det sandsynligvis vil være relevant bevismateriale, v) at andre metoder til fremskaffelse af materialet enten er forsøgt eller ikke er forsøgt, fordi de sandsynligvis ikke ville give det ønskede resultat, og vi) at det er i offentlighedens interesse, at materialet frembringes, eller at der gives adgang til det, på baggrund af en vurdering af fordelene ved efterforskningen og de omstændigheder, hvorunder den pågældende person er i besiddelse af materialet. Det andet sæt af betingelser kræver i), at der på stedet forefindes materiale, der er underlagt en særlig procedure eller består af udelukket materiale, ii), at der kunne være udstedt en ransagningskendelse for materialet, hvis der ikke var tale om et forbud mod ransagning foretaget på grundlag af en lovgivning, der er vedtaget før PACE, vedrørende materiale underlagt en særlig procedure, udelukket materiale eller fortroligt materiale, og iii), at det ville have været hensigtsmæssigt at gøre dette.

([187]) Domstolsprøvelse er den retlige procedure, hvorved afgørelser truffet af et offentligt organ kan anfægtes ved High Court. Domstolene »prøver« den afgørelse, der anfægtes, og afgør under hensyntagen til offentligretlige begreber/principper, om det kan hævdes, at afgørelsen er behæftet med retlige fejl. De væsentligste grunde til domstolsprøvelse er ulovlighed, manglende rationalitet, proceduremæssig utilbørlighed, berettigede forventninger og menneskerettigheder. Efter en vellykket domstolsprøvelse kan en domstol træffe afgørelse om en række forskellige retsmidler. Det mest almindelige er en annullationsordre (som annullerer den oprindelige afgørelse — dvs. afgørelsen om at udstede en ransagningskendelse), og dette kan i nogle tilfælde også omfatte tilkendelse af økonomisk kompensation. Yderligere oplysninger om domstolsprøvelse i Det Forenede Kongerige findes i myndighedernes juridiske afdelings publikation »Judge Over Your Shoulder — a guide to good decision-making«, som kan findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

myndighed bør derfor være i overensstemmelse med princippet om, at formålet med behandlingen skal angives og være udtrykkeligt og legitimt ([188]), og at de personoplysninger, der behandles af en kompetent myndighed, skal være relevante for dette formål og ikke være uforholdsmæssige ([189]).

3.2.1.2. Efterforskningsbeføjelser med henblik på retshåndhævelse

(139) Med henblik på at forebygge eller afsløre alvorlig kriminalitet ([190]) kan visse retshåndhævende myndigheder, herunder National Crime Agency (det nationale kontor for kriminalitet) og Chief of Police ([191]) (politichefen), anvende målrettede efterforskningsbeføjelser i henhold til IPA 2016. I dette tilfælde vil de garantier, der er fastsat i IPA 2016, finde anvendelse ud over dem, der er fastsat i Part 3 i DPA 2018. De specifikke efterforskningsbeføjelser, som disse retshåndhævende myndigheder kan påberåbe sig, er: målrettet aflytning (Part 2 i IPA 2016), indsamling af kommunikationsdata (Part 3 i IPA 2016), opbevaring af kommunikationsdata (Part 4 i IPA 2016) og målrettet indgreb i udstyr (Part 5 i IPA 2016). Aflytning omfatter erhvervelse af indholdet af en kommunikation ([192]), mens indsamling og opbevaring af kommunikationsdata ikke har til formål at erhverve indholdet af kommunikationen, men at registrere »hvem«, »hvornår«, »hvor« og »hvordan« i forbindelse med kommunikationen. Dette omfatter f.eks. tidspunktet for kommunikationen og dens varighed, afsenderens og modtagerens telefonnummer eller e-mailadresse og nogle gange placeringen af det udstyr, hvorfra kommunikationen blev foretaget, abonnenten på en telefontjeneste eller en specificeret regning ([193]). Indgreb i udstyr omfatter en række teknikker, der anvendes til at indhente diverse data fra udstyr, herunder computere, tablets og smartphones samt kabler og lagringsenheder ([194]).

(140) Beføjelser til at foretage målrettet aflytning kan også anvendes, når »det er nødvendigt for at gennemføre bestemmelserne i et EU-instrument for gensidig bistand eller en international aftale om gensidig bistand« (en såkaldt »kendelse om gensidig bistand« ([195])). Kendelser om gensidig bistand gives kun i forbindelse med aflytning, ikke indsamling af kommunikationsdata eller indgreb i udstyr. Disse målrettede beføjelser er reguleret i Investigatory Powers Act 2016 (IPA 2016) ([196]), som sammen med Regulation of Investigatory Powers Act 2000 (RIPA) for England, Wales og Nordirland og Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) for Skotland fastlægger retsgrundlaget og fastsætter de gældende begrænsninger og garantier for anvendelsen af sådanne beføjelser. IPA 2016 indeholder også bestemmelser om anvendelse af beføjelser til efterforskning af massedata, selv om disse ikke er til rådighed for de retshåndhævende myndigheder (kun efterretningstjenester kan gøre brug af dem) ([197]).

([188]) Section 36(1) i DPA 2018.

([189]) Section 37 i DPA 2018.

([190]) Section 263(1) i IPA 2016 fastsætter, at der ved »alvorlig kriminalitet« forstås en lovovertrædelse, for hvilken en voksen, som ikke tidligere har været dømt, med rimelighed kan forventes at blive idømt en fængselsstraf på tre år eller derover, eller handlingen indebærer brug af vold, medfører betydelig økonomisk gevinst eller foretages af et stort antal personer. Med henblik på indsamling af kommunikationsdata i henhold til Part 4 i IPA 2016 fastsættes det desuden i Section 87(10B), at der ved »alvorlig kriminalitet« forstås en forbrydelse, for hvilken der kan idømmes en fængselsstraf på 12 måneder eller derover, eller en lovovertrædelse begået af en person, der ikke er en fysisk person, eller som en integrerende del heraf indebærer afsendelse af kommunikation eller krænkelse af en persons privatliv.

([191]) Navnlig følgende retshåndhævende myndigheder kan ansøge om en kendelse om målrettet aflytning: Director General of the National Crime Agency (generaldirektøren for det nationale kriminalitetsagentur), Commissioner of Police of the Metropolis (politikommissæren i hovedstadsområdet), Chief Constable of the Police Service of Northern Ireland (rigspolitichefen for Nordirland), Chief Constable of the Police Service of Scotland (rigspolitichefen for Skotland), Commissioner for Her Majesty's Revenue and Customs (chefen for told- og skatteväsenet), Chief of Defence Intelligence (chefen for forsvarets efterretningstjeneste) samt personer, der er kompetente myndigheder i lande eller territorier uden for Det Forenede Kongerige for så vidt angår et EU-instrument om gensidig bistand eller en international aftale om gensidig bistand (Section 18(1) i IPA 2016).

([192]) Se Section 4 i IPA 2016.

([193]) Se Section 261, stk. 5, i IPA 2016 og Code of Practice on Bulk Acquisition of Communications Data (adfærdskodeksen for masseindsamling af kommunikationsdata), som kan findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, paragraph 2.9.

([194]) Code of Practice on Equipment Interference (adfærdskodeks for indgreb i udstyr), som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, paragraph 2.2.

([195]) En kendelse om gensidig bistand bemyndiger en myndighed i Det Forenede Kongerige til at yde bistand til en myndighed uden for Det Forenede Kongeriges område med henblik på aflytning og videregivelse af det aflyttede materiale til denne myndighed i overensstemmelse med et internationalt instrument for gensidig bistand (Section 15(4) i IPA 2016).

([196]) Investigatory Powers Act 2016 (se: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) erstattede anden lovgivning om aflytning af kommunikation, indgreb i udstyr og indsamling af kommunikationsdata, navnlig Part I i RIPA 2000, som tidligere udgjorde den generelle lovgivningsmæssige ramme for retshåndhævende og nationale sikkerhedsmyndigheders anvendelse af efterforskningsbeføjelser.

([197]) Section 138(1), 158(1), 178(1) og 199(1) i IPA 2016.

(141) For at kunne udøve disse beføjelser skal myndighederne indhente en kendelse ([198]), der er afsagt af en kompetent myndighed ([199]) og godkendt af en uafhængig Judicial Commissioner ([200]) (den såkaldte »double-lock«-procedure). For at indhente en sådan kendelse skal der foretages en nødvendigheds- og proportionalitetstest ([201]). Eftersom disse målrettede efterforskningsbeføjelser, der er fastsat i IPA 2016, er de samme som dem, der er til rådighed for nationale sikkerhedsagenturer, behandles de betingelser, begrænsninger og garantier, der gælder for sådanne beføjelser, nærmere i afsnittet om Det Forenede Kongeriges offentlige myndigheders adgang til og brug af personoplysninger til nationale sikkerhedsformål (se betragtning 177 ff.).

3.2.2. *Yderligere anvendelse af de indsamlede oplysninger*

(142) En retshåndhævende myndigheds deling af oplysninger med en anden myndighed til andre formål end dem, hvortil de oprindeligt blev indsamlet (såkaldt »videredeling«), er underlagt visse betingelser.

(143) I lighed med hvad der er fastsat i artikel 4, stk. 2, i direktiv (EU) 2016/680, giver Section 36, stk. 3, i DPA 2018 mulighed for, at personoplysninger, der indsamles af en kompetent myndighed med henblik på retshåndhævelse, efterfølgende kan behandles (enten af den oprindelige dataansvarlige eller af en anden dataansvarlig) med henblik på ethvert andet retshåndhævelsesformål, forudsat at den dataansvarlige ved lov er bemyndiget til at behandle oplysninger til det andet formål, og at behandlingen er nødvendig og står i et rimeligt forhold til dette formål ([202]). I dette tilfælde finder alle de garantier, der er fastsat i Part 3 i DPA 2018, og som er omhandlet i betragtning 122 og 124 anvendelse på den behandling, der foretages af den modtagende myndighed.

(144) I Det Forenede Kongeriges retsorden tillader forskellige love udtrykkeligt en sådan videredeling. Navnlig giver Digital Economy Act 2017 (lov om den digitale økonomi) mulighed for deling mellem offentlige myndigheder til flere formål, f.eks. i tilfælde af svig mod den offentlige sektor, som ville medføre tab eller risiko for tab for offentlige myndigheder ([203]), eller i tilfælde af gæld til en offentlig myndighed eller Kronen ([204]). ii) Desuden tillader Crime and Courts Act 2013 (lov om kriminalitet og domstole) udveksling af oplysninger med National Crime Agency ([205]) med henblik på at bekæmpe, efterforske og retsforfølge grov og organiseret kriminalitet. iii) Endelig giver Serious Crime Act 2007 (lov om grov kriminalitet) offentlige myndigheder mulighed for at videregive oplysninger til organisationer, der bekæmper svig, med henblik på at forebygge svig ([206]).

(145) Disse love fastsætter udtrykkeligt, at udvekslingen af oplysninger skal være i overensstemmelse med principperne i DPA 2018. Desuden har politiakademiet udarbejdet en vejledning i informationsudveksling ([207]) for at hjælpe politiet med at opfylde deres databeskyttelsesforpligtelser i henhold til UK GDPR, DPA og Human Rights Act 1998.

([198]) Chapter 2 i Part 2 i IPA 2016 omhandler et begrænset antal tilfælde, hvor aflytning kan foretages uden retskendelse. Der er bl.a. tale om aflytning med afsenderens eller modtagerens samtykke, aflytning til administrative eller håndhævelsesmæssige formål, aflytning i visse institutioner (fængsler, psykiatriske hospitaler og tilbageholdelsesfaciliteter i forbindelse med immigration) samt aflytning i overensstemmelse med en relevant international aftale.

([199]) I de fleste tilfælde er Secretary of State den myndighed, der udsteder kendelser i henhold til IPA 2016, mens de skotske ministre har beføjelse til at udstede kendelser om målrettet aflytning og anmodninger om gensidig bistand og foretage målrettet indgreb i udstyr, når de personer eller lokaler, der skal aflyttes, og det udstyr, der skal foretages indgreb i, befinder sig i Skotland (se Section 22 og 103 i IPA 2016). I tilfælde af målrettet indgreb i udstyr kan en leder af en retshåndhævende myndighed (beskrevet i Part 1 og 2 i Schedule 6 til IPA 2016) udstede kendelsen i henhold til betingelserne i Section 106 i IPA 2016.

([200]) Judicial Commissioners (særlige juridiske rådgivere) bistår Investigatory Powers Commissioner (kommissær for efterforskningsbeføjelser, IPC), som er et uafhængigt organ, der udøver tilsynsfunktioner i forbindelse med efterretningstjenesternes brug af efterforskningsbeføjelser (nærmere oplysninger findes i betragtning 162 ff.).

([201]) Se navnlig Section 19 og 23 i IPA 2016.

([202]) Section 36(3) i DPA 2018.

([203]) Section 56 i Digital Economy Act 2017, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2017/30/section/56.

([204]) Section 48 i Digital Economy Act 2017.

([205]) Section 7 i Crime and Courts Act 2013, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2013/22/section/7.

([206]) Section 68 i Serious Crime Act 2007, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([207]) Authorised Professional Practice on Information Sharing, som kan findes på følgende link: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

Udvekslingens overensstemmelse med de gældende retlige rammer for databeskyttelse er naturligvis underlagt domstolskontrol ([208]).

(146) I lighed med, hvad der er fastsat i artikel 9 i direktiv (EU) 2016/680, fastsætter DPA 2018 desuden, at personoplysninger, der indsamles med henblik på retshåndhævelse, kan behandles med henblik på et formål, der ikke er retshåndhævelse, når behandlingen er tilladt ved lov ([209]).

(147) Denne slags deling omfatter to scenarier, nemlig 1) ét, hvor en retshåndhævende myndighed på det strafferetlige område deler oplysninger med en anden retshåndhævende myndighed end en efterretningsmyndighed (f.eks. en finans- eller skattemyndighed eller en myndighed på området for konkurrence, ungdomsforsorg osv.), og 2) ét, hvor en retshåndhævende myndighed på det strafferetlige område deler data med en efterretningstjeneste. I det første scenarie vil behandlingen af personoplysninger falde ind under anvendelsesområdet for UK GDPR og Part 2 i DPA 2018. Kommissionen har i betragtning 12 til 111 vurderet de garantier, der er fastsat i UK GDPR og Part 2 i DPA 2018, og er nået til den konklusion, at Det Forenede Kongerige sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres inden for anvendelsesområdet for forordning (EU) 2016/679 fra Den Europæiske Union til Det Forenede Kongerige.

(148) I det andet scenarie vedrørende udveksling af oplysninger indsamlet af en retshåndhævende myndighed på det strafferetlige område med en efterretningstjeneste til formål, der vedrører statens sikkerhed, er retsgrundlaget for en sådan udveksling Section 19 i Counter Terrorism Act 2008 (lov om terrorbekæmpelse) ([210]). I henhold til denne lov kan enhver person videregive oplysninger til en hvilken som helst efterretningstjeneste med henblik på varetagelse af en hvilken som helst af denne tjenestes funktioner, herunder »statens sikkerhed«.

(149) Med hensyn til betingelserne for udveksling af oplysninger af hensyn til statens sikkerhed begrænser Intelligence Services Act ([211]) og Security Service Act ([212]) efterretningstjenesternes mulighed for at indhente data til, hvad der er nødvendigt for at udføre deres lovbestemte funktioner. De retshåndhævende myndigheder, der ønsker at udveksle oplysninger med efterretningstjenesterne, vil skulle tage hensyn til en række faktorer/begrænsninger ud over de lovbestemte funktioner, der er fastsat i Intelligence Services Act og Security Service Act ([213]). Section 20 i Counter Terrorism Act 2008 præciserer, at enhver dataudveksling i henhold til Section 19 stadig skal være i overensstemmelse med databeskyttelseslovgivningen, hvilket indebærer, at alle begrænsninger og krav i Part 3 i DPA 2018 finder anvendelse. Da de kompetente myndigheder desuden er offentlige myndigheder i henhold til Human Rights Act 1998, skal de sikre, at de handler i overensstemmelse med rettighederne i konventionerne, herunder EMRK's artikel 8. Disse begrænsninger sikrer, at al dataudveksling mellem de retshåndhævende myndigheder og efterretningstjenesterne er i overensstemmelse med databeskyttelseslovgivningen og EMRK.

([208]) Se f.eks. sagen M, R mod Chief Constable of Sussex Police [2019] EWHC 975 (Admin), hvor High Court blev anmodet om at træffe afgørelse om dataudveksling mellem politiet og Business Crime Reduction Partnership (BCRP), som er en organisation, der er bemyndiget til at forvalte ordninger om forbud mod bestemte personers adgang til medlemmernes forretningslokaler. Retten gennemgik dataudvekslingen, som fandt sted på grundlag af en aftale, der havde til formål at beskytte offentligheden og forebygge kriminalitet, og konkluderede i sidste ende, at de fleste aspekter af dataudvekslingen var lovlige, undtagen i forbindelse med visse følsomme oplysninger, der blev udvekslet mellem politiet og BCRP. Et andet eksempel er sagen Cooper mod NCA [2019] EWCA Civ 16, hvor appeldomstolen stadfæstede dataudvekslingen mellem politiet og Serious Organised Crime Agency (agenturet for bekæmpelse af grov organiseret kriminalitet), som er en retshåndhævende myndighed, der i øjeblikket er en del af National Crime Agency.

([209]) Section 36(4) i DPA 2018.

([210]) Counter Terrorism Act 2008, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([211]) Intelligence Service Act 1994, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) Security Service Act 1989, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) Section 2(2) i Intelligence Services Act 1994 bestemmer, at »chefen for efterretningstjenesten er ansvarlig for denne tjenestes effektivitet, og det påhviler vedkommende at sikre, a) at der er truffet foranstaltninger til at sikre, at efterretningstjenesten ikke indhenter oplysninger, medmindre det er nødvendigt for, at efterretningstjenesten kan udføre sine opgaver korrekt, og at den ikke videregiver oplysninger, undtagen i det omfang det er nødvendigt i) til dette formål, ii) af hensyn til statens sikkerhed, iii) med henblik på forebyggelse eller afsløring af grov kriminalitet eller iv) med henblik på en straffesag, og b) at efterretningstjenesten ikke træffer foranstaltninger med henblik på at fremme et britisk politisk partis interesser«, mens Section 2(2) i Security Services Act 1989 fastsætter, at »generaldirektøren er ansvarlig for tjenestens effektivitet, og at det er hans pligt at sikre, a) at der er truffet foranstaltninger til at sikre, at tjenesten ikke indhenter oplysninger, undtagen i det omfang det er nødvendigt for, at den kan udføre sine opgaver korrekt, eller videregiver sådanne oplysninger, medmindre det er nødvendigt af hensyn til dette formål eller med henblik på at forebygge eller afsløre [grov kriminalitet eller med henblik på en straffesag], b) at tjenesten ikke foretager sig noget for at fremme et politisk partis interesser, samt c) at der er indgået aftale med generaldirektøren for National Crime Agency om koordinering af tjenestens aktiviteter i medfør af denne lovs Section 1(4) med politistyrkernes, National Crime Agency's og andre retshåndhævende myndigheders aktiviteter«.

(150) Når en kompetent myndighed har til hensigt at dele personoplysninger, der behandles i henhold til Part 3 i DPA 2018, med retshåndhævende myndigheder i et tredjeland, gælder der særlige krav ([214]). Sådanne delinger kan navnlig finde sted, når de er baseret på bestemmelser om et tilstrækkeligt beskyttelsesniveau, der er udstedt af Secretary of State. Hvis der ikke findes sådanne bestemmelser, skal der sikres passende garantier. Section 75 i DPA 2018 fastsætter, at de fornødne garantier er indført, når de er fastsat i en retsakt, der er bindende for den tiltænkte modtager, eller hvis den dataansvarlige efter at have vurderet alle omstændighederne i forbindelse med videregivelsen af denne type personoplysninger til tredjelandet eller den internationale organisation konkluderer, at de fornødne garantier for beskyttelse af oplysningerne findes.

(151) Hvis en overførsel ikke er baseret på en bestemmelse om tilstrækkeligheden af beskyttelsesniveauet eller de fornødne garantier, kan den kun finde sted under visse nærmere angivne »særlige omstændigheder« ([215]). Dette er tilfældet, når overførslen er nødvendig a) for at beskytte den registreredes eller en anden persons vitale interesser, b) for at beskytte den registreredes legitime interesser, c) for at afværge en umiddelbar og alvorlig trussel mod en medlemsstats eller et tredjelands offentlige sikkerhed, d) for at opnå et af retshåndhævelsesformålene i individuelle sager eller e) for at opnå et retligt formål i individuelle sager (f.eks. i forbindelse med retssager eller for at indhente juridisk rådgivning). Det skal bemærkes, at litra d) og e) ikke finder anvendelse, hvis den registreredes rettigheder og frihedsrettigheder går forud for samfundets interesse i overførslen. Disse omstændigheder svarer til de særlige situationer og betingelser, der kan betegnes som »undtagelser« i henhold til artikel 38 i direktiv (EU) 2016/680.

(152) Når materiale, som de retshåndhævende myndigheder har erhvervet i henhold til en kendelse, der giver tilladelse til brug af aflytning eller indgreb i udstyr, overdrages til et tredjeland, pålægger IPA 2016 desuden yderligere sikkerhedsforanstaltninger. Navnlig er en sådan videregivelse, der defineres som »udenlandsk videregivelse«, kun tilladt, hvis udstedelsesmyndigheden finder, at der findes særlige passende ordninger, som begrænser antallet af personer, som oplysningerne videregives til, i hvilket omfang materiale videregives eller stilles til rådighed, samt i hvilket omfang materialet kopieres og antallet af kopier. Desuden kan den udstedende myndighed kræve, at der iværksættes passende foranstaltninger for at sikre, at alle kopier, der laves af en hvilken som helst del af materialet, skal destrueres, så snart der ikke længere er nogen relevante grunde til at opbevare det (hvis det ikke er destrueret tidligere) ([216]).

(153) Endelig vil specifikke former for videreoverførsel fra Det Forenede Kongerige til USA i fremtiden kunne finde sted på grundlag af »Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime« (aftale mellem regeringen for Det Forenede Kongerige Storbritannien og Nordirland og Amerikas Forenede Staters regering om adgang til elektroniske data med henblik på bekæmpelse af grov kriminalitet (»aftalen mellem Det Forenede Kongerige og USA« eller »aftalen«) ([217]), der blev indgået i oktober 2019 ([218]). Selv om aftalen endnu ikke er trådt i kraft på tidspunktet for vedtagelsen af denne afgørelse, kan dens forventede ikrafttræden påvirke videreoverførsler til USA af oplysninger, der først overføres til Det Forenede Kongerige på grundlag af afgørelsen. Mere specifikt kan oplysninger, der overføres fra EU til tjenesteudbydere i Det Forenede Kongerige, være genstand for kendelser om fremlæggelse af elektronisk bevismateriale udstedt af kompetente amerikanske retshåndhævende myndigheder og gjort anvendelige i Det Forenede Kongerige i henhold til denne aftale, når den er trådt i kraft. Af disse grunde er vurderingen af de betingelser og garantier, hvorunder sådanne kendelser kan udstedes og fuldbyrdes, relevant for denne afgørelse.

([214]) Se Chapter 5 i Part 3 i DPA 2018.

([215]) Section 76 i DPA 2018.

([216]) Section 54 og Section 130 i IPA 2016. De udstedende myndigheder skal overveje behovet for at indføre særlige sikkerhedsforanstaltninger for det materiale, der overdrages til udenlandske myndigheder, for at sikre, at oplysningerne er omfattet af garantier med hensyn til opbevaring, tilintetgørelse og videregivelse af oplysninger svarende til dem, der er fastsat i Section 53 og Section 129 i IPA 2016.

([217]) Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, som kan findes på følgende 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]) Dette er den første aftale, som blev indgået inden for rammerne af US Clarifying Lawful Overseas Use of Data (CLOUD) Act. Denne lov er en amerikansk forbundslov, der blev vedtaget den 23. marts 2018, og som via en ændring af Stored Communications Act fra 1986 præciserer, at amerikanske tjenesteudbydere er forpligtet til at efterkomme amerikanske kendelser om at videregive indhold og andre data end indhold (non-content data), uanset hvor sådanne data er opbevaret. CLOUD-loven giver også mulighed for at indgå administrative aftaler med udenlandske regeringer, på grundlag af hvilke amerikanske tjenesteudbydere vil kunne levere indholdsdata direkte til disse udenlandske regeringer (CLOUD-loven findes på følgende link: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf) .

(154) I denne forbindelse skal det for det første bemærkes, at aftalen for så vidt angår dens materielle anvendelsesområde kun finder anvendelse på forbrydelser, der kan straffes med fængsel med en strafferamme på mindst tre år (defineret som »grov kriminalitet«) ([219]), herunder »terrorvirksomhed«. For det andet må oplysninger, der behandles i den anden jurisdiktion, kun indhentes i henhold til denne aftale på baggrund af en »kendelse [...], der i henhold til udstedelsespartens nationale lovgivning er underlagt kontrol eller tilsyn af en domstol, dommer eller anden uafhængig myndighed forud for eller under procedurer vedrørende fuldbyrdelse af kendelsen« ([220]). For det tredje skal enhver kendelse »bygge på krav om en rimelig begrundelse baseret på håndgribelige og troværdige kendsgerninger, specificitet, lovlighed og grovhed vedrørende den adfærd, der undersøges« ([221]), og »være rettet mod specifikke konti samt identificere en bestemt person, konto, adresse eller form for personligt udstyr eller en anden specifik identifikator« ([222]). For det fjerde nyder data, der er indhentet i henhold til denne aftale, samme beskyttelse som de specifikke garantier i den såkaldte »paraplyaftale mellem EU og USA« ([223]) — en omfattende databeskyttelsesaftale, der blev indgået af EU og USA i december 2016, og som fastsætter de garantier og rettigheder, der gælder for dataoverførsler inden for retshåndhævelsessamarbejde — som alle er indarbejdet i denne aftale ved henvisning med de fornødne ændringer for navnlig at tage hensyn til overførslernes særlige karakter (dvs. overførsler fra private operatører til retshåndhævende myndigheder snarere end overførsler mellem retshåndhævende myndigheder) ([224]). Aftalen mellem Det Forenede Kongerige og USA fastsætter specifikt, at en tilsvarende beskyttelse som den, der er fastsat i paraplyaftalen mellem EU og USA, vil blive anvendt »på alle personoplysninger, der fremkommer i forbindelse med gennemførelsen af kendelser, der er omfattet af aftalen, med henblik på at frembringe tilsvarende beskyttelse« ([225]).

(155) Oplysninger, der overføres til de amerikanske myndigheder i henhold til aftalen mellem Det Forenede Kongerige og USA, bør derfor nyde godt af den beskyttelse, der er fastsat i et EU-retligt instrument, med de tilpasninger, der er nødvendige for at afspejle de omhandlede overførslers art. Myndighederne i Det Forenede Kongerige har endvidere bekræftet, at den beskyttelse, som paraplyaftalen yder, vil finde anvendelse på alle personoplysninger, der frembringes eller opbevares i henhold til aftalen, uanset arten eller typen af det organ, der fremsætter anmodningen (f.eks. både føderale og statslige retshåndhævende myndigheder i USA), således at der i alle tilfælde skal ydes tilsvarende beskyttelse. Myndighederne i Det Forenede Kongerige har imidlertid også forklaret, at detaljerne vedrørende den konkrete gennemførelse af databeskyttelsesgarantierne stadig er genstand for drøftelser mellem Det Forenede Kongerige og USA. I forbindelse med drøftelserne med Kommissionens tjenestegrene om denne afgørelse har myndighederne i Det Forenede Kongerige bekræftet, at de først vil lade aftalen træde i kraft, når de finder det godtgjort, at dens gennemførelse er i overensstemmelse med de retlige forpligtelser, der er fastsat i den, bl.a. vedrørende klarhed med hensyn til overholdelse af databeskyttelsesstandarderne for alle oplysninger, der anmodes om i henhold til aftalen. Da en eventuel ikrafttrædelse af aftalen kan påvirke det beskyttelsesniveau, der vurderes i denne afgørelse, bør Det Forenede Kongerige give Kommissionen meddelelse om enhver information om og fremtidig afklaring af, hvordan USA vil opfylde sine forpligtelser i henhold til aftalen, så snart denne afklaring foreligger, under alle omstændigheder dog inden aftalens ikrafttræden, for at sikre korrekt overvågning af denne afgørelse i overensstemmelse med artikel 45, stk. 4, i forordning (EU) 2016/679. Der vil blive lagt særlig vægt på anvendelsen og tilpasningen af paraplyaftalens beskyttelse af den specifikke type overførsler, der er omfattet af aftalen mellem Det Forenede Kongerige og USA.

(156) Mere generelt vil der blive taget behørigt hensyn til enhver relevant udvikling med hensyn til aftalens ikrafttræden og anvendelse i forbindelse med den løbende overvågning af denne afgørelse, herunder med hensyn til de nødvendige konsekvenser, der skal drages, hvis der er tegn på, at et i det væsentlige tilsvarende beskyttelsesniveau ikke længere er sikret.

3.2.3. *Tilsyn*

(157) Afhængigt af de beføjelser, som de kompetente myndigheder anvender i forbindelse med behandling af personoplysninger med henblik på retshåndhævelse (uanset om det er i henhold til DPA 2018 eller IPA 2016), sikrer forskellige organer tilsyn med anvendelsen af disse beføjelser. Navnlig fører Information Commissioner tilsyn

([219]) Artikel 1, stk. 14, i aftalen.
([220]) Artikel 5, stk. 2, i aftalen.
([221]) Artikel 5, stk. 1, i aftalen.
([222]) Artikel 4, stk. 5, i aftalen. Der gælder yderligere og strengere standarder med hensyn til tidstro aflytning: Kendelserne skal være af begrænset varighed, dvs. ikke længere end hvad der med rimelighed er nødvendigt for at opfylde deres formål, og de må kun udstedes, hvis de samme oplysninger ikke med rimelighed kunne indhentes ved en mindre indgribende metode (aftalens artikel 5, stk. 3).
([223]) Aftale mellem Amerikas Forenede Stater og Den Europæiske Union om beskyttelse af personoplysninger i forbindelse med forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, EUT L 336 af 10.12.2016, s. 3, der findes på følgende link: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:22016A1210(01)&from=DA.
([224]) Artikel 9, stk. 1, i aftalen.
([225]) Artikel 9, stk. 1, i aftalen.

med behandlingen af personoplysninger, når den falder ind under anvendelsesområdet for Part 3 i DPA 2018 ([226]). Uafhængigt og retligt tilsyn med anvendelsen af efterforskningsbeføjelser i henhold til IPA 2016 sikres af Investigatory Powers Commissioner's Office (IPCO) ([227]) (denne del behandles i betragtning 250 til 255). Parlamentet og andre organer sikrer desuden yderligere tilsyn.

3.2.3.1. Tilsyn med Part 3 i DPA 2018

(158) De generelle opgaver, der påhviler Information Commissioner — hvis uafhængighed og organisation er forklaret i betragtning 87 — i forbindelse med behandling af personoplysninger, der er omfattet af Part 3 i DPA 2018, er fastlagt i Schedule 13 til DPA 2018. Information Commissioners hovedopgave er at overvåge og håndhæve Part 3 i DPA 2018 samt at fremme offentlighedens bevidsthed og rådgive parlamentet, regeringen og andre institutioner og organer. Af hensyn til opretholdelsen af retsvæsenets uafhængighed har Information Commissioner ikke bemyndigelse til at udøve sine funktioner i forbindelse med behandling af personoplysninger, som foretages af en person, der handler i egenskab af domstol, eller en ret, som handler i sin egenskab af domstol. Under sådanne omstændigheder vil andre organer varetage tilsynsfunktionerne som forklaret i betragtning 99 til 103.

(159) Information Commissioner har generelle efterforsknings-, korrektions-, godkendelses- og rådgivningsbeføjelser i forbindelse med behandling af personoplysninger, som Part 3 finder anvendelse på. Information Commissioner har navnlig beføjelse til at underrette den dataansvarlige eller databehandleren om en angivelig overtrædelse af Part 3 i DPA 2018, til at give advarsler eller irettesættelser til en dataansvarlig eller databehandler, der har overtrådt bestemmelserne i Part 3 i loven, og til af egen drift eller efter anmodning at afgive udtalelser til parlamentet, regeringen eller andre institutioner og organer samt til offentligheden om ethvert spørgsmål vedrørende beskyttelse af personoplysninger ([228]).

(160) Desuden har Information Commissioner beføjelser til at udstede »information notices« ([229]), »assessment notices« ([230]) og »enforcement notices« ([231]) samt til at få adgang til dataansvarliges og databehandleres dokumenter og lokaler ([232]) og til at udstede administrative bøder i form af »penalty notices ([233])«. Information Commissioner's Regulatory Action Policy beskriver de omstændigheder, hvorunder ICO-kontoret udsteder henholdsvis »information notices«, »assessment notices«, »enforcement notices« og »penalty notices« ([234]) (se også betragtning 93 og betragtning 101-102 i direktiv (EU) 2016/680 vedrørende afgørelser om tilstrækkeligheden af beskyttelsesniveauet).

(161) Information Commissioner har ifølge sine seneste årsberetninger (for 2018-2019 ([235]) og 2019-2020 ([236])) gennemført en række undersøgelser og truffet håndhævelsesforanstaltninger med hensyn til retshåndhævende myndigheders databehandling. Eksempelvis har Information Commissioner gennemført en undersøgelse og i oktober 2019 offentliggjort en udtalelse om de retshåndhævende myndigheders anvendelse af ansigtsgenkendelsesteknologi på offentlige steder. Denne undersøgelse fokuserede navnlig på anvendelsen af ansigtsgenkendelse på stedet hos politiet i South Wales og Metropolitan Police Service (MPS) (politistyrken i Greater London). Information Commissioner har også undersøgt MPS's »Gangs Matrix« ([237]) (database over mistænkte bandemedlemmer i London) og konstateret en række alvorlige overtrædelser af databeskyttelseslovgivningen, som sandsynligvis ville undergrave offentlighedens tillid til databasen og den måde, som dataene blev anvendt på. I november 2018 udstedte Information Commissioner en »enforcement notice«, og MPS tog efterfølgende de nødvendige skridt til at øge sikkerheden og ansvarligheden og til at sikre, at dataene blev anvendt forholdsmæssigt. Et andet eksempel på en håndhævelsesforanstaltning på dette område er den bøde på 325 000 GBP, som Information Commissioner i maj

([226]) Section 116 i DPA 2018.
([227]) Se IPA 2016, navnlig Chapter 1, Part 8.
([228]) Paragraph 2 i Schedule 13 til DPA 2018.
([229]) Pålægger den dataansvarlige og databehandleren (og under visse omstændigheder en anden person) at fremlægge nødvendige oplysninger (Section 142 i DPA 2018).
([230]) Tillader gennemførelse af undersøgelser og revisioner, som kan nødvendiggøre, at den dataansvarlige eller databehandleren tillader, at Information Commissioner får adgang til bestemte lokaler, gennemgår dokumenter eller inspicerer udstyr eller interviewer personer, der behandler personoplysninger på vegne af den dataansvarlige (Section 146 i DPA 2018).
([231]) Tillader udøvelse af korrigerende beføjelser, som pålægger dataansvarlige/databehandlere at træffe eller undlade at træffe bestemte foranstaltninger (Section 149 i DPA 2018).
([232]) Section 154 i DPA 2018.
([233]) Section 155 i DPA 2018.
([234]) Regulatory Action Policy, jf. fodnote 96.
([235]) Information Commissioner's Annual Report and Financial Statements 2018- 19, jf. fodnote 101.
([236]) Information Commissioner's Annual Report and Financial Statements 2019- 20, jf. fodnote 82.
([237]) En database med oplysninger om påståede bandemedlemmer og ofre for banderelaterede forbrydelser.

2018 udstedte mod Crown Prosecution Service (en uafhængig retsforfølgningstjeneste) for at have mistet ukrypterede dvd'er med optagelser af politiafhøringer. Information Commissioner har også gennemført undersøgelser af bredere emner. For eksempel undersøgte ICO i første halvdel af 2020 en praksis med at trække data ud af mobiltelefoner i forbindelse med politiarbejde og politiets behandling af ofrenes data. Desuden er Information Commissioner i øjeblikket i færd med at undersøge en sag, der involverer retshåndhævende myndigheders adgang til data, som en enhed i den private sektor, Clearview AI Inc. ([238]), er i besiddelse af.

(162) Som beskrevet i betragtning 160 og 161 har Information Commissioner en række håndhævelsesbeføjelser. Derudover udgør visse overtrædelser af databeskyttelseslovgivningen strafbare handlinger, som derfor kan gøres til genstand for strafferetlige sanktioner (Section 196 i DPA 2018). Dette gælder f.eks. indsamling, videregivelse og opbevaring af personoplysninger uden den dataansvarliges samtykke og formidling af videregivelse af personoplysninger til en anden person uden den dataansvarliges samtykke ([239]). genidentifikation af oplysninger, der er anonymiserede personoplysninger, uden samtykke fra den dataansvarlige, som er ansvarlig for anonymiseringen af personoplysningerne ([240]), forsætligt at hindre Information Commissioner i at udøve sine beføjelser i forbindelse med kontrol af personoplysninger i overensstemmelse med internationale forpligtelser ([241]), afgive urigtige erklæringer som svar på en »information notice« eller tilintetgøre oplysninger i forbindelse med »information notices« og »assessment notices« ([242]).

3.2.3.2. Andre kontrolorganer inden for strafferetlig håndhævelse

(163) Ud over Information Commissioner findes der flere kontrolorganer inden for strafferetlig håndhævelse med specifikke mandater, der er relevante for databeskyttelsesspørgsmål. Det drejer sig om f.eks. Commissioner for the Retention and Use of Biometric Material (biometrikommissæren, »Biometrics Commissioner« ([243])) og Surveillance Camera Commissioner ([244]) (kommissæren for overvågningskameraer).

3.2.3.3. Parlamentarisk kontrol på det strafferetlige område

(164) Home Affairs Select Committee (det særlige udvalg for indre anliggender, HASC) sikrer parlamentarisk kontrol på retshåndhævelsesområdet. Dette udvalg består af 11 medlemmer af parlamentet, der kommer fra de tre største politiske partier. Udvalget har til opgave at gennemgå udgifter, administration og politik i Home Office og de dertil knyttede offentlige organer, herunder politiet og NCA — hvis arbejde udvalget specifikt kan undersøge ([245]).

([238]) Se ICO's erklæring, som kan findes på følgende 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]) Section 170 i DPA 2018.

([240]) Section 171 i DPA 2018.

([241]) Section 119(6) i DPA 2018.

([242]) I løbet af regnskabsåret, der dækker perioden fra den 1. april 2019 til den 31. marts 2020, har ICO's undersøgelser ført til fire advarsler og otte retsforfølgelser. Disse sager blev retsforfulgt i henhold til Section 55 i Data Protection Act 1998, Section 77 i Freedom of Information Act 2000 og Section 170 i Data Protection Act 2018. I 75 % af sagerne erkendte de tiltalte sig skyldige, og der var således ikke behov for langvarige retssager med de dermed forbundne omkostninger. (Information Commissioner's Annual Report and Financial Statements 2019/2020, jf. fodnote 87, s. 40).

([243]) Biometrics Commissioner blev oprettet ved Protection of Freedoms Act 2012 (lov om beskyttelse af frihedsrettigheder fra 2012) (se: https://www.legislation.gov.uk/ukpga/2012/9/contents). Biometrics Commissioner afgør bl.a., om politiet må opbevare DNA-profilregistreringer og fingeraftryk fra personer, der er anholdt, men ikke anklaget for en kvalificeret lovovertrædelse (Section 63G i PACE 1984). Desuden har denne generelt ansvar for at overvåge opbevaring og anvendelse af DNA og fingeraftryk og opbevaring begrundet i hensyn til statens sikkerhed (Section 20(2) i PoFA 2012). Biometrics Commissioner udpeges i henhold til Code for Public Appointments (loven om offentlige udnævnelser) (loven findes på følgende link: https://www.gov.uk/government/publications/governance-code-for-public-appointments), og i henhold til udnævnelsesbetingelserne kan vedkommende kun afskediges af indenrigsministeren under nøje definerede omstændigheder. Disse omfatter undladelse af at udføre sine opgaver i en periode på tre måneder, domfældelse for en strafbar handling eller manglende opfyldelse af udnævnelsesbetingelserne.

([244]) Surveillance Camera Commissioner blev oprettet ved Protection of Freedoms Act 2012 og har til opgave at tilskynde til overholdelse af Surveillance Camera Code of Practice (adfærdskodeksen for overvågningskameraer), at gennemgå anvendelsen af denne kodeks og at rådgive ministrene om, hvorvidt denne kodeks skal ændres. Den pågældende Commissioner udnævnes efter de samme regler som Biometrics Commissioner og har de samme beføjelser, ressourcer og nyder samme beskyttelse mod fjernelse.

([245]) Se https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/.

(165) Udvalget kan inden for rammerne af sit ansvarsområde vælge, hvad det vil undersøge, herunder konkrete sager, så længe spørgsmålet ikke er indbragt for en domstol. Udvalget kan også indhente skriftlig og mundtlig dokumentation fra en bred vifte af relevante grupper og enkeltpersoner. Det udarbejder rapporter om sine resultater og forelægger anbefalinger for regeringen ([246]). Regeringen forventes at reagere på alle rapportens anbefalinger og skal reagere inden for 60 dage ([247]).

(166) På overvågningsområdet udarbejdede udvalget også en rapport om Regulation of Investigatory Powers Act 2000 (lov om efterforskningsbeføjelser fra 2000, RIPA 2000) ([248]), hvori det blev konstateret, at RIPA 2000 ikke var egnet til formålet. Deres rapport blev taget i betragtning, da betydelige dele af RIPA 2000 blev erstattet med IPA 2016. En fuldstændig liste over undersøgelser findes på udvalgets websted ([249]).

(167) HASC's opgaver varetages i Skotland af Justice Subcommittee on Policing (underudvalget for politispørgsmål under retsudvalget) og i Nordirland af Committee for Justice (retsudvalget) ([250]).

3.2.4. *Klageadgang*

(168) Hvad angår de retshåndhævende myndigheders behandling af oplysninger findes der klagemekanismer i henhold til Part 3 i DPA 2018 og IPA 2016 samt i henhold til Human Rights Act 1998.

(169) Denne række af mekanismer giver de registrerede effektive administrative og retslige klagemuligheder, der navnlig sætter dem i stand til at sikre deres rettigheder, herunder retten til at få adgang til deres personoplysninger eller til at opnå berigtigelse eller sletning af sådanne oplysninger.

(170) For det første har den registrerede i henhold til Section 165 i DPA 2018 ret til at indgive en klage til Information Commissioner, hvis den registrerede mener, at der i forbindelse med personoplysninger, som vedrører vedkommende, foreligger en overtrædelse af Part 3 i DPA 2018 ([251]). Information Commissioner har beføjelse til at vurdere den dataansvarliges og databehandlerens overholdelse af DPA 2018, kræve, at de tager de nødvendige skridt i tilfælde af manglende overholdelse, og pålægge dem bøder.

([246]) Særlige udvalg, herunder Home Affairs Select Committee, er underlagt Standing Orders of the House of Commons (Underhusets forretningsorden). Standing Orders er regler, der er vedtaget af Underhuset, og som regulerer den måde, hvorpå parlamentet fungerer. De særlige udvalgs sagsområde er bredt, idet Standing Order 152(1) bestemmer, at »de særlige udvalg udpeges til at gennemgå udgifter, administration og politik for de vigtigste ministerier, jf. paragraph (2) i denne bekendtgørelse, og de tilknyttede offentlige organer«. Dette giver Home Affairs Select Committee mulighed for at undersøge enhver politik, der hører under Home Office, og som omfatter politikker (og tilhørende lovgivning) vedrørende efterforskningsbeføjelser. Endvidere fremgår det af Standing Order 152(4), at udvalgene har forskellige beføjelser, herunder til at anmode personer om at afgive forklaring eller fremlægge dokumenter om et bestemt emne og til at udarbejde rapporter. TUdvalgets nuværende og tidligere undersøgelser findes på følgende link: https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Beføjelserne for Home Affairs Select Committee i England og Wales er fastlagt i Standing Orders of the House of Commons, som findes på følgende link: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Findes på følgende link: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm.

([249]) Findes på følgende link: https://committees.parliament.uk/committee/83/home-affairs-committee.

([250]) Reglerne for Justice Subcommittee on Policing i Skotland findes på følgende link https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, og reglerne for Committee of Justice i Nordirland findes på følgende link: http://www.niassembly.gov.uk/assembly-business/standing-orders/.

([251]) ICO's seneste årsberetning indeholder en oversigt over arten af de klager, der er modtaget og færdigbehandlet. Navnlig udgør antallet af indkomne klager vedrørende »politi- og strafferegistre« 6 % af det samlede antal indkomne klager (en stigning på 1 % i forhold til det foregående regnskabsår). Årsberetningen viser også, at klager vedrørende registreredes anmodninger om aktindsigt udgør det højeste antal (46 % af det samlede antal klager, en stigning på 8 % i forhold til det foregående regnskabsår) (ICO's årsberetning 2019-2020, s. 55; se fodnote 88).

(171) For det andet giver DPA 2018 adgang til retsmidler over for Information Commissioner, hvis denne ikke behandler en klage fra den registrerede korrekt. Nærmere bestemt: Hvis Information Commissioner ikke »gør fremskridt« ([252]) med en klage indgivet af den registrerede, har klageren adgang til retsmidler, idet denne kan anmode First Tier Tribunal ([253]) (ret i første instans) om at pålægge Information Commissioner at træffe passende foranstaltninger til at besvare klagen eller underrette klageren om forløbet af klagen ([254]). Desuden kan enhver person, der modtager en af ovennævnte meddelelser (information, assessment, enforcement eller penalty notice) fra Information Commissioner, appellere til en First Tier Tribunal. Hvis denne First Tier Tribunal finder, at Information Commissioners afgørelse ikke er i overensstemmelse med loven, eller hvis Information Commissioner burde have udøvet sin skønsbeføjelse anderledes, skal retten tage appellen til følge eller erstatte meddelelsen med en anden meddelelse eller afgørelse, som Information Commissioner måtte have forkyndt eller truffet ([255]).

(172) For det tredje kan enkeltpersoner anlægge sag direkte mod dataansvarlige og databehandlere ved domstolene. Navnlig kan en registreret i henhold til Section 167 i DPA 2018 anlægge sag ved domstolen om krænkelse af sine rettigheder i henhold til databeskyttelseslovgivningen, og domstolen kan ved kendelse anmode den dataansvarlige om at tage (eller undlade at tage) et hvilket som helst skridt med hensyn til behandlingen for at overholde DPA 2018. I henhold til Section 169 i DPA 2018 har enhver, der har lidt skade som følge af en overtrædelse af et krav i databeskyttelseslovgivningen (herunder Part 3 i DPA 2018), ud over UK GDPR, desuden ret til erstatning fra den dataansvarlige eller databehandleren for denne skade, medmindre den dataansvarlige eller databehandleren godtgør, at den dataansvarlige eller databehandleren ikke på nogen måde er ansvarlig for den begivenhed, der forårsagede skaden. Skader omfatter både økonomiske tab og skader, der ikke indebærer økonomiske tab, såsom overlast.

(173) Endelig kan enhver person, for så vidt som de mener, at deres rettigheder, herunder retten til privatlivets fred og databeskyttelse, er blevet krænket af offentlige myndigheder, indbringe sagen for domstolene i Det Forenede Kongerige i henhold til Human Rights Act 1998 ([256]), og efter at have udtømt de nationale retsmidler kan en person, en ikkestatslig organisation og grupper af enkeltpersoner indbringe sager for Den Europæiske Menneskerettighedsdomstol for krænkelser af de rettigheder, der er garanteret i henhold til den europæiske menneskerettighedskonvention ([257]) (se betragtning 111).

3.2.4.1. Klagemekanismer under IPA 2016

(174) Enkeltpersoner kan få erstatning for overtrædelser af IPA 2016 ved Investigatory Powers Tribunal. De klagemuligheder, der er tilgængelige under IPA 2016, er beskrevet i betragtning 263 til 269 nedenfor.

([252]) Section 166 i DPA 2018 omhandler specifikt følgende situationer: a) Information Commissioner undlader at træffe passende foranstaltninger for at reagere på klagen, b) Information Commissioner undlader at give klageren oplysninger om forløbet af klagen eller om resultatet af klagen inden udløbet af den periode på 3 måneder, der begynder på det tidspunkt, hvor Information Commissioner modtager klagen, eller c) hvis Information Commissioners behandling af klagen ikke er afsluttet i løbet af denne periode, undlader at give klageren sådanne oplysninger i en efterfølgende periode på 3 måneder.

([253]) First Tier Tribunal er den domstol, der har kompetence til at behandle klager over afgørelser truffet af statslige tilsynsorganer. For så vidt angår Information Commissioners afgørelse er den kompetente afdeling »General Regulatory Chamber« (afdelingen for sager om statsligt tilsyn), som har kompetence i hele Det Forenede Kongerige.

([254]) Section 166 i DPA 2018. Eksempler på søgsmål mod ICO, hvor sagsøger fik medhold ved retten, omfatter en sag, hvor ICO bekræftede modtagelsen af en klage fra en registreret, men ikke angav, hvilken fremgangsmåde den agtede at følge, og derfor blev dømt til inden for 21 kalenderdage at bekræfte, om den ville undersøge klagerne og, hvis dette var tilfældet, informere klageren om undersøgelsens forløb mindst hver 21. kalenderdag (dommen er endnu ikke offentliggjort), og en sag, hvor First Tier Tribunal fandt, at det var uklart, hvorvidt ICO's svar til en klager udgjorde »resultatet« af klagen (se Susan Milne v The Information Commissioner [2020]; dommen kan findes på følgende link:. https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) Section 162 og 163 i DPA 2018.

([256]) Se f.eks. Brown mod Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724, hvor der blev tilkendt en erstatning på 9 000 GBP i henhold til DPA 1998 og Human Rights Act 1998 for ulovlig indsamling og misbrug af personoplysninger, og R (on the application of Bridges) mod Chief Constable of South Wales [2020] EWCA Civ 1058, hvor Court of Appeal erklærede, at det walisiske politis anvendelse af et ansigtsgenkendelsessystem var ulovlig, da det var i strid med artikel 8 i EMRK, og da konsekvensanalysen vedrørende databeskyttelse, som den dataansvarlige havde gennemført, ikke var i overensstemmelse med DPA 2018.

([257]) Artikel 34 i den europæiske menneskerettighedskonvention fastsætter, at »[d]omstolen kan modtage klager fra enhver person, enhver ikkestatslig organisation eller gruppe af enkeltpersoner, der hævder at være blevet krænket af en af de høje kontraherende parter i de rettigheder, der er anerkendt ved denne konvention eller de dertil knyttede protokoller. De høje kontraherende parter forpligter sig til ikke på nogen måde at lægge hindringer i vejen for den effektive udøvelse af denne ret«.

3.3. **Det Forenede Kongeriges myndigheders adgang og brug med henblik på nationale sikkerhedsformål**

(175) I Det Forenede Kongeriges retsorden har følgende efterretningstjenester beføjelse til at indsamle elektroniske oplysninger, som dataansvarlige eller databehandlere er i besiddelse af af hensyn til den nationale sikkerhed, i situationer, der er relevante for et tilstrækkelighedsscenarie: Security Service ([258]) (sikkerhedstjenesten, MI5), Secret Intelligence Service ([259]) (efterretningstjenesten, SIS) og Government Communications Headquarters ([260]) (regeringens hovedkvarter for kommunikation, GCHQ) ([261]).

3.3.1. *Retsgrundlag, begrænsninger og garantier*

(176) I Det Forenede Kongerige er efterretningstjenesternes beføjelser fastlagt i IPA 2016 og RIPA 2000, som sammen med DPA 2018 fastsætter det fysiske og personlige anvendelsesområde for disse beføjelser samt begrænsninger og garantier med hensyn til anvendelsen heraf. Disse beføjelser samt de begrænsninger og garantier, der gælder for dem, vurderes i detaljer i de følgende afsnit.

3.3.1.1. Efterforskningsbeføjelser udøvet i forbindelse med statens sikkerhed

(177) IPA 2016 udgør den retlige ramme for anvendelsen af efterforskningsbeføjelser, dvs. beføjelsen til at aflytte og skaffe sig adgang til kommunikationsdata og foretage indgreb i udstyr. Med IPA 2016 indføres et generelt forbud, og det gøres til en strafbar handling at anvende teknikker, der giver adgang til indholdet af kommunikation eller til kommunikationsdata, eller at foretage indgreb i udstyr uden lovlig bemyndigelse ([262]). Dette afspejles i, at anvendelsen af disse efterforskningsbeføjelser kun er lovlig, når den finder sted på grundlag af en kendelse eller en tilladelse ([263]).

(178) IPA 2016 fastsætter detaljerede regler for omfanget og anvendelsen af de enkelte efterretningsbeføjelser samt deres specifikke begrænsninger og garantier. Der gælder forskellige regler afhængigt af typen af efterforskningsbeføjelser (aflytning af kommunikation, indsamling og opbevaring af kommunikationsdata og indgreb i

([258]) MI5 er underlagt Home Secretarys myndighed. Security Service Act 1989 fastsætter MI5's funktioner: beskytte den nationale sikkerhed (herunder beskyttelse mod trusler om spionage, terrorisme og sabotage, mod udenlandske magters aktiviteter og mod handlinger, der har til formål at vælte eller underminere det parlamentariske demokrati ved hjælp af politiske, industrielle eller voldelige midler), beskytte Det Forenede Kongeriges økonomiske velfærd mod eksterne trusler og støtte politistyrkernes og andre retshåndhævende myndigheders aktiviteter i forbindelse med forebyggelse og afsløring af grov kriminalitet.

([259]) SIS er underlagt Foreign Secretarys myndighed, og dens funktioner er fastsat i Intelligence Services Act 1994. Den har til opgave at indsamle og tilvejebringe oplysninger om handlinger eller hensigter hos personer uden for De Britiske Øer og at udføre andre opgaver i forbindelse med sådanne personers handlinger eller hensigter. Disse funktioner kan kun udøves af hensyn til den nationale sikkerhed, af hensyn til Det Forenede Kongeriges økonomiske velfærd eller til støtte for forebyggelse eller afsløring af grov kriminalitet.

([260]) GCHQ er underlagt Foreign Secretarys myndighed, og dets funktioner er fastsat i Intelligence Services Act 1994. Det drejer sig om a) at overvåge, udnytte eller aflytte elektromagnetiske og andre emissioner og udstyr, der frembringer sådanne emissioner, at indsamle og tilvejebringe oplysninger afledt af eller relateret til sådanne emissioner eller sådant udstyr og af krypteret materiale, b) at yde rådgivning og bistand vedrørende sprog, herunder terminologi, der anvendes i forbindelse med tekniske spørgsmål og kryptografi, og andre spørgsmål vedrørende beskyttelse af oplysninger til de væbnede styrker, regeringen eller andre organisationer eller personer, der anses for passende. Disse funktioner kan kun udøves af hensyn til den nationale sikkerhed, af hensyn til Det Forenede Kongeriges økonomiske velfærd i forbindelse med handlinger eller hensigter fra personer uden for De Britiske Øer eller til støtte for forebyggelse eller afsløring af grov kriminalitet.

([261]) Andre offentlige organer, der varetager funktioner, som er relevante for den nationale sikkerhed, er Defence Intelligence (DI), National Security Council and Secretariat, Joint Intelligence Organisation (JIO) og Joint Intelligence Committee (JIC). Hverken JIC eller JIO kan imidlertid gøre brug af efterforskningsbeføjelser i henhold til IPA 2016, mens DI har begrænsede muligheder for at udnytte sine beføjelser.

([262]) Forbuddet gælder både offentlige og private kommunikationsnet samt den offentlige posttjeneste, når aflytningen finder sted i Det Forenede Kongerige. Forbuddet gælder ikke for den dataansvarlige for det private netværk, hvis den dataansvarlige udtrykkeligt eller stiltiende har givet samtykke til at foretage aflytningen (Section 3 i IPA 2016).

([263]) I særlige begrænsede tilfælde er lovlig aflytning uden retskendelse mulig, dvs. ved aflytning med afsenderens eller modtagerens samtykke (Section 44 i IPA 2016), ved begrænsede administrative eller håndhævelsesmæssige formål (Section 45-48 i IPA), i visse særlige institutioner (Section 49- 51 i IPA 2016) og i henhold til oversøiske anmodninger (Section 52 i IPA 2016).

udstyr) ([264]) samt af, om beføjelsen udøves på et bestemt mål eller som masseaflytning. Nærmere oplysninger om anvendelsesområde, garantier og begrænsninger for hver foranstaltning under IPA 2016 er beskrevet i det specifikke afsnit nedenfor.

(179) Desuden suppleres IPA 2016 med en række lovfæstede adfærdskodekser, der er udstedt af Secretary of State og godkendt af begge kamre i parlamentet ([265]), som gælder i hele landet, og som indeholder yderligere vejledning om anvendelsen af disse beføjelser ([266]). Selv om de registrerede direkte kan påberåbe sig bestemmelserne i IPA 2016 for at udøve deres rettigheder, præciseres det i Schedule 7, paragraph 5, til IPA 2016, at adfærdskodekserne kan anvendes som bevismateriale i civile sager og straffesager, og at domstolen, retten eller tilsynsmyndigheden kan tage hensyn til enhver manglende overholdelse af kodekserne, når de skal afgøre et relevant spørgsmål i retssager ([267]). I forbindelse med sin vurdering af »lovgivningens kvalitet« i Det Forenede Kongeriges tidligere lovgivning på tilsynsområdet, RIPA 2000, anerkendte Den Europæiske Menneskerettighedsdomstols Store Afdeling udtrykkeligt relevansen af Det Forenede Kongeriges adfærdskodeks og accepterede, at dens bestemmelser kunne tages i betragtning ved vurderingen af forudsigeligheden af den lovgivning, der tillader overvågning ([268]).

(180) Det skal også bemærkes, at de nationale sikkerhedsagenturer og visse retshåndhævende myndigheder ([269]) har adgang til målrettede beføjelser (målrettet aflytning ([270]), indsamling af kommunikationsdata ([271]), opbevaring af kommunikationsdata ([272]) og målrettede indgreb i udstyr ([273])), mens det kun er efterretningstjenesterne, der kan gøre brug af masseindsamling (f.eks. masseaflytning ([274]), masseindsamling af kommunikationsdata ([275]), masseindgreb i udstyr ([276]) og datasæt med massepersonoplysninger ([277])).).

(181) Ved afgørelsen af hvilken efterforskningsbeføjelse der skal anvendes, skal efterretningstjenesten opfylde de »generelle forpligtelser vedrørende privatlivets fred«, der er anført i Section 2(2)(a) i IPA 2016, som omfatter en nødvendigheds- og proportionalitetstest. Nærmere bestemt skal en offentlig myndighed, der har til hensigt at gøre brug af en undersøgelsesbeføjelse, i henhold til denne bestemmelse overveje, i) om det, der søges opnået med kendelsen,

([264]) Hvad angår f.eks. anvendelsesområdet for sådanne foranstaltninger er foranstaltningens anvendelsesområde i henhold til Part 3 og Part 4 (opbevaring og indsamling af kommunikationsdata) nøje knyttet til definitionen af »teleoperatører«, hvis brugeres data er omfattet af foranstaltningen. Der kan gives et andet eksempel i forbindelse med anvendelsen af »massebeføjelser«. I dette tilfælde er omfanget af disse beføjelser begrænset til »meddelelser, der sendes eller modtages af enkeltpersoner uden for den britiske ø«.

([265]) I Schedule 7 til IPA 2016 er anvendelsesområdet for kodekserne, den procedure, der skal følges ved udstedelsen af dem, reglerne for revision af dem og virkningen af kodekserne fastsat.

([266]) Adfærdskodekserne under IPA 2016 findes på følgende link: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

([267]) Domstolene og retterne anvender adfærdskodeksen til at vurdere lovligheden af myndighedernes handlinger. Se f.eks.: Dias mod Cleveland Police, [2017] UKIPTrib15_586-CH, hvor Investigatory Powers Tribunal henviste til specifikke passager i Code of Practice on Communication Data (adfærdskodeksen for kommunikationsdata) for at forstå definitionen af grundlaget for »forebyggelse eller afsløring af kriminalitet eller forebyggelse af uro«, der blev anvendt til at indsamle kommunikationsdata. Kodeksen er medtaget i begrundelsen for at fastslå, om denne begrundelse er blevet anvendt forkert. Retten konkluderede derefter, at de anfægtede handlinger var ulovlige. Domstolene har også foretaget en evaluering af beskyttelsesniveauet i kodekserne, se f.eks. Just for Law Kids mod Secretary of State for the Home Department [2019] EWHC 1772 (Admin), hvor High Court fandt, at primær og afledt ret sammen med de interne retningslinjer gav tilstrækkelige garantier. Eller R (National Council for Civil Liberties) mod Secretary of State for the Home Department & Others [2019] EWHC 2057 (Admin), hvor den fandt, at både IPA 2016 og Code of Practice on Equipment Interference (adfærdskodeksen om indgreb i udstyr) indeholdt tilstrækkelige bestemmelser om behovet for særlige kendelser.

([268]) I Big Brother Watch-sagen anerkendte Den Europæiske Menneskerettighedsdomstols Store Afdeling, at »IC Code er et offentligt dokument, der skal godkendes af begge kamre i parlamentet, der offentliggøres af regeringen online og i en trykt udgave, og som skal tages i betragtning både af dem, der udfører aflytningsopgaver, og af domstole og retter (se præmis 93-94 ovenfor). Domstolen har således accepteret, at dens bestemmelser kan tages i betragtning ved vurderingen af forudsigeligheden af RIPA (jf. Kennedy-dommen ovenfor, præmis 157). Domstolen ville derfor acceptere, at national ret var tilstrækkeligt «tilgængelig».« (Se Den Europæiske Menneskerettighedsdomstols Store Afdelings dom af 25. maj 2021, Big Brother Watch m.fl. mod Det Forenede Kongerige, sag nr. 58170/13, 62322/14 og 24960/15, præmis 366).

([269]) Listen over relevante retshåndhævende myndigheder, der kan udøve målrettede efterforskningsbeføjelser i henhold til IPA 2016, findes i fodnote (139).

([270]) Part 2 i IPA 2016.

([271]) Part 3 i IPA 2016.

([272]) Part 4 i IPA 2016.

([273]) Part 5 i IPA 2016.

([274]) Section 136 i IPA 2016.

([275]) Section 158 i IPA 2016.

([276]) Section 176 i IPA 2016.

([277]) Section 199 i IPA 2016.

tilladelsen eller meddelelsen, med rimelighed kan opnås med andre, mindre indgribende midler, ii) om det beskyttelsesniveau, der skal anvendes i forbindelse med indsamling af oplysninger i medfør af kendelsen, tilladelsen eller meddelelsen, er højere på grund af disse oplysningers særligt følsomme karakter, iii) offentlighedens interesse i telekommunikationssystemernes og posttjenesternes integritet og sikkerhed og iv) alle andre aspekter af offentlighedens interesse i beskyttelsen af privatlivets fred ([278]).

(182) Måden, hvorpå disse kriterier skal anvendes — og måden, hvorpå deres overholdelse vurderes som led i Secretary of States og de uafhængige Judicial Commissioners tilladelse til at anvende sådanne beføjelser — præciseres yderligere i de relevante adfærdskodekser. Navnlig skal anvendelsen af en af disse efterforskningsbeføjelser altid »stå i et rimeligt forhold til det, der søges opnået, [som] indebærer en afvejning af alvoren af krænkelsen af privatlivets fred (og andre hensyn, der er anført i Section 2(2)) i forhold til behovet for aktiviteten af efterforsknings-, drifts- eller kapacitetsmæssige grunde«. Dette betyder navnlig, at den »bør give en realistisk udsigt til at opnå den forventede fordel og ikke være uforholdsmæssig eller vilkårlig«, og at »[i]ntet indgreb i privatlivets fred bør anses for at stå i et rimeligt forhold til formålet, hvis de oplysninger, der efterspørges, med rimelighed kan fremskaffes ved andre, mindre indgribende midler« ([279]). Nærmere bestemt skal overholdelsen af proportionalitetsprincippet vurderes på grundlag af følgende kriterier: »i) omfanget af det foreslåede indgreb i privatlivets fred i forhold til, hvad der søges opnået, ii) hvordan og hvorfor de metoder, der skal anvendes, vil medføre det mindst mulige indgreb over for den pågældende person og andre, iii) om aktiviteten udgør en hensigtsmæssig anvendelse af loven og en rimelig metode efter at have overvejet alle rimelige alternativer til at opnå det, der søges opnået, iv) hvilke andre metoder, alt efter hvad der er relevant, der enten ikke er blevet indført eller ikke er blevet anvendt, men som vurderes at være utilstrækkelige til at opfylde operationelle mål uden brug af den foreslåede undersøgelsesbeføjelse« ([280]).

(183) Som forklaret af Det Forenede Kongeriges myndigheder sikrer dette i praksis, at en efterretningstjeneste for det første fastsætter det operationelle mål (og dermed afgrænser indsamlingen, f.eks. et mål vedrørende international terrorbekæmpelse i et bestemt geografisk område), og for det andet på grundlag af dette operationelle mål skal overveje, hvilken teknisk mulighed (f.eks. målrettet aflytning eller masseaflytning, indgreb i udstyr, indsamling af kommunikationsdata) der er mest forholdsmæssig (dvs. udgør det mindste indgreb i privatlivets fred, jf. Section 2(2) i IPA), i forhold til, hvad der søges opnået, og som derfor kan godkendes i henhold til gældende lovgivning.

(184) Det er værd at bemærke, at denne anvendelse af standarder for nødvendighed og proportionalitet også er blevet bemærket og hilst velkommen af FN's særlige rapportør om retten til privatlivets fred, Joseph Cannataci, som med hensyn til det system, der blev indført ved IPA 2016, anførte, at »[d]e procedurer, der er indført både inden for efterretningstjenesterne og inden for de retshåndhævende myndigheder, kræver tilsyneladende systematisk, at der tages hensyn til nødvendigheden og proportionaliteten af en overvågningsforanstaltning eller en overvågningsoperation, inden den anbefales til godkendelse, samt et tilsyn på det samme grundlag« ([281]). Han bemærkede også, at han på sit møde med repræsentanter for de retshåndhævende myndigheder og de nationale sikkerhedsagenturer »konstaterede, at der var enighed om, at retten til privatlivets fred skal komme i første række i forbindelse med enhver beslutning om overvågningsforanstaltninger. Alle forstod og påskønnede nødvendigheden og proportionaliteten som hovedprincipper, der skal tages i betragtning«.

([278]) I Code of Practice on Interception of Communications (adfærdskodeksen for aflytning af kommunikation) præciseres det, at andre elementer i proportionalitetstesten er: »i) omfanget af det foreslåede indgreb i privatlivets fred i forhold til, hvad der søges opnået, ii) hvordan og hvorfor de metoder, der skal anvendes, vil medføre det mindst mulige indgreb over for den pågældende person og andre, iii) om aktiviteten udgør en hensigtsmæssig anvendelse af loven og en rimelig metode efter at have overvejet alle rimelige alternativer til at opnå det, der søges opnået, iv) hvilke andre metoder, alt efter hvad der er relevant, der enten ikke er blevet indført eller ikke er blevet anvendt, men som vurderes at være utilstrækkelige til at opfylde operationelle mål uden brug af den foreslåede undersøgelsesbeføjelse«. Code of Practice on Interception of Communications, paragraph 4.16, som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([279]) Se Code of Practice on Interception of Communications, paragraph 4.12 og 4.15, som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([280]) Se Code of Practice on Interception of Communications, paragraph 4.16.

([281]) End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, som findes på følgende link: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, afsnit 1.a.

(185) De specifikke kriterier for udstedelse af de forskellige kendelser samt de begrænsninger og garantier, der er fastsat i IPA 2016 for hver undersøgelsesbeføjelse, er nærmere beskrevet i betragtning 186 til 243.

3.3.1.1.1. Målrettet aflytning og undersøgelse

(186) Der findes tre typer kendelser for målrettet aflytning: en kendelse om målrettet aflytning ([282]), en kendelse om målrettet undersøgelse og en kendelse om gensidig bistand ([283]). Betingelserne for at opnå disse kendelser og de relevante sikkerhedsforanstaltninger er fastsat i Part 2, Chapter 1, i IPA 2016.

(187) En kendelse om målrettet aflytning giver mulighed for aflytning af den kommunikation, der er beskrevet i kendelsen, under transmission af denne og for indsamling af andre data, der er relevante for denne kommunikation ([284]), herunder sekundære data ([285]). En kendelse om målrettet undersøgelse gør det muligt for en person at udvælge og undersøge aflyttet indhold, der er indsamlet i henhold til en masseaflytningskendelse ([286]).

(188) Enhver kendelse i henhold til Part 2 i IPA 2016 kan udstedes af Secretary of State ([287]) og godkendes af en Judicial Commissioner ([288]). Under alle omstændigheder er varigheden af enhver form for målrettet kendelse begrænset til seks måneder ([289]), og der gælder særlige regler for ændring ([290]) og fornyelse ([291]) heraf.

(189) Inden udstedelsen af kendelsen skal Secretary of State foretage en vurdering af nødvendighed og proportionalitet ([292]). I forbindelse med en kendelse om målrettet aflytning og en kendelse om målrettet undersøgelse bør Secretary of State navnlig kontrollere, om foranstaltningen er nødvendig af en af følgende grunde: hensynet til den nationale sikkerhed forebyggelse eller afsløring af grov kriminalitet eller hensynet til Det Forenede Kongeriges økonomiske velfærd ([293]), for så vidt som disse interesser også er relevante for den nationale sikkerhed ([294]). På den anden side kan der kun udstedes en kendelse om gensidig bistand (se betragtning 139 ovenfor), hvis Secretary of State mener, at der foreligger omstændigheder svarende til dem, hvorunder han/hun ville udstede en kendelse med henblik på at forebygge og afsløre grov kriminalitet ([295]).

(190) Desuden bør Secretary of State vurdere, om foranstaltningen står i rimeligt forhold til det, der søges opnået ([296]). Vurderingen af proportionaliteten af de foranstaltninger, der anmodes om, skal tage hensyn til de generelle forpligtelser vedrørende privatlivets fred, der er fastsat i Section 2(2) i IPA 2016, navnlig behovet for at vurdere, om det, der søges opnået med kendelsen, tilladelsen eller meddelelsen, med rimelighed kan opnås med andre, mindre

([282]) Section 15(2) i IPA 2016.
([283]) Section 15(4) i IPA 2016.
([284]) Section 15(2) i IPA 2016.
([285]) Sekundære data er data, der er vedhæftet eller logisk forbundet med den aflyttede kommunikation, som logisk kan adskilles fra den, og, hvis en sådan adskillelse foretages, ikke afslører noget af, hvad der med rimelighed kan anses for at være betydningen (om nogen) af kommunikationen. Nogle eksempler på sekundære data omfatter routerkonfigurationer eller firewalls eller den periode, hvor en router har været aktiv på et netværk, når de indgår i, er forbundet med eller logisk tilknyttet den aflyttede kommunikation. Se definitionen i Section 16 i IPA 2016 og Code of Practice on Interception of Communications, paragraph 2.19, jf. fodnote 278 for yderligere oplysninger.
([286]) Denne undersøgelse foretages som en undtagelse fra Section 152, stk. 4, i IPA 2016, der indeholder et forbud mod at søge at identificere kommunikation fra personer, der befinder sig på De Britiske Øer. Jf. betragtning 229.
([287]) Den skotske minister godkender kendelsen, når den vedrører grov kriminel aktivitet i Skotland (se Section 21 og Section 22 i IPA 2016), mens Secretary of State kan udpege en højtstående embedsmand til at udstede en kendelse om gensidig bistand, når det viser sig, at aflytningen vedrører en eller flere personer eller lokaliteter uden for Det Forenede Kongerige (Section 40 i IPA 2016).
([288]) Section 19 og 23 i IPA 2016.
([289]) Section 32 i IPA 2016.
([290]) Section 39 i IPA 2016. De foreskrevne personer kan foretage begrænsede ændringer af kendelsen på de betingelser, der er fastsat i IPA 2016. Den person, der har udstedt en kendelse, kan når som helst annullere den. Den pågældende skal gøre dette, hvis kendelsen ikke længere er nødvendig af nogen relevant grund, eller hvis de handlinger, der tillades i henhold til kendelsen, ikke længere står i et rimeligt forhold til det, der søges opnået.
([291]) Section 33 i IPA 2016. Afgørelsen om forlængelse af kendelsen skal godkendes af en Judicial Commissioner.
([292]) Section 19 i IPA 2016.
([293]) Med hensyn til begrebet »Det Forenede Kongeriges økonomiske velfærdsinteresser, når disse interesser også er relevante for den nationale sikkerhed«, henviser Den Europæiske Menneskerettighedsdomstols Store Afdeling i sagen Big Brother Watch m.fl. mod Det Forenede Kongerige (jf. fodnote 268 ovenfor), præmis 371, til, at dette begreb ikke var tilstrækkelig fokuseret på national sikkerhed. Selv om rettens konklusion i denne sag vedrørte anvendelsen af dette begreb i RIPA 2000, anvendes det samme begreb i IPA 2016.
([294]) Section 20(2) i IPA 2016.
([295]) Section 20(3) i IPA 2016.
([296]) Section 19(1)(b), 19(2)(b) og 19(3)(b) i IPA 2016.

indgribende midler, og om det beskyttelsesniveau, der skal anvendes i forbindelse med indsamling af oplysninger i henhold til kendelsen, er højere på grund af disse oplysningers særligt følsomme karakter (se betragtning 181 ovenfor).

(191) Med henblik herpå skal Secretary of State tage hensyn til alle elementerne i ansøgningen fra den myndighed, der indgiver anmodningen, navnlig dem, der vedrører de personer, hvis kommunikation skal aflyttes, samt foranstaltningens relevans for undersøgelsen. Sådanne elementer er beskrevet i Code of Practice on Interception of Communications og skal beskrives med en vis detaljeringsgrad ([297]). Desuden kræves det i Section 17 i IPA 2016, at enhver kendelse udstedt i henhold til Chapter 2 skal angive eller beskrive den specifikke person eller gruppe af personer, eller de organisationer eller lokaliteter, der skal aflyttes (»målet«). I tilfælde af en kendelse om målrettet aflytning eller en kendelse om målrettet undersøgelse kan disse også vedrøre en gruppe personer, mere end én person eller organisation eller mere end ét sæt lokaler (også kaldet »thematic warrant« (tematisk kendelse)) ([298]). I disse tilfælde bør kendelsen beskrive det fælles formål eller den fælles aktivitet for gruppen af personer eller operationen/undersøgelserne og angive eller beskrive så mange af de personer/organisationer eller sæt af lokaliteter, som det med rimelighed er praktisk muligt ([299]). Endelig skal alle de kendelser, der afsiges i henhold til Part 2 i IPA 2016, indeholde oplysninger om adresser, numre, apparater, faktorer eller kombinationer af faktorer, der skal anvendes til at identificere meddelelserne ([300]). I denne forbindelse præciseres det i Code of Practice on Interception of Communications, at i tilfælde af en kendelse om målrettet aflytning og en kendelse om målrettet undersøgelse »skal kendelsen angive (eller beskrive) de faktorer eller en kombination af faktorer, der skal anvendes til at identificere kommunikationen. Hvis kommunikationen f.eks. skal identificeres ved henvisning til et telefonnummer, skal nummeret angives i sin helhed. Men hvis der skal anvendes meget komplekse eller konstant skiftende internets-elektorer til at identificere kommunikationen, bør disse selektorer så vidt muligt beskrives« ([301]).

(192) En vigtig garanti i denne forbindelse er, at den vurdering, som Secretary of State foretager med henblik på at udstede en kendelse, skal godkendes af en Judicial Commissioner ([302]), der navnlig vil kontrollere, om afgørelsen om at udstede kendelsen er i overensstemmelse med nødvendigheds- og proportionalitetsprincipperne ([303]) (om Judicial Commissioners status og rolle, se betragtning 251 til 256 nedenfor). I IPA 2016 præciseres det også, at Judicial Commissioner ved gennemførelsen af en sådan kontrol skal anvende de samme principper, som en domstol ville anvende i forbindelse med en anmodning om domstolsprøvelse ([304]). Dette sikrer, at overholdelsen af nødvendigheds- og proportionalitetsprincippet i hvert enkelt tilfælde, og inden der gives adgang til data, kontrolleres systematisk af et uafhængigt organ.

(193) I IPA 2016 er der fastsat få specifikke og snævre undtagelser for målrettet aflytning uden retskendelse. De begrænsede tilfælde er nærmere beskrevet i loven ([305]), og bortset fra sager, der er baseret på afsenderens/modtagerens »samtykke«, gennemføres de af personer (private eller offentlige organer), der er forskellige fra de nationale sikkerhedsagenturer. Desuden foretages denne type aflytning til andre formål end indsamling af »efterretninger« ([306]), og for nogle af dem er det meget usandsynligt, at indsamlingen kan finde sted i forbindelse med

([297]) De oplysninger, der anmodes om, omfatter oplysninger om baggrunden (beskrivelse af personer/organisationer/sæt af lokaler, den kommunikation, der skal aflyttes), og hvordan indsamling af disse oplysninger vil gavne undersøgelsen samt en beskrivelse af de handlinger, der skal godkendes. Hvis det ikke er muligt at beskrive personerne/organisationen/lokalerne, skal der gives en forklaring på, hvorfor det ikke var muligt, eller hvorfor der kun blev givet en generel beskrivelse (Code of Practice on Interception of Communications, paragraph 5.32 og 5.34, jf. fodnote 278).

([298]) Section 17(2) i IPA 2016. Se også Code of Practice on Interception of Communications, paragraph 5.11 ff., jf. fodnote 278.

([299]) Section 31(4) og (5) i IPA 2016.

([300]) Section 31(8) i IPA 2016.

([301]) Code of Practice on Interception of Communications, paragraph 5.37 og 5.38, jf. fodnote 278.

([302]) Der kræves ikke godkendelse fra en Judicial Commissioner, når Secretary of State mener, at der er et presserende behov for at udstede kendelsen (Section 19, stk. 1, i IPA). Judicial Commissioner skal imidlertid underrettes inden for kort tid og skal afgøre, om kendelsen skal godkendes eller ej. Hvis det ikke er tilfældet, ophører kendelsen med at have virkning (Section 24 og 25 i IPA 2016).

([303]) Section 23(1) i IPA 2016.

([304]) Section 23(2) i IPA 2016.

([305]) Se Section 44-51 i IPA 2016 og Section 12 i Interception Communication Code of Practice (jf. fodnote 278).

([306]) Dette er eksempelvis tilfældet, når der er behov for en aflytning i fængslet eller på et psykiatrisk hospital (for at kontrollere tilbageholdte personers eller patienters adfærd) eller af en post- eller teleoperatør, f.eks. for at afsløre misbrug af indhold.

et »overførselsscenarie« (f.eks. i tilfælde af aflytning på psykiatriske hospitaler eller i fængsler). I betragtning af karakteren af det organ, som disse specifikke sager finder anvendelse på (som er forskellige fra de nationale sikkerhedsagenturer), vil alle de garantier, der er fastsat i Part 2 i DPA 2018 og UK GDPR, finde anvendelse, herunder ICO's tilsyn og de tilgængelige klagemekanismer. Ud over de garantier, der er fastsat i DPA 2018, indeholder IPA 2016 desuden i visse tilfælde også bestemmelser om IPCO's *efterfølgende* tilsyn. ([307])

(194) Når der gennemføres en aflytning, gælder der yderligere begrænsninger og garantier i lyset af den specifikke status for den eller de personer, hvis kommunikation skal aflyttes ([308]). Opsnapning af materiale, der er omfattet af retten til fortrolighed mellem advokat og klient, er eksempelvis kun tilladt under ekstraordinære og tvingende omstændigheder, og den person, der udsteder kendelsen, skal tage hensyn til offentlighedens interesse i fortroligheden af materiale, der er omfattet af retten til fortrolighed mellem advokat og klient, og sikre, at der er fastsat særlige krav til håndtering, opbevaring og videregivelse af sådant materiale ([309]).

(195) Desuden indeholder IPA 2016 specifikke garantier vedrørende sikkerhed, opbevaring og videregivelse, som Secretary of State bør tage hensyn til, inden han udsteder en målrettet kendelse ([310]). Navnlig kræver Section 53(5) i IPA 2016, at alle eksemplarer, der er fremstillet af alt dette materiale, der er indsamlet i henhold til kendelsen, skal opbevares sikkert og destrueres, så snart der ikke længere foreligger nogen relevante grunde til at beholde det, mens Section 53(2) i IPA 2016 kræver, at antallet af personer, som materialet videregives til, og omfanget i hvilket materiale videregives, stilles til rådighed eller kopieres, begrænses til det minimum, der er nødvendigt af hensyn til de lovbestemte formål.

(196) Endelig fastsættes det i IPA 2016, at når det materiale, der er blevet opsnappet enten ved en kendelse om målrettet aflytning eller en kendelse om gensidig bistand, skal udleveres til et tredjeland (»oversøiske oplysninger«), fastsætter IPA, at Secretary of State skal sikre, at der er truffet passende foranstaltninger til at sikre, at der findes lignende garantier for sikkerhed, opbevaring og videregivelse i det pågældende tredjeland ([311]). I henhold til Section 109(2) i DPA 2018 må efterretningstjenesterne endvidere kun overføre personoplysninger til et territorium uden for Det Forenede Kongerige, hvis denne overførsel er nødvendig og står i et rimeligt forhold til formålet med den dataansvarliges lovbestemte funktioner eller til andre formål, der er fastsat i Section 2(2)(a) i Security Service Act 1989 eller Section 2(2)(a) og Section 4(2)(a) i Intelligence Services Act 1994 ([312]). Det er vigtigt at bemærke, at disse krav også gælder i tilfælde, hvor den nationale sikkerhedsundtagelse i henhold til Section 110 i DPA 2018 påberåbes, da Section 110 i DPA 2018 ikke opregner Section 109 i DPA 2018 som en af de bestemmelser, der kan fraviges, hvis en undtagelse fra visse bestemmelser er nødvendig for at beskytte den nationale sikkerhed.

3.3.1.1.2. Målrettet indsamling og opbevaring af kommunikationsdata

(197) IPA 2016 giver Secretary of State mulighed for at kræve, at teleoperatører opbevarer kommunikationsdata med henblik på målrettet adgang for en række offentlige myndigheder, herunder retshåndhævende myndigheder og efterretningstjenester. Part 4 i IPA 2016 indeholder bestemmelser om opbevaring af kommunikationsdata, mens Part 3 omhandler målrettet indsamling af kommunikationsdata. Part 3 og Part 4 i IPA 2016 fastsætter også specifikke begrænsninger for udøvelsen af disse beføjelser og fastsætter specifikke sikkerhedsforanstaltninger.

([307]) Se Section 229(4) i IPA som modstykke hertil.

([308]) I Section 26- 29 i IPA 2016 er der indført begrænsninger med hensyn til at opnå kendelser om målrettet aflytning og undersøgelse i forbindelse med aflytning af kommunikation, der sendes af eller er rettet til en person, der er medlem af parlamentet (alle parlamenter i Det Forenede Kongerige), opsnapning af materiale, der er omfattet af retten til fortrolighed mellem advokat og klient, aflytning af kommunikation, som efter den aflyttende myndigheds mening vil være kommunikation, der indeholder fortroligt journalistisk materiale, og når formålet med kendelsen er at identificere eller bekræfte en kilde til journalistisk information.

([309]) Section 26 i IPA 2016.

([310]) Section 19(1) i IPA 2016.

([311]) Section 54 i IPA 2016. Garantier vedrørende videregivelse af materiale til udenlandske myndigheder præciseres yderligere i adfærdskodekserne: Se navnlig paragraph 9.26 ff. og 9.87 i Code of Practice on the Interception of Communications (adfærdskodeksen om aflytning af kommunikation) og paragraph 9.33 ff. og 9.41 i Code of Practice on Equipment Interference (adfærdskodeksen for udstyrsinterferens) (jf. fodnote 278).

([312]) Disse formål er: for Security Service forebyggelse eller afsløring af grov kriminalitet eller straffesager (Section 2(2)(a) i Security Service Act 1989), for Intelligence Service hensynet til den nationale sikkerhed, forebyggelse eller afsløring af grov kriminalitet eller straffesager (Section 2(2)(a), i Intelligence Services Act 1994) og for GCHQ alle straffesager (Section 4(2)(a) i Intelligence Services Act 1994). Se også forklarende bemærkninger til DPA 2018, som findes på følgende link: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Udtrykket »kommunikationsdata« dækker »hvem«, »hvornår«, »hvor« og »hvordan« for kommunikation, men ikke indholdet, dvs. hvad der blev sagt eller skrevet. I modsætning til aflytning har indsamling og opbevaring af kommunikationsdata ikke til formål at få adgang til indholdet af kommunikationen, men derimod at indsamle oplysninger såsom abonnenten på en telefonitjeneste eller en udspecificeret regning. Dette kan omfatte tidspunkt og varighed af kommunikationen, afsenderens og modtagerens nummer eller e-mailadresse og undertiden placeringen af det udstyr, hvorfra telekommunikationen fandt sted ([313]).

(199) Det bør bemærkes, at opbevaring og indsamling af kommunikationsdata normalt ikke vedrører personoplysninger om registrerede i EU, der overføres til Det Forenede Kongerige i henhold til denne afgørelse. Forpligtelsen til at opbevare eller videregive kommunikationsdata i henhold til Part 3 og 4 i IPA 2016 omfatter data, der indsamles af teleoperatører i Det Forenede Kongerige direkte fra brugerne af en telekommunikationstjeneste ([314]). Denne type »kundeorienterede« behandling indebærer typisk ikke en overførsel på grundlag af denne afgørelse, dvs. en overførsel fra en dataansvarlig/databehandler i EU til en dataansvarlig/databehandler i Det Forenede Kongerige.

(200) For fuldstændighedens skyld analyseres betingelserne og garantierne for disse ordninger for indsamling og opbevaring i nedenstående betragtninger.

(201) Det er en forudsætning, at både nationale sikkerhedsagenturer og visse retshåndhævende myndigheder har adgang til opbevaring og målrettet indsamling af kommunikationsdata ([315]). Betingelserne for at kræve opbevaring og/eller indsamling af kommunikationsdata kan variere afhængigt af grunden til at anmode om foranstaltningen, især af hensyn til den nationale sikkerhed eller til et retshåndhævelsesformål.

(202) Selv om den nye ordning har indført det generelle krav om *forudgående* tilladelse fra et uafhængigt organ, som vil finde anvendelse i alle tilfælde, hvor kommunikationsdata opbevares og/eller indsamles (enten til retshåndhævelsesformål eller til af hensyn til den nationale sikkerhed), er der efter EU-Domstolens dom *Tele2/Watson* ([316]) blevet indført særlige garantier, når der anmodes om en foranstaltning med henblik på retshåndhævelse. Når der anmodes om opbevaring eller indsamling af kommunikationsdata med henblik på retshåndhævelse, skal *forhånds*godgodkendelsen altid gives af Investigatory Power Commissioner. Dette er ikke altid tilfældet, når der anmodes om en foranstaltning af hensyn til den nationale sikkerhed, da denne type foranstaltninger som beskrevet nedenfor i visse tilfælde kan godkendes af en anden »person, der giver tilladelse«. Desuden har den nye ordning hævet tærsklen for, hvornår opbevaring og indsamling af kommunikationsdata kan tillades, til »alvorlige forbrydelser« ([317]).

([313]) Kommunikationsdata er defineret i Section 261(5) i IPA 2016. Kommunikationsdata opdeles i »hændelsesdata« (alle data, der identificerer eller beskriver en hændelse, enten ved henvisning til dens placering, i eller ved hjælp af et telekommunikationssystem, hvor hændelsen består af en eller flere enheder, der udøver en specifik aktivitet på et bestemt tidspunkt) og »enhedsdata« (alle data, som a) vedrører i) en enhed, ii) en forbindelse mellem en telekommunikationstjeneste og en enhed eller iii) en forbindelse mellem en hvilken som helst del af et telekommunikationssystem og en enhed, b) som består af eller omfatter data, der identificerer eller beskriver enheden (uanset om det sker med henvisning til enhedens placering eller ej), og c) der ikke er hændelsesdata).

([314]) Dette følger af definitionen af kommunikationsdata i Section 261, stk. 5, i IPA 2016, ifølge hvilken kommunikationsdata opbevares eller indsamles af en teleoperatør og enten vedrører brugeren af en telekommunikationstjeneste og leveringen af denne tjeneste, eller er omfattet af, en del af, vedføjet eller logisk forbundet med kommunikation (se også Code of Practice on Communications Data, der findes på følgende link https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, paragraph 2.22 til 2.33). Desuden kræver definitionen af teleoperatør i Section 261(10) i IPA 2016, at en teleoperatør er en person, der tilbyder eller leverer en teletjeneste til personer i Det Forenede Kongerige, eller som kontrollerer eller leverer et telekommunikationssystem, som (helt eller delvist) er etableret i eller kontrolleres af Det Forenede Kongerige. Disse definitioner gør det klart, at forpligtelser i henhold til IPA 2016 ikke kan pålægges teleoperatører, hvis udstyr ikke befinder sig i eller kontrolleres af Det Forenede Kongerige, og som ikke tilbyder eller leverer tjenester til personer i Det Forenede Kongerige (se også Code of Practice on Communications Data, paragraph 2.1). Hvis EU-abonnenter (uanset om de er etableret i EU eller i Det Forenede Kongerige) har gjort brug af tjenester i Det Forenede Kongerige, vil enhver kommunikation i forbindelse med leveringen af denne tjeneste blive indsamlet direkte af tjenesteudbyderen i Det Forenede Kongerige i stedet for at blive overført fra EU.

([315]) De relevante myndigheder er anført i bilag 4 til IPA 2016, og de omfatter politi, efterretningstjenester, visse ministerier og departementer, National Crime Agency (det nationale kriminalitetsagentur), Her Majesty's Revenue and Customs (told- og skattevæsenet), Competition and Markets Authority (konkurrence- og markedsmyndigheden), Information Commissioner, ambulance-, brand- og redningstjenester samt myndigheder inden for sundhed og fødevaresikkerhed.

([316]) Forenede sager C-203/15 og C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).

([317]) Se Section 61.7(b) vedrørende indsamling af kommunikationsdata og Section 87.10A vedrørende opbevaring af kommunikationsdata.

i) *Tilladelse til at indsamle kommunikationsdata*

(203) I henhold til Part 3 i IPA 2016 er relevante offentlige myndigheder bemyndiget til at indsamle kommunikationsdata fra en teleoperatør eller enhver person, der er i stand til at indsamle og videregive sådanne data. Tilladelsen må ikke tillade aflytning af kommunikationens indhold ([318]) og ophører med at have virkning efter en periode på en måned ([319]) med mulighed for forlængelse efter en yderligere tilladelse ([320]). Indsamling af kommunikationsdata kræver tilladelse fra Investigatory Powers Commissioner (kommissær for efterforskningsbeføjelser, IPC) ([321]) (om IPC's status og beføjelser, se betragtning 250 til 251 nedenfor). Dette er altid tilfældet, hvor en relevant retshåndhævende myndighed anmoder om indsamling af kommunikationsdata. I henhold til Section 61 i IPA 2016 fastsættes det imidlertid, at når der indsamles data til Det Forenede Kongeriges nationale sikkerhed eller økonomiske velfærd, så længe det er relevant for den nationale sikkerhed, eller hvis en ansøgning indgives af et medlem af en efterretningstjeneste i henhold til Section 61(7)(b) ([322]), kan indsamlingen alternativt ([323]) godkendes af IPC eller af en udpeget overordnet embedsmand ([324]). Den udpegede embedsmand skal være uafhængig af den pågældende efterforskning og have praktisk kendskab til menneskerettighedsprincipper og -lovgivning, navnlig principperne om nødvendighed og proportionalitet ([325]). Den afgørelse, der træffes af den udpegede embedsmand, vil være underlagt den efterfølgende kontrol, der udøves af IPC (se betragtning 254 nedenfor for yderligere oplysninger om IPC's efterfølgende kontrolfunktioner).

(204) Tilladelsen til at indsamle kommunikationsdata er baseret på en vurdering af foranstaltningens nødvendighed og proportionalitet. Nærmere bestemt vurderes nødvendigheden af foranstaltningen i lyset af de grunde, der er anført i lovgivningen ([326]). I betragtning af denne foranstaltnings målrettede karakter skal den også være nødvendig for en specifik undersøgelse eller foranstaltning ([327]). Yderligere krav til vurderingen af, om foranstaltningerne er nødvendige, er fastsat i Code of Practice on Communications Data ([328]). Det fastsættes navnlig i denne kodeks, at den bistandssøgende myndighed i sin anmodning skal identificere mindst tre elementer for at begrunde nødvendigheden af en sådan anmodning: i) den hændelse, der efterforskes, såsom en forbrydelse eller lokalisering af en sårbar forsvundet person, ii) den person, hvis oplysninger der ønskes adgang til, såsom en mistænkt, et vidne eller en forsvundet person, og hvordan de er knyttet til hændelsen, og iii) de kommunikationsdata, der anmodes om, såsom telefonnummer eller IP-adresse, og hvordan disse data er relateret til personen og hændelsen ([329]).

(205) Desuden skal indsamlingen af kommunikationsdata stå i et rimeligt forhold til, hvad der søges opnået ([330]). I Code of Practice on Communications Data præciseres det, at den godkendende fysiske person i forbindelse med en sådan vurdering bør foretage en afvejning mellem »omfanget af indgrebet i en persons rettigheder og frihedsrettigheder i forhold til en specifik fordel for den undersøgelse eller operation, der gennemføres af en relevant offentlig myndighed i offentlighedens interesse«, og at et indgreb i en persons rettigheder under hensyntagen til alle

([318]) Section 60A(6) i IPA 2016.

([319]) Denne frist nedsættes til tre dage, når tilladelsen gives på grund af sagens hastende karakter (Section 65(3)A i IPA 2016).

([320]) I henhold til Section 65 i IPA 2016 gælder den fornyede tilladelse for en periode på en måned fra den dato, hvor den nuværende tilladelse udløber. Den person, der har givet tilladelsen, kan når som helst tilbagekalde den, hvis vedkommende mener, at kravene ikke længere er opfyldt.

([321]) Section 60A(1) i IPA 2016. Office for Communications Data Authorisations (OCDA) varetager denne funktion på vegne af IPC (jf. Communication Data Codes of Practice (adfærdskodekser for kommunikationsdata), para. 5.6).

([322]) Ansøgningen efter Section 61(7)(b) i IPA 2016 er indgivet med henblik på »et relevant kriminalitetsbekæmpelsesformål«, jf. Section 61(7)A i IPA 2016: »hvis kommunikationsdataene helt eller delvist er hændelsesdata; formålet med dem er at forebygge eller afsløre grov kriminalitet, i alle andre tilfælde; formålet er at forebygge eller afsløre kriminalitet eller at forebygge uro«.

([323]) I Code of Practice on Communication Data hedder det: »Hvis en ansøgning vedrørende den nationale sikkerhed kan indgives i henhold til enten Section 60A eller Section 61, er det op til de enkelte offentlige myndigheder at afgøre, hvilken tilladelsesprocedure der er mest hensigtsmæssig i en given sag. Offentlige myndigheder, der ønsker at benytte proceduren med den udpegede ledende embedsmand, bør have klare retningslinjer for, hvornår denne tilladelsesprocedure er hensigtsmæssig« (Code of Practice on Communication Data, paragraph 5. 19, der findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) Section 70(3) i IPA 2016 indeholder definitionen af en »udpeget embedsmand«, som varierer afhængigt af den relevante offentlige myndighed (som fastsat i Schedule 4 til IPA 2016).

([325]) Yderligere oplysninger om den udpegede ledende embedsmands uafhængighed findes i Communication Data Code of practice (Code of Practice on Communications Data, paragraph 4.12-4.17, jf. fodnote 323).

([326]) Begrundelsen er: i) den nationale sikkerhed, ii) forebyggelse eller afsløring af kriminalitet eller forebyggelse af uro (i tilfælde af »hændelsesdata« kun alvorlig kriminalitet), iii) hensynet til Det Forenede Kongeriges økonomiske velfærd, for så vidt som disse interesser også er relevante for den nationale sikkerhed, iv) hensynet til den offentlige sikkerhed, v) at forebygge død eller tilskadekomst eller skade på en persons fysiske eller mentale sundhed eller at afbøde enhver form for personskade eller skade på en persons fysiske eller mentale sundhed, vi) at bistå med efterforskningen af påståede rettergangsfejl eller vii) at identificere en afdød person eller en person, der ikke er i stand til at identificere sig på grund af en særlig omstændighed (Section 61(7) i IPA 2016).

([327]) Section 60A(1)(b) i IPA 2016.

([328]) Code of Practice on Communications Data, paragraph 3.3 ff., jf. fodnote 323.

([329]) Code of Practice on Communications Data, paragraph 3.13, jf. fodnote 323.

([330]) Section 60(1)(c) i IPA 2016.

overvejelser i et konkret tilfælde stadig ikke nødvendigvis er berettiget, fordi den negative indvirkning på en anden enkeltpersons eller gruppe af personers rettigheder er for alvorlig. For specifikt at vurdere foranstaltningens proportionalitet opregner kodeksen desuden en række elementer, der bør indgå i den anmodning, der indgives af den bistandssøgende myndighed ([331]). Desuden skal der tages særligt hensyn til, hvilken type kommunikationsdata (»enhedsdata« eller »hændelsesdata« ([332])) der skal indsamles, og der skal fortrinsvis benyttes mindre indgribende datakategorier ([333]). Code of Practice on Communications Data indeholder også specifikke instrukser for tilladelser, der omfatter kommunikationsdata om personer i bestemte erhverv (f.eks. læger, advokater, journalister, parlamentarikere eller præster) ([334]), som er underlagt yderligere sikkerhedsforanstaltninger ([335]).

ii) *Meddelelse om krav om opbevaring af kommunikationsdata*

(206) Part 4 i IPA 2016 fastsætter reglerne for opbevaring af kommunikationsdata og navnlig de kriterier, der giver Secretary of State mulighed for at udstede en »retention notice« (opbevaringsmeddelelse) ([336]). De garantier, der indføres med IPA, gælder både, når dataene opbevares med henblik på retshåndhævelse og af hensyn til den nationale sikkerhed.

(207) Udstedelsen af sådanne retention notices har til formål at sikre, at teleoperatører i en periode på højst 12 måneder opbevarer relevante kommunikationsdata, som ellers ville blive slettet, når de ikke længere er nødvendige til erhvervsmæssige formål ([337]). De opbevarede data skal forblive tilgængelige i den krævede periode, hvis det efterfølgende bliver nødvendigt for en offentlig myndighed at indsamle dem i henhold til en tilladelse til målrettet indsamling af kommunikationsdata ifølge Part 3 i IPA 2016 og som beskrevet i betragtning 203 til 205.

(208) Udøvelsen af beføjelsen til at kræve opbevaring af visse oplysninger er underlagt en række begrænsninger og garantier. Secretary of State kan kun udstede en retention notice til en eller flere operatører ([338]), hvis han mener, at kravet om opbevaring af oplysningerne er nødvendigt af hensyn til en af de lovbestemte formål ([339]), og det står i rimeligt forhold til det, der søges opnået ([340]). Som

([331]) Disse oplysninger skal omfatte: i) en oversigt over, hvordan indsamling af data vil gavne efterforskningen eller operationen, ii) en redegørelse for relevansen af de ønskede tidsrum, herunder hvordan disse tidsrum står i forhold til den hændelse, der undersøges, iii) en forklaring af, hvorfor indgrebets omfang er berettiget, når der tages hensyn til den fordel, som dataene vil medføre for efterforskningen (denne begrundelse bør omfatte overvejelser om, hvorvidt mindre indgribende efterforskninger kan gennemføres for at nå målet), iv) hensyntagen til individets rettigheder (navnlig til privatlivets fred og i relevante tilfælde ytringsfrihed) og en afvejning af disse rettigheder i forhold til fordelene for efterforskningen, v) nærmere oplysninger om, hvilke tilhørende indgreb der kan forekomme, og hvordan de ønskede tidsrum indvirker på de tilhørende indgreb (Code of Practice on Communications Data, paragraph 3.22- 3.26, jf. fodnote 323).

([332]) Jf. fodnote 313.

([333]) Når der ønskes mere indgribende kommunikationsdata (dvs. hændelsesdata), præciseres det i kodeksen, at det er mere hensigtsmæssigt at indsamle førstegangsdata eller at indsamle direkte hændelsesdata i begrænsede hastetilfælde (Code of Practice on Communications Data, paragraph 6.10-6.14, jf. fodnote 323).

([334]) Code of Practice on Communications Data, paragraph 8.8-8.44, jf. fodnote 323.

([335]) I adfærdskodeksen præciseres det, at »en person, der giver tilladelse, skal udvise særlig omhu ved behandlingen af sådanne anmodninger, herunder yderligere overvejelser om, hvorvidt der kan være utilsigtede konsekvenser af sådanne anmodninger, og om almenhedens interesse bedst tilgodeses ved anmodningen« (Code of Practice on Communications Data, paragraph 8.8). Desuden skal der føres fortegnelser over denne type anmodninger, og ved næste inspektion skal sådanne anmodninger markeres for at gøre IPC opmærksom på dem (Code of Practice on Communications Data, paragraph 8.10, jf. fodnote 323).

([336]) Section 87 til 89 i IPA 2016.

([337]) I henhold til Section 90 i IPA 2016 kan en teleoperatør, der modtager en retention notice, anmode den Secretary of State, der har udstedt den, om en fornyet gennemgang.

([338]) I henhold til Section 87(2)(a) i IPA 2016 kan en opbevaringsmeddelelse vedrøre »en bestemt operatør eller en beskrivelse af operatører«.

([339]) Formålene er i) hensynet til den nationale sikkerhed, ii) det relevante kriminalitetsbekæmpelsesformål (som defineret i Section 87.10A i IPA 2016), iii) hensynet til Det Forenede Kongeriges økonomiske velfærd, for så vidt som dette hensyn også er relevant for den nationale sikkerhed, iv) hensynet til den offentlige sikkerhed, v) at forebygge død eller tilskadekomst eller skade på en persons fysiske eller mentale sundhed eller at afbøde enhver form for personskade eller skade på en persons fysiske eller mentale sundhed eller vi) at bistå med efterforskningen af påståede rettergangsfejl (Section 87 i IPA).

([340]) Section 87 i IPA 2016. I henhold til den relevante adfærdskodeks finder kriterierne i Section 2(2) i IPA 2016 desuden anvendelse med henblik på at vurdere proportionaliteten af den pågældende retention notice, navnlig kravet om at vurdere, om det, der søges opnået med den pågældende retention notice, med rimelighed kan opnås ved hjælp af mindre indgribende midler. I lighed med vurderingen af proportionaliteten i forbindelse med indsamling af kommunikationsdata præciseres det i Code of Practice on Communications Data, at en sådan vurdering indebærer en »afvejning mellem omfanget af indgrebet i en persons ret til respekt for privatliv og en specifik fordel for undersøgelsen« (Code of Practice on Communications Data, paragraph 16.3, jf. fodnote 323).

præciseret i selve IPA 2016 ([341]) skal Secretary of State inden udstedelsen af en retention notice tage hensyn til: de sandsynlige fordele ved den pågældende retention notice ([342]), en beskrivelse af telekommunikationstjenesterne, det hensigtsmæssige ved at begrænse de data, der skal opbevares, under henvisning til placering eller beskrivelser af de personer, som telekommunikationstjenesterne leveres til ([343]), det sandsynlige antal brugere (hvis kendt) af de teletjenester, som den pågældende retention notice vedrører ([344]), den tekniske gennemførlighed af at efterkomme den pågældende retention notice, de sandsynlige omkostninger ved at efterkomme den pågældende retention notice og eventuelle andre virkninger af meddelelsen for den teleoperatør (eller beskrivelse af operatører), som den vedrører ([345]). Som nærmere beskrevet i Chapter 17 i Code of Practice on Communications Data skal alle retention notices angive hver enkelt datatype, der skal opbevares, og hvordan denne datatype opfylder de nødvendige krav for opbevaring.

(209) I alle tilfælde (både af hensyn til den nationale sikkerhed og retshåndhævelse) skal Secretary of States afgørelse om at udstede opbevaringsmeddelelsen godkendes af en uafhængig Judicial Commissioner i henhold til den såkaldte »double-lock-procedure«, som navnlig skal kontrollere, om meddelelsen om opbevaring af relevante kommunikationsdata er nødvendig og står i rimeligt forhold til et eller flere af de lovbestemte formål ([346]).

3.3.1.1.3. Indgreb i udstyr

(210) Indgreb i udstyr er en række teknikker, der anvendes til at indsamle en række data fra udstyr ([347]), herunder computere, tablets og smartphones samt kabler, ledninger og lagringsenheder ([348]). Indgreb i udstyr gør det muligt at indsamle både indholdet af kommunikation og udstyrsdata ([349]).

(211) I overensstemmelse med Section 13, stk. 1, i IPA 2016 kræver en efterretningstjenestes brug af udstyr en tilladelse i form af en kendelse i henhold til »double-lock-proceduren«, der er fastsat i IPA 2016, forudsat at der er en »forbindelse til De Britiske Øer« ([350]). Ifølge Det Forenede Kongeriges myndigheders forklaringer vil der i situationer, hvor data overføres fra Den Europæiske Union til Det Forenede Kongerige inden for rammerne af denne afgørelse,

([341]) Se Section 88 i IPA 2016.

([342]) Fordelene kan være eksisterende eller planlagte og skal være i overensstemmelse med de lovmæssige formål, hvortil dataene kan opbevares (Code of Practice on Communications Data, paragraph 17.17, jf. fodnote 323).

([343]) Disse overvejelser vil omfatte en vurdering af, om den fulde geografiske rækkevidde af den pågældende retention notice er nødvendig og forholdsmæssig, og om det er nødvendigt og forholdsmæssigt at medtage eller udelukke særlige beskrivelser af personer (Code of Practice on Communications Data, paragraph 17.17, jf. fodnote 323).

([344]) Dette vil hjælpe Secretary of State med at overveje både graden af indgriben over for kunderne, men også de sandsynlige fordele ved de data, der skal opbevares (Code of Practice on Communications Data, paragraph 17.17, jf. fodnote 323).

([345]) Section 88 i IPA 2016.

([346]) Section 89 i IPA 2016.

([347]) I henhold til Section 135(1) og 198(1) i IPA 2016 dækker »udstyr« over udstyr, der frembringer elektromagnetiske, akustiske eller andre emissioner, og enhver anordning, der kan anvendes i forbindelse med sådant udstyr.

([348]) Code of Practice on Equipment Interference (adfærdskodeks for indgreb i udstyr), som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, paragraph 2.2.

([349]) Udstyrsdata defineres i Section 100 i IPA 2016 som systemdata og data, som a) indgår i, er en del af, er knyttet til eller logisk forbundet med kommunikation (af afsenderen eller på anden måde) eller enhver anden oplysning, b) logisk kan adskilles fra den resterende del af meddelelsen eller oplysningerne, og c) hvis en sådan adskillelse foretages, ikke afslører noget af, hvad der med rimelighed kan anses for at være betydningen (om nogen) af meddelelsen eller informationen.

([350]) For at kravet om retskendelse skal være obligatorisk, kræves det i Section 13, stk. 1, i IPA 2016 ligeledes, at efterretningstjenestens handlinger udgør en eller flere overtrædelser i henhold til Section 1-3A i Computer Misuse Act 1990 (lov om misbrug af computere), hvilket vil være tilfældet under langt de fleste omstændigheder, se Code of Practice on Equipment Interference, paragraph 3.32 og 3.6-3.9). I henhold til Section 13(2) i IPA 2016 er der en »forbindelse til De Britiske Øer«, hvis a) en hvilken som helst del af handlingerne finder sted på De Britiske Øer (uanset hvor udstyret, som ville eller kan blive berørt af indgrebet, befinder sig), b) efterretningstjenesten mener, at alt udstyr, som ville eller kan blive berørt af indgrebet, ville eller kan befinde sig på De Britiske Øer på et tidspunkt, hvor indgrebet finder sted, eller c) et af formålene med indgrebet er at indsamle i) kommunikation, der sendes af eller til en person, som befinder sig, eller som efterretningstjenesten mener befinder sig, på De Britiske Øer, ii) private oplysninger vedrørende en person, som befinder sig, eller som efterretningstjenesten mener befinder sig, på De Britiske Øer, eller iii) udstyrsdata, som udgør en del af eller har forbindelse med kommunikation eller private oplysninger, der hører under afsnit i) eller ii).

altid være en »forbindelse til De Britiske Øer«, og ethvert indgreb i udstyr, der omfatter sådanne data, vil derfor være underlagt det obligatoriske krav om en retskendelse i Section 13, stk. 1, i IPA 2016 ([351]).

(212) Reglerne for kendelser om målrettede indgreb i udstyr er fastsat i Part 5 i IPA 2016. Ligesom målrettet aflytning skal målrettede indgreb i udstyr vedrøre et specifikt »mål«, som skal angives i kendelsen ([352]). Detaljerne for, hvordan et »mål« skal identificeres, afhænger af emnet og typen af udstyr, der skal aflyttes. Navnlig Section 115(3) i IPA specificerer de elementer, der skal fremgå af kendelsen (f.eks. personens eller organisationens navn, en beskrivelse af stedet), f.eks. afhængigt af om indgrebet vedrører udstyr, der tilhører eller anvendes til en bestemt person eller en organisation eller en gruppe af personer eller er i disses besiddelse, befinder sig på et bestemt sted osv. ([353]). Det er den offentlige myndighed, der anmoder om en kendelse, der afgør, til hvilke formål det er berettiget at foretage indgreb i det pågældende udstyr ([354]).

(213) I lighed med målrettet aflytning skal udstedelsesmyndigheden overveje, om foranstaltningen er nødvendig for at opnå et specifikt formål, og om den står i rimeligt forhold til det, der søges opnået ([355]). Desuden bør den også overveje, om der findes beskyttelsesforanstaltninger i forbindelse med sikkerhed, opbevaring og videregivelse samt i forbindelse med »offentliggørelse i udlandet« ([356]) (se betragtning 196).

(214) Kendelsen skal godkendes af en Judicial Commissioner, undtagen i hastetilfælde ([357]). I sidstnævnte tilfælde skal en Judicial Commissioner underrettes om, at der er udstedt en kendelse, og godkende den inden for tre hverdage. Hvis Judicial Commissioner nægter at godkende kendelsen, mister den sin virkning og kan ikke forlænges ([358]). Desuden har Judicial Commissioner beføjelse til at kræve, at alle oplysninger, der er indhentet i henhold til kendelsen, slettes ([359]). Det forhold, at en kendelse blev udstedt som en hastesag, påvirker ikke det *efterfølgende* tilsyn (se betragtning 244 til 255) eller enkeltpersoners muligheder for at klage (se betragtning 260 til 270). Enkeltpersoner kan klage til ICO eller fremsætte krav om påstået adfærd over for Investigatory Powers Tribunal på sædvanlig vis. I alle tilfælde skal den prøve, som Judicial Commissioner gennemfører, når det skal besluttes, hvorvidt en kendelse kan godkendes eller ej, være den nødvendigheds- og proportionalitetstest, som også finder anvendelse på anmodninger om målrettet aflytning ([360]) (se betragtning 192 ovenfor).

([351]) For fuldstændighedens skyld skal det bemærkes, at selv i situationer, hvor der ikke er nogen »forbindelse til De Britiske Øer«, og indgrebet i udstyret derfor ikke er omfattet af det obligatoriske krav om retskendelse i Section 13(1) i IPA 2016, bør en efterretningstjeneste, der planlægger at deltage i aktiviteter, for hvilke den kan indhente en kendelse om masseindgreb i udstyr, indhente en sådan retskendelse af politiske årsager (jf. Code of Practice on Equipment Interference, paragraph 3.24). Selv i de tilfælde, hvor en kendelse til indgreb i udstyr i henhold til IPA 2016 hverken er retligt påkrævet eller begrundet i politiske hensyn, er efterretningstjenesternes handlinger underlagt en række betingelser og begrænsninger i henhold til Section 7 i Intelligence Services Act 1994. Dette omfatter navnlig kravet om tilladelse fra Secretary of State, som skal være overbevist om, at enhver handling ikke går ud over, hvad der er nødvendigt for, at efterretningstjenesten kan udføre sine opgaver korrekt.

([352]) Section 115 i IPA 2016 regulerer indholdet af kendelsen og præciserer, at den skal indeholde navnet på eller en beskrivelse af de personer, de organisationer, det sted eller den gruppe af personer, der udgør »målet«, en beskrivelse af efterforskningens art og en beskrivelse af de aktiviteter, som udstyret anvendes til. Den skal også indeholde en beskrivelse af udstyrets art og de handlinger, som den person, kendelsen er rettet til, er bemyndiget til at foretage.

([353]) Se også Code of Practice on Equipment Interference, paragraph 5.7, jf. fodnote 348.

([354]) Nationale sikkerhedsagenturer kan anmode om en kendelse til indgreb i udstyr, når det er nødvendigt af hensyn til den nationale sikkerhed, med henblik på at afsløre alvorlig kriminalitet og/eller af hensyn til Det Forenede Kongeriges økonomi, for så vidt disse interesser også er relevante for den nationale sikkerhed (Section 102-103 i IPA 2016). Afhængig af agenturet kan der anmodes om en kendelse til indgreb i udstyr med henblik på retshåndhævelse, når det er nødvendigt for at afsløre eller forebygge grov kriminalitet eller for at forebygge død eller tilskadekomst eller skade på en persons fysiske eller mentale sundhed eller at afbøde enhver form for personskade eller skade på en persons fysiske eller mentale sundhed (se Section 106(1) og 106(3) i IPA 2016).

([355]) Section 102(1) i IPA 2016.

([356]) Section 129-131 i IPA 2016.

([357]) Section 109 i IPA 2016.

([358]) Section 109(4) i IPA 2016.

([359]) Section 110(3)(b) i IPA 2016. I henhold til Code of Practice on Equipment Interference, paragraph 5.67, afgøres karakteren af hastesag af, om det med rimelighed er praktisk muligt at anmode om Judicial Commissioners godkendelse til at udstede kendelsen inden for den tid, der er til rådighed til at opfylde et operationelt eller efterforskningsmæssigt behov. Hastekendelser bør falde ind under en eller begge af følgende kategorier: i) overhængende fare for liv eller alvorlig overlast — f.eks. hvis en person er blevet kidnappet, og det vurderes, at deres liv er i overhængende fare eller ii) en efterretningsrelateret indsamling eller efterforskningsmulighed med begrænset tid — f.eks. er en sending af stoffer i klasse A ved at komme ind i Det Forenede Kongerige, og retshåndhævende myndigheder ønsker at have dækket gerningsmændene til grov kriminalitet for at foretage anholdelser. Jf. fodnote 348.

([360]) Section 108 i IPA 2016.

(215) Endelig finder de specifikke garantier, der gælder for målrettet aflytning, også anvendelse på indgreb i udstyr for så vidt angår varigheden, fornyelsen og ændringen af kendelsen samt aflytning af parlamentsmedlemmer, af oplysninger, der er omfattet af retten til fortrolighed mellem advokat og klient, og af journalistisk materiale (se nærmere oplysninger i betragtning 193).

3.3.1.1.4. Udøvelse af beføjelser vedrørende masseindsamling

(216) Beføjelser vedrørende masseindsamling er reguleret i Part 6 i IPA 2016. Desuden indeholder adfærdskodekserne flere detaljer om anvendelsen af beføjelser vedrørende masseindsamling. Selv om der i Det Forenede Kongeriges lovgivning ikke findes nogen definition af »beføjelser vedrørende masseindsamling«, er de i forbindelse med IPA 2016 blevet beskrevet som indsamling og opbevaring af store mængder data, som regeringen har indsamlet på forskellige måder (dvs. beføjelser til masseaflytning, masseindsamling, masseindgreb og massepersonoplysninger), og som myndighederne efterfølgende kan få adgang til. Denne beskrivelse præciseres ved at stille den over for, hvad »beføjelser vedrørende masseindsamling« ikke er: Der er ikke tale om såkaldt »masseovervågning« uden begrænsninger eller sikkerhedsforanstaltninger. Som forklaret nedenfor indeholder de tværtimod begrænsninger og garantier, der har til formål at sikre, at der ikke gives adgang til oplysninger på et vilkårligt eller uberettiget grundlag ([361]). Navnlig kan beføjelser vedrørende masseindsamling kun anvendes, hvis der etableres en forbindelse mellem den tekniske foranstaltning, som en national efterretningstjeneste har til hensigt at anvende, og det operationelle mål, som der anmodes om en sådan foranstaltning til.

(217) Desuden har kun efterretningstjenesterne adgang til beføjelser til masseindsamling, og de er altid underlagt en kendelse, der er udstedt af Secretary of State og godkendt af en Judicial Commissioner. Ved valget af metoder til indsamling af efterretninger skal det undersøges, om det pågældende mål kan forfølges med »mindre indgribende midler« ([362]). Denne tilgang følger af rammerne for lovgivningen, som bygger på proportionalitetsprincippet og derfor prioriterer målrettet indsamling frem for masseindsamling.

3.3.1.1.4.1. Masseaflytning og masseindgreb i udstyr

(218) Ordningen for masseaflytning er fastsat i Chapter 1 i Part 6 i IPA 2016, mens Chapter 3 i samme Part regulerer masseindgreb i udstyr. Disse ordninger er stort set de samme, så de betingelser og yderligere garantier, der gælder for disse kendelser, analyseres samlet.

i) *Betingelser og kriterier for udstedelse af kendelsen*

(219) En masseaflytningskendelse er begrænset til aflytning af kommunikation under dens transmission, hvor den sendes eller modtages af personer uden for De Britiske Øer ([363]), såkaldt »oversøisk kommunikation« ([364]), samt andre relevante data og den efterfølgende udvælgelse med henblik på undersøgelse af det aflyttede

([361]) Ifølge rapporten om beføjelser til masseindsamling fra Lord David Anderson, som foretog en uafhængig gennemgang af terrorlovgivningen forud for godkendelsen af IPA 2016, »bør det være klart, at masseindsamling og -opbevaring ikke svarer til såkaldt »masseovervågning«. Ethvert retssystem med respekt for sig selv vil indeholde begrænsninger og garantier, der netop er udformet med henblik på at sikre, at adgang til lagre af følsomme oplysninger (...) ikke gives på et vilkårligt eller uberettiget grundlag. *Sådanne begrænsninger og garantier findes helt sikkert i lovforslaget*«, Lord David Anderson, Report of the bulk power review, august 2016, paragraph 1.9 (fremhævelse tilføjet), som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) Section 2,2 i IPA 2016. Se f.eks. Code of Practice on Bulk Acquisition of Communications Data (adfærdskodeksen for masseindsamling af kommunikationsdata), paragraph 4.11, som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

([363]) »De Britiske Øer« består af Det Forenede Kongerige, Kanaløerne og Isle of Man og er defineret i Schedule 1 til Interpretation Act 1978 (lov om fortolkning), som findes på følgende link: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) I henhold til Section 136 i IPA 2016 forstås ved »oversøisk kommunikation«: i) meddelelser, der sendes af personer uden for De Britiske Øer, eller ii) meddelelser, der modtages af personer uden for De Britiske Øer. Denne ordning omfatter, som bekræftet af de britiske myndigheder, også kommunikation mellem to personer, der begge befinder sig uden for De Britiske Øer. Den Europæiske Menneskerettighedsdomstols Store Afdeling i sagen Big Brother Watch m.fl. mod Det Forenede Kongerige (jf. fodnote 279 ovenfor), præmis 376, fastslog med hensyn til en tilsvarende begrænsning (med henvisning til »ekstern kommunikation«) af de meddelelser, der kan opfanges ved masseaflytning i henhold til RIPA 2000, at den var tilstrækkeligt afgrænset og forudsigelig.

materiale ([365]). En kendelse om masseindgreb i udstyr ([366]) giver adressaten tilladelse til at skaffe sig adgang til alt udstyr med henblik på at indsamle oversøisk kommunikation (herunder alt, der omfatter tale, musik, lyd, visuelle billeder eller data af en hvilken som helst art), udstyrsdata (data, der muliggør eller letter en posttjenestes, et telekommunikationssystems eller en telekommunikationstjenestes funktion) eller andre oplysninger ([367]).

(220) Secretary of State kan kun udstede en kendelse om masseindgreb efter anmodning fra lederen af en efterretningstjeneste ([368]). En kendelse, der tillader masseaflytning eller masseindgreb i udstyr, må kun udstedes, hvis det er nødvendigt af hensyn til den nationale sikkerhed og af hensyn til forebyggelsen eller afsløringen af grov kriminalitet eller af hensyn til Det Forenede Kongeriges økonomiske velfærd, når det er relevant for den nationale sikkerhed ([369]). Desuden kræves det i Section 142(7) i IPA 2016, at en kendelse om masseaflytning skal specificeres mere detaljeret end ved blot at henvise til »hensynet til den nationale sikkerhed«, »Det Forenede Kongeriges økonomiske velfærd« og »forebyggelse og bekæmpelse af grov kriminalitet«, og at der skal etableres en forbindelse mellem den foranstaltning, der søges om tilladelse til, og et eller flere operationelle formål, som skal indgå i kendelsen.

(221) Valget af det operationelle formål er resultatet af en proces i flere tempi. Section 142(4) bestemmer, at de operationelle formål, der er angivet i kendelsen, skal være angivet på en liste, der føres af cheferne for efterretningstjenesterne, som formål, de anser for at være operationelle formål, som gør det muligt at udvælge aflyttet indhold eller sekundære data, der er indsamlet i henhold til kendelser om masseaflytning, til undersøgelse. Listen over operationelle formål skal godkendes af Secretary of State. Secretary of State kan kun give en sådan godkendelse, hvis han eller hun finder det godtgjort, at det operationelle formål er mere detaljeret end de generelle grunde til at udstede kendelsen (statens sikkerhed eller statens sikkerhed og økonomiske velfærd eller forebyggelse af grov kriminalitet) ([370]). Ved udløbet af hver relevant periode på tre måneder skal Secretary of State udlevere en kopi af listen over operationelle formål til parlamentets ISC. Endelig skal premierministeren revidere listen over operationelle formål mindst én gang om året ([371]). Som High Court bemærkede, må »[d]isse ikke [...] tilsidesættes som ubetydelige garantier, da de tilsammen udgør et avanceret system af ansvarlighedsformer, som involverer både parlamentet og medlemmer af regeringen på højeste niveau« ([372]).

(222) Sådanne operationelle formål begrænser også omfanget af udvælgelsen af aflytningsmaterialet til undersøgelsesfasen. Udvælgelsen til undersøgelse af materiale, der indsamles i henhold til kendelsen om masseindsamling, skal begrundes i lyset af det/de operationelle formål. Som forklaret af Det Forenede Kongeriges myndigheder betyder dette, at Secretary of State skal vurdere de praktiske ordninger for undersøgelsen allerede på stadiet med kendelsen, idet den pågældende skal modtage tilstrækkelige oplysninger til at opfylde de lovbestemte forpligtelser i henhold til Section 152 og 193 i IPA 2016 ([373]). De oplysninger, der gives til Secretary of State i forbindelse med disse ordninger, skal f.eks. omfatte oplysninger (hvis det er relevant) om, hvordan filtreringsordningerne kan variere i den periode, hvor en kendelse har virkning ([374]). Yderligere oplysninger om processen og de sikkerhedsforanstaltninger, der anvendes i filtrerings- og undersøgelsesfaserne, findes i betragtning 229 nedenfor.

([365]) Section 136(4) i IPA 2016. Ifølge de forklaringer, der er modtaget fra den britiske regering, kan masseaflytning f.eks. anvendes til at identificere hidtil ukendte trusler mod den nationale sikkerhed i Det Forenede Kongerige ved at filtrere og analysere aflyttet materiale med henblik på at identificere kommunikation af efterretningsværdi (UK Explanatory Framework, section H: National Security, s. 27-28, jf. fodnote 29). Som forklaret af de britiske myndigheder kan sådanne instrumenter anvendes til at etablere forbindelse mellem kendte personer af interesse og til at søge efter spor efter aktiviteter udført af enkeltpersoner, som måske endnu ikke er kendte, men som dukker op i forbindelse med en efterforskning, og til at identificere aktivitetsmønstre, der kan tyde på en trussel mod Det Forenede Kongerige.

([366]) I overensstemmelse med Section 13, stk.1, i IPA 2016 kræver en efterretningstjenestes brug af udstyr en tilladelse i form af en kendelse i henhold til IPA 2016, forudsat at der er en »forbindelse til De Britiske Øer«, jf. betragtning 211.

([367]) Section 176 i IPA 2016. En kendelse til masseindgreb i udstyr kan ikke give tilladelse til handlinger, der (medmindre det sker med lovlig bemyndigelse) ville udgøre ulovlig aflytning (undtagen i forbindelse med opbevaret kommunikation). Ifølge UK Explanatory Framework kan de indsamlede oplysninger være nødvendige for at identificere interessante personer og vil normalt være hensigtsmæssige operationer i stor målestok (UK Explanatory Framework, section H: National Security, s. 28, se fodnote 29).

([368]) Section 138(1) og 178(1) i IPA 2016.

([369]) Section 138 (2) og 178(2) i IPA 2016.

([370]) Ifølge de britiske myndigheders forklaringer kan et operationelt formål f.eks. begrænse foranstaltningens anvendelsesområde til forekomsten af en trussel i et bestemt geografisk område.

([371]) Section 142(4)-(10) i IPA 2016.

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

([373]) I henhold til Section 152 og 193 i IPA 2016: a) skal udvælgelsen til undersøgelse foretages udelukkende med henblik på de operationelle formål, der er angivet i kendelsen, b) skal udvælgelsen til undersøgelse være nødvendig og forholdsmæssig under alle omstændigheder, og c) må udvælgelsen til undersøgelse ikke være i strid med forbuddet mod at udvælge materiale og identificere meddelelser, der er sendt af eller er beregnet til personer, som man ved opholder sig på De Britiske Øer på det pågældende tidspunkt.

([374]) Se Code of Practice on Interception of Communications, paragraph 6.6, jf. fodnote 278.

(223) En beføjelse til masseindsamling kan kun godkendes, hvis den står i et rimeligt forhold til det, der søges opnået ([375]). Som anført i Code of Practice on Interception of Communications indebærer enhver proportionalitetsvurdering »en afvejning af alvoren af krænkelsen af privatlivets fred (og andre hensyn, der er anført i Section 2(2)) i forhold til behovet for aktiviteten med hensyn til efterforskning, drift eller kapacitet. Den godkendte handling bør have en realistisk udsigt til at opnå den forventede fordel og bør ikke være uforholdsmæssig eller vilkårlig« ([376]). Som allerede nævnt betyder dette i praksis, at proportionalitetstesten er baseret på en afvejning mellem det, der søges opnået (»operationelle formål«), og de tilgængelige tekniske muligheder (f.eks. målrettet aflytning eller masseaflytning, indgreb i udstyr, indsamling af kommunikationsdata), idet de mindst indgribende midler foretrækkes (se betragtning 181 og 182 ovenfor). Hvis mere end én foranstaltning er hensigtsmæssig i forhold til målet, skal de mindst indgribende midler foretrækkes.

(224) En yderligere garanti for vurderingen af proportionaliteten af den foranstaltning, der anmodes om, ligger i, at Secretary of State skal modtage de relevante oplysninger, der er nødvendige for, at den pågældende kan foretage sin vurdering korrekt. Navnlig kræves det i Code of Practice on Interception of Communications og i Code of Practice on Equipment Interference, at anmodningen, der indgives af den relevante myndighed, skal indeholde baggrunden for anmodningen, en beskrivelse af den kommunikation, der skal aflyttes, og de teleoperatører, der skal bistå med aflytningen, en beskrivelse af de handlinger, der skal godkendes, de operationelle formål og en redegørelse for, hvorfor handlingerne er nødvendige og forholdsmæssige ([377]).

(225) Endelig er det vigtigt, at Secretary of States afgørelse om at udstede kendelsen skal godkendes af en uafhængig Judicial Commissioner, der vurderer, om den foreslåede foranstaltning er nødvendig og forholdsmæssig, med anvendelse af de samme principper, som en domstol ville anvende i forbindelse med en anmodning om domstolsprøvelse ([378]). Mere specifikt vil Judicial Commissioner gennemgå Secretary of States konklusioner om, hvorvidt kendelsen er nødvendig, og om handlingerne er forholdsmæssige i lyset af principperne i Section 2(2) i IPA 2016 (generelle forpligtelser vedrørende privatlivets fred). Judicial Commissioner vil også gennemgå Secretary of States konklusioner med hensyn til, om hvert af de operationelle formål, der er angivet i kendelsen, er et formål, som udvælgelsen er eller kan være nødvendig for. Hvis Judicial Commissioner nægter at godkende afgørelsen om at udstede en kendelse, kan Secretary of State enten: i) acceptere afgørelsen og derfor undlade at udstede kendelsen eller ii) henvise sagen til Investigatory Powers Commissioner med henblik på en afgørelse (medmindre Investigatory Powers Commissioner har truffet den oprindelige afgørelse) ([379]).

ii) *Yderligere beskyttelsesforanstaltninger*

(226) Med IPA 2016 er der indført yderligere begrænsninger af varigheden, fornyelsen og ændringen af en kendelse om masseindsamling. Kendelsen skal have en varighed på højst seks måneder, og enhver afgørelse om forlængelse eller ændring (bortset fra mindre ændringer) af kendelsen skal også godkendes af en Judicial Commissioner ([380]). I Code of Practice on Interception og Code of Practice on Equipment Interference præciseredes det, at en ændring af kendelsens operationelle formål betragtes som en større ændring af kendelsen ([381]).

([375]) Section 138(1)(b) og (c) og Section 178(b) og (c) i IPA 2016.

([376]) Code of Practice on Interception of Communications, paragraph 4.10, jf. fodnote 278.

([377]) Code of Practice on Interception of Communications, paragraph 6.20, jf. fodnote 278, og Code of Practice on Equipment Interference, paragraph 6.13, jf. fodnote 348.

([378]) Section 138(1)(g) og 178(1)(f) i IPA 2016. Den Europæiske Menneskerettighedsdomstol har navnlig identificeret en forudgående godkendelse fra et uafhængigt organ som en vigtig garanti mod misbrug i forbindelse med masseaflytning. Den Europæiske Menneskerettighedsdomstol (Store Afdeling), Big Brother Watch m.fl. mod Det Forenede Kongerige (jf. fodnote 269 ovenfor), præmis 351 og 352. Det er vigtigt at huske på, at denne dom vedrørte den tidligere retlige ramme (RIPA 2000), som ikke indeholdt nogle af de garantier (herunder forudgående godkendelse fra en uafhængig Judicial Commissioner), der blev indført med IPA 2016.

([379]) Section 159 (3) og (4) i IPA 2016.

([380]) Section 143-146 og 184-188 i IPA 2016. I tilfælde af en hastende ændring kan Secretary of State foretage ændringen uden godkendelse, men skal underrette Judicial Commissioner, som derefter skal beslutte, om ændringen skal tillades eller afvises (Section 147 i IPA 2016). Kendelser skal annulleres, hvis de ikke længere er nødvendige eller forholdsmæssige, eller hvis undersøgelsen af aflyttet indhold, metadata eller andre data, der er indsamlet i henhold til kendelsen, ikke længere er nødvendig med henblik på de operationelle formål, der er angivet i kendelsen (Section 148 og 189 i IPA 2016).

([381]) Code of Practice on Interception of Communications, paragraph 6.44-6.47, jf. fodnote 278, og Code of Practice on Equipment Interference, paragraph 6.48, jf. fodnote 348.

(227) I lighed med hvad der er fastsat for målrettet aflytning, fastsætter Part 6 i IPA 2016, at Secretary of State skal sikre, at der er indført ordninger til sikring af opbevaring og videregivelse af materiale, der er fremskaffet i henhold til kendelsen ([382]), samt til offentliggørelse i udlandet ([383]). Navnlig kræver Section 150(5) og 191(5) i IPA 2016, at alle eksemplarer, der er fremstillet af det materiale, der er indsamlet i henhold til kendelsen, skal opbevares sikkert og destrueres, så snart der ikke længere foreligger nogen relevante grunde til at beholde dem, mens Section 150(2) og 191(2) kræver, at antallet af personer, som materialet videregives til, og omfanget i hvilket materialet videregives, stilles til rådighed eller kopieres, begrænses til det minimum, der er nødvendigt af hensyn til de lovbestemte formål ([384]).

(228) Endelig fastsættes det i IPA 2016, at når det materiale, der er blevet opsnappet enten gennem masseaflytning eller masseindgreb i udstyr, skal overdrages til et tredjeland (»oversøiske oplysninger«), skal Secretary of State sikre, at der er truffet passende foranstaltninger til at sikre, at der findes lignende foranstaltninger vedrørende sikkerhed, opbevaring og videregivelse i det pågældende tredjeland ([385]). I henhold til Section 109 i DPA 2018 gælder der særlige krav for internationale overførsler af personoplysninger fra efterretningstjenester til tredjelande eller internationale organisationer, og oplysningerne må ikke overføres til et land eller territorium uden for Det Forenede Kongerige eller til en international organisation, medmindre overførslen er nødvendig og står i et rimeligt forhold til formålet med den dataansvarliges lovbestemte funktioner eller til andre formål, der er fastsat i Section 2(2)(a) i Security Service Act 1989 eller Section 2(2)(a) og 4(2)(a) i Intelligence Services Act 1994 ([386]). Det er vigtigt at bemærke, at disse krav også gælder i tilfælde, hvor den nationale sikkerhedsundtagelse i henhold til Section 110 i DPA 2018 påberåbes, da Section 110 i DPA 2018 ikke opregner Section 109 i DPA 2018 som en af de bestemmelser, der kan fraviges, hvis en undtagelse fra visse bestemmelser er nødvendig for at beskytte den nationale sikkerhed.

(229) Når kendelsen er godkendt, og dataene er masseindsamlet, vil de blive gjort til genstand for en udvælgelse, inden de undersøges. Udvælgelses- og undersøgelsesfasen er genstand for en yderligere proportionalitetstest udført af analytikeren, som på grundlag af de operationelle formål, der indgår i kendelsen (og eventuelt eksisterende filtreringsordninger), definerer udvælgelseskriterierne. Som fastsat i Section 152 og 193 i IPA skal Secretary of State ved udstedelsen af kendelsen sikre, at der er truffet foranstaltninger til at sikre, at udvælgelsen af materialet kun sker til de angivne operationelle formål, og at dette er nødvendigt og rimeligt under alle omstændigheder. I den forbindelse præciserede Det Forenede Kongeriges myndigheder, at det materiale, der masseindsamles, først og fremmest udvælges via automatisk filtrering med henblik på at frasortere data, der sandsynligvis ikke vil være af interesse for den nationale sikkerhed. Filtrene vil variere fra tid til anden (efterhånden som internettrafikmønstre, -typer og -protokoller ændrer sig) og afhænger af teknologien og den operationelle sammenhæng. Efter denne fase kan dataene kun udvælges til undersøgelse, hvis de er relevante for de operationelle formål, der er angivet i kendelsen ([387]). De garantier, der er fastsat i IPA 2016 for undersøgelse af det indsamlede materiale, gælder for alle typer oplysninger (både tilbageholdt indhold og sekundære oplysninger) ([388]). Section 152 og 193 i IPA 2016 indeholder også et generelt forbud mod at udvælge materiale til undersøgelse, der henviser til samtaler, der sendes af eller er beregnet til personer, der befinder sig på De Britiske Øer. Hvis myndighederne ønsker at undersøge dette materiale, skal de indgive en anmodning om en kendelse om målrettet undersøgelse i henhold til Part 2 og Part 4 i IPA 2016, udstedt af Secretary of State og godkendt af en Judicial Commissioner ([389]). Hvis en person bevidst udvælger aflyttet indhold til undersøgelse i strid med kravene i lovgivningen ([390]), begår vedkommende en strafbar handling ([391]).

([382]) Section 156 i IPA 2016.

([383]) Section 150 og 191 i IPA 2016.

([384]) Den Europæiske Menneskerettighedsdomstols Store Afdeling i sagen Big Brother Watch m.fl. mod Det Forenede Kongerige (jf. fodnote 268 ovenfor) opretholdt den ordning med yderligere garantier for opbevaring, adgang og videregivelse, der blev indført i henhold til RIPA 2000, jf. præmis 392-394 og 402-405. IPA 2016 indeholder samme garantiordning.

([385]) Section 151 og 192 i IPA 2016.

([386]) Se fodnote 312 for yderligere oplysninger om formålene.

([387]) I kodekserne for aflytning af kommunikation præciseres det i denne forbindelse, at »[d]isse behandlingssystemer behandler data fra de kommunikationsforbindelser eller signaler, som den aflyttende myndighed har valgt at aflytte. Der foretages derefter en vis filtrering af trafikken på disse forbindelser og signaler, der er udformet med henblik på at udvælge typer af kommunikation af potentiel efterretningsmæssig værdi og samtidig frasortere dem, der med mindst sandsynlighed vil have efterretningsmæssig værdi. Som følge af denne filtrering, som vil variere mellem behandlingssystemerne, vil en betydelig del af kommunikationen på disse forbindelser og signaler automatisk blive frasorteret. Der kan derefter foretages yderligere komplekse søgninger for at uddrage yderligere meddelelser, der med størst sandsynlighed vil have den største efterretningsmæssige værdi, og som vedrører agenturets lovbestemte funktioner. Disse meddelelser kan derefter udvælges til undersøgelse med henblik på et eller flere af de operationelle formål, der er angivet i kendelsen, hvis betingelserne for nødvendighed og proportionalitet er opfyldt. Kun materiale, der ikke er filtreret fra, kan eventuelt udvælges til undersøgelse af bemyndigede personer« (adfærdskodekser for aflytning af kommunikation, paragraph 6.6, jf. fodnote 278).

([388]) Se Section 152(1) (a) og (b) i IPA 2016, ifølge hvilke undersøgelsen af begge typer oplysninger (tilbageholdt indhold og sekundære oplysninger) kun skal udføres til det angivne formål og være nødvendig og forholdsmæssig under alle omstændigheder.

([389]) Denne type kendelse er ikke påkrævet, når data vedrørende personer, der befinder sig på den britiske ø, er »sekundære oplysninger« (se Section 152 (1) (c) i IPA 2016).

([390]) Section 152 og 193 i IPA 2016.

([391]) Section 155 og 196 i IPA 2016.

(230) Den vurdering, som analytikeren foretager af udvælgelsen af materialet, er underlagt efterfølgende kontrol fra IPC's side, som evaluerer overholdelsen af de specifikke sikkerhedsforanstaltninger, der er fastsat i IPA 2016 for undersøgelsesfasen ([392]) (se også betragtning 229). IPC skal løbende overvåge (herunder gennem revision, undersøgelse og efterforskning) de offentlige myndigheders udøvelse af de efterforskningsbeføjelser, der er omhandlet i IPA 2016 ([393]). I denne forbindelse præciseres det i Code of Practice on Interception og Code of Practice on Equipment Interference, at agenturet skal føre fortegnelser med henblik på efterfølgende undersøgelser og revisioner, og i disse fortegnelser skal der redegøres for, hvorfor autoriserede personers adgang til materialet er nødvendig og forholdsmæssig, samt de gældende operationelle formål ([394]). For eksempel konkluderede Investigatory Powers Commissioner Office (IPCO) ([395]) i sin årsberetning for 2018, at de begrundelser, som analytikerne havde registreret for undersøgelse af visse typer af materiale, der var masseindsamlet, overholdt den krævede proportionalitetsstandard, idet de omfattede tilstrækkelige oplysninger om årsagerne til deres »forespørgsler« i forhold til det formål, der søgtes opfyldt ([396]). I sin rapport fra 2019 gav IPCO hvad massebeføjelser angår klart udtryk for, at hensigten var at fortsætte inspektionerne af masseaflytninger, herunder en detaljeret undersøgelse af selektorerne og søgekriterierne ([397]). IPCO vil endvidere i hvert enkelt tilfælde fortsat nøje undersøge valget af overvågningsforanstaltninger (målrettet mod masseaflytninger) både under behandlingen af ansøgninger om retskendelse under double-lock-proceduren og ved inspektioner ([398]). Der vil blive taget behørigt hensyn til denne yderligere overvågning i forbindelse med Kommissionens overvågning af denne afgørelse, jf. betragtning 281-284.

3.3.1.1.4.2. Masseindsamling af kommunikationsdata

(231) Chapter 2 i Part 6 i IPA 2016 regulerer kendelser om masseindsamling, der giver adressaten tilladelse til at kræve, at en teleoperatør videregiver eller indsamler kommunikationsdata, som operatøren er i besiddelse af. Disse kendelser giver også den anmodende myndighed tilladelse til at udvælge data til den videre fase af efterforskningen. Som det er tilfældet med målrettet opbevaring og indsamling af kommunikationsdata (se betragtning 199), vedrører masseindsamling af kommunikationsdata normalt ikke personoplysninger om registrerede i EU, der overføres til Det Forenede Kongerige i henhold til denne afgørelse. Forpligtelsen til at videregive kommunikationsdata i henhold til Chapter 2 i Part 6 i IPA 2016 omfatter data, der indsamles af teleoperatører i Det Forenede Kongerige direkte fra brugerne af en telekommunikationstjeneste ([399]). Denne type »kundeorienterede« behandling indebærer typisk ikke en overførsel på grundlag af denne afgørelse, dvs. en overførsel fra en dataansvarlig/databehandler i EU til en dataansvarlig/databehandler i Det Forenede Kongerige.

(232) For fuldstændighedens skyld er betingelserne og garantierne for masseindsamling af kommunikationsdata imidlertid beskrevet nedenfor.

([392]) Section 152 og 193 i IPA 2016.
([393]) Section 229 i IPA 2016.
([394]) Code of Practice on Interception of Communications, paragraph 6.74, jf. fodnote 278, og Code of Practice on Equipment Interference, paragraph 6.78, jf. fodnote 348.
([395]) IPCO er oprettet i henhold til Section 238 i IPA 2016 for at give IPC det personale og udstyr og de lokaler og andre faciliteter og tjenester, der er nødvendige for, at denne kan udføre sine opgaver (se betragtning 251).
([396]) I IPCO's årsberetning for 2018 præciserede man, at de begrundelser, som analytikere i GCHQ havde registreret, »opfyldte den krævede standard, og analytikerne tog tilstrækkeligt hensyn til proportionaliteten af deres forespørgsler om massedata«. Årsberetning fra Investigatory Powers Commissioner 2018, paragraph 6.22, jf. fodnote 464.
([397]) Årsberetning fra Investigatory Powers Commissioner 2019, paragraph 7.6, jf. fodnote 463.
([398]) Årsberetning fra Investigatory Powers Commissioner 2019, paragraph 10.22, jf. fodnote 463.
([399]) Dette følger af definitionen af kommunikationsdata i Section 261(5) i IPA 2016, ifølge hvilken kommunikationsdata opbevares eller indsamles af en teleoperatør og enten vedrører brugeren af en telekommunikationstjeneste og vedrører leveringen af denne tjeneste eller er omfattet af, en del af, vedføjet eller logisk forbundet med kommunikation (se også Code of Practice on Bulk Acquisition of Communications Data, der findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, paragraph 2.15 til 2.22). Desuden kræver definitionen af teleoperatør i Section 261(10) i IPA 2016, at en teleoperatør er en person, der tilbyder eller leverer en teletjeneste til personer i Det Forenede Kongerige, eller som kontrollerer eller leverer et telekommunikationssystem, som (helt eller delvist) er etableret i eller kontrolleres af Det Forenede Kongerige. Disse definitioner gør det klart, at forpligtelser i henhold til IPA 2016 ikke kan pålægges teleoperatører, hvis udstyr ikke befinder sig i eller kontrolleres af Det Forenede Kongerige, og som ikke tilbyder eller leverer tjenester til personer i Det Forenede Kongerige (se også Code of Practice on Bulk Acquisition of Communications Data, paragraph 2.2). Hvis EU-abonnenter (uanset om de er etableret i EU eller i Det Forenede Kongerige) har gjort brug af tjenester i Det Forenede Kongerige, vil enhver kommunikation i forbindelse med leveringen af denne tjeneste blive indsamlet direkte af tjenesteudbyderen i Det Forenede Kongerige i stedet for at blive overført fra EU.

(233) IPA 2016 erstatter lovgivningen om masseindsamling af kommunikationsdata, som var genstand for EU-Domstolens dom i sagen Privacy International. Den i denne sag omhandlede lovgivning blev ophævet, og den nye ordning fastsætter særlige betingelser og garantier for, hvornår en sådan foranstaltning kan tillades.

(234) I modsætning til den tidligere ordning, i henhold til hvilken Secretary of State havde fuld skønsbeføjelse med hensyn til at godkende foranstaltningen ([400]), kræver IPA 2016 navnlig, at Secretary of State kun udsteder en kendelse, hvis foranstaltningen er nødvendig og forholdsmæssig. Dette betyder i praksis, at der skal være en sammenhæng mellem adgangen til oplysningerne og det tilstræbte mål ([401]). Mere specifikt skal Secretary of State vurdere, om der er en sammenhæng mellem den foranstaltning, der anmodes om, og et eller flere »operationelle formål«, der er anført i kendelsen (se betragtning 219), for så vidt angår vurderingen af proportionaliteten. I den relevante adfærdskodeks præciseres det, at »Secretary of State skal tage hensyn til, om det, der søges opnået med kendelsen, med rimelighed kan opnås med andre, mindre indgribende midler (Section 2(2)(a) i loven). For eksempel indsamling af de krævede oplysninger ved hjælp af en mindre indgribende foranstaltning såsom målrettet indsamling af kommunikationsdata ([402]).

(235) Med henblik på at foretage en sådan vurdering vil Secretary of State tage udgangspunkt i oplysninger, som lederne af efterretningstjenesterne ([403]) skal fremlægge i deres ansøgning, såsom grundene til, at foranstaltningen anses for nødvendig af en af de lovbestemte grunde, og grundene til, at det, der søges opnået, ikke med rimelighed kan opnås med andre, mindre indgribende midler ([404]). Desuden begrænser de operationelle formål det omfang, hvortil data, der er indsamlet i henhold til kendelsen, kan udvælges til undersøgelse ([405]). Som anført i den relevante adfærdskodeks skal de operationelle formål beskrive et klart krav og indeholde tilstrækkeligt detaljerede oplysninger til, at Secretary of State har vished for, at de indsamlede oplysninger kun kan udvælges til undersøgelse af specifikke grunde ([406]). Secretary of State skal nemlig, inden kendelsen godkendes, sikre, at der er truffet særlige foranstaltninger for at sikre, at kun det materiale, der anses for nødvendigt med henblik på en undersøgelse med et operationelt formål og et lovbestemt formål, udvælges til undersøgelsen og skal under alle omstændigheder være forholdsmæssigt afpasset og nødvendigt. Dette specifikke krav, som fremgår af Section 158 og 172 ([407]) i IPA 2016, vedrørende den forudgående vurdering af nødvendigheden og proportionaliteten af de kriterier, der anvendes i forbindelse med udvælgelsen, udgør endnu en vigtig nyskabelse ved ordningen, der blev indført med IPA 2016, sammenlignet med den tidligere gældende ordning.

(236) IPA 2016 indførte også en forpligtelse for Secretary of State til at sikre, at der, inden kendelsen til masseindsamling af kommunikationsdata udstedes, indføres specifikke begrænsninger for sikkerheden, opbevaringen og videregivelsen af de indsamlede personoplysninger ([408]). I tilfælde af offentliggørelse i udlandet finder de beskyttelsesforanstaltninger, der er beskrevet i betragtning 227, for masseaflytning og masseindgreb i udstyr også anvendelse i denne sammenhæng ([409]). Der er fastsat yderligere begrænsninger i lovgivningen om varighed ([410]), fornyelse ([411]) og ændring af kendelser om masseindsamling ([412]).

(237) Det er vigtigt at bemærke, at Secretary of State, for så vidt angår de øvrige beføjelser vedrørende masseindsamling, inden han eller hun udsteder kendelsen, skal have en godkendelse fra en Judicial Commissioner ([413]). Dette er et centralt element i den ordning, der blev indført med IPA 2016.

([400]) Section 94(1) i Telecommunication Act 1984 bestemte, at Secretary of State kan udstede »generelle instrukser, som denne finder nødvendige eller hensigtsmæssige af hensyn til den nationale sikkerhed« (jf. fodnote 451).

([401]) Se Privacy International, præmis 78.

([402]) Se Code of Practice on Bulk Acquisition of Communications Data, paragraph 4.11 (jf. fodnote 399-414).

([403]) En kendelse om masseindsamling kan kun kræves af lederne af efterretningstjenesterne, som er: i) Director General of the Security Service (generaldirektøren for sikkerhedstjenesten), ii) Chief of the Secret Intelligence Service (chefen for efterretningstjenesten) eller iii) Director of the GCHQ (direktøren for GCHQ (se Section 158 og 263 i IPA 2016).

([404]) Code of practice on bulk acquisition of communications data, paragraph 4.5 (jf. fodnote 399).

([405]) I henhold til Section 161 i IPA 2016 skal de operationelle formål, der er angivet i kendelsen, være angivet på en liste, der føres af lederne af efterretningstjenesterne (»listen over operationelle formål«), som formål, de anser for at være operationelle formål, som gør det muligt at udvælge kommunikationsdata, der er indsamlet i forbindelse med masseindsamling, til undersøgelse.

([406]) Code of Practice on Bulk Acquisition of Communications Data, paragraph 6.6 (jf. fodnote 399).

([407]) I henhold til Section 172 i IPA 2016 skal der indføres særlige sikkerhedsforanstaltninger for filtrerings- og udvælgelsesfasen med henblik på gennemgang af kommunikation, der er masseindsamlet. Desuden er en bevidst undersøgelse i strid med disse garantier også en strafbar handling (se Section 173 i IPA 2016).

([408]) Section 171 i IPA 2016.

([409]) Section 171(9) i IPA 2016.

([410]) Section 162 i IPA 2016.

([411]) Section 163 i IPA 2016.

([412]) Section 164-166 i IPA 2016.

([413]) Section 159 i IPA 2016.

(238) IPC fører efterfølgende kontrol med undersøgelsesproceduren for det materiale (kommunikationsdata), der masseindsamles (se betragtning 254 nedenfor). I den forbindelse indførtes der med IPA 2016 et krav om, at den efterretningsanalytiker, der foretager undersøgelsen, inden udvælgelsen af de data, der skal undersøges, skal registrere årsagen til, at den foreslåede undersøgelse er nødvendig og står i et rimeligt forhold til et bestemt operationelt formål ([414]). I IPCO's årsberetning for 2019 blev det konstateret med hensyn til GCHQ's og MI5's praksis, at »den kritiske rolle, som massekommunikationsdata spiller for de forskellige aktiviteter, der udføres i GCHQ, var veldefineret i det sagsarbejde, vi kontrollerede. Vi vurderede arten af de ønskede data og de anførte efterretningsbehov og fandt det godtgjort, at dokumentationen viste, at deres tilgang var nødvendig og forholdsmæssig ([415]). MI5's registrerede begrundelser var af god standard og opfyldte principperne om nødvendighed og proportionalitet« ([416]).

3.3.1.1.4.3. Opbevaring og undersøgelse af datasæt med massepersonoplysninger

(239) Kendelser om datasæt med massepersonoplysninger ([417]) giver efterretningstjenesterne tilladelse til at opbevare og undersøge datasæt, der indeholder personoplysninger om en række personer. I henhold til Det Forenede Kongeriges myndigheders forklaringer kan analysen af sådanne datasæt være »den eneste måde, hvorpå UKIC kan komme videre i efterforskningen og identificere terrorister ud fra meget begrænsede efterretninger om de pågældende, eller når deres kommunikation bevidst er holdt skjult« ([418]). Der findes to typer kendelser: »Class BPD warrants« ([419]) (kendelser om en kategori af datasæt med massepersonoplysninger), der vedrører en bestemt kategori af datasæt, dvs. datasæt, der er ens med hensyn til indhold og tiltænkt anvendelse, og som giver anledning til overvejelser med hensyn til f.eks. graden af indgriben og følsomhed samt forholdsmæssigheden af at anvende dataene, således at Secretary of State kan overveje nødvendigheden og proportionaliteten af at indsamle alle data inden for den relevante kategori på én gang. For eksempel kan en class BPD warrant omfatte rejsedatasæt vedrørende ruter, der minder om hinanden ([420]). »Specific BPD warrants« ([421]) (kendelser om et specifikt datasæt med massepersonoplysninger) vedrører i stedet et specifikt datasæt, f.eks. et datasæt med en ny eller usædvanlig type oplysninger, som ikke falder ind under en eksisterende kategori af datasæt med massepersonoplysninger, eller et datasæt, der vedrører specifikke typer personoplysninger ([422]) og derfor kræver yderligere sikkerhedsforanstaltninger ([423]). Bestemmelserne i IPA 2016 vedrørende datasæt med massepersonoplysninger giver kun mulighed for at undersøge og opbevare sådanne datasæt, hvis det er nødvendigt og forholdsmæssigt ([424]), og i overensstemmelse med de generelle forpligtelser vedrørende privatlivets fred ([425]).

(240) Beføjelsen til at udstede en kendelse om et datasæt med massepersonoplysninger er underlagt »double-lock-proceduren«: Vurderingen af, om foranstaltningen er nødvendig og forholdsmæssig, foretages først af Secretary of State og derefter af Judicial Commissioner ([426]). Secretary of State er forpligtet til at tage stilling til arten og omfanget af den type kendelse, der anmodes om, den pågældende kategori af oplysninger og antallet af individuelle datasæt med massepersonoplysninger, der kan tænkes at falde ind under den specifikke type kendelse ([427]). Som anført i Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets skal der føres detaljerede registre, som skal underkastes IPC-revision ([428]). Opbevaring og undersøgelse af datasæt med massepersonoplysninger uden for rammerne af IPA 2016 er en strafbar handling ([429]).

([414]) IPCO Annual Report 2019, paragraph 8.6, jf. fodnote 463.
([415]) IPCO Annual Report 2019, paragraph 10.4, jf. fodnote 463.
([416]) IPCO Annual Report 2019, paragraph 8.37, jf. fodnote 463.
([417]) Section 200 i IPA 2016.
([418]) UK Explanatory Framework for Adequacy Discussions, section H: National Security, s. 34, se fodnote 29.
([419]) Section 204 i IPA 2016.
([420]) Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, paragraph 4.7, som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) Section 205 i IPA 2016.
([422]) For eksempel følsomme personoplysninger, se Section 202 i IPA 2016 og Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, paragraph 4.21 og 4.12, se fodnote 469.
([423]) En ansøgning om en kendelse om et specifikt datasæt med massepersonoplysninger skal behandles individuelt af Secretary of State, dvs. med hensyn til ét specifikt datasæt. I henhold til Section 205 i IPA skal efterretningstjenesten i sin ansøgning om en kendelse om et specifikt datasæt med massepersonoplysninger medtage en detaljeret redegørelse for arten og omfanget af det pågældende materiale og en liste over de »operationelle formål«, hvortil den relevante efterretningstjeneste ønsker at undersøge datasættet med massepersonoplysninger (hvor efterretningstjenesten ansøger om en kendelse til opbevaring og undersøgelse i stedet for kun opbevaring). Når der udstedes en kendelse om en kategori af datasæt med massepersonoplysninger, tager Secretary of State i stedet hensyn til hele kategorien af datasæt på én gang.
([424]) Section 204 og Section 205 i IPA 2016.
([425]) Section 2 i IPA 2016.
([426]) Section 204 og 205 i IPA 2016.
([427]) Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, paragraph 5.2, jf. fodnote 420.
([428]) Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, paragraph 8.1-8.15, jf. fodnote 420.
([429]) UK Explanatory Framework for Adequacy Discussions, section H: National Security, s. 34, se fodnote 29.

3.3.2. *Yderligere anvendelse af de indsamlede oplysninger*

(241) Personoplysninger, der behandles i henhold til Part 4 i DPA 2018, må ikke behandles på en måde, der er uforenelig med det formål, hvortil de blev indsamlet ([430]). DPA 2018 fastsætter, at den dataansvarlige kan behandle oplysningerne til et andet formål end det, hvortil oplysningerne blev indsamlet, når det er foreneligt med det oprindelige formål, og forudsat at den dataansvarlige ved lov er bemyndiget til at behandle oplysningerne, og at behandlingen er nødvendig og forholdsmæssig ([431]). Desuden præciseres det i Security Service Act 1989 og Intelligence Services Act 1994, at lederne af efterretningstjenesterne har pligt til at sikre, at ingen oplysninger indsamles eller videregives, medmindre det er nødvendigt for den korrekte varetagelse af agenturets funktioner eller til andre begrænsede og specifikke formål, der er anført i de relevante bestemmelser ([432]).

(242) Desuden indeholder Section 109 i DPA 2018 specifikke krav til efterretningstjenesters internationale videregivelse af personoplysninger til tredjelande eller internationale organisationer. I henhold til denne bestemmelse må personoplysninger ikke videregives til et land eller territorium uden for Det Forenede Kongerige eller til en international organisation, medmindre videregivelsen er nødvendig og står i et rimeligt forhold til formålet med den dataansvarliges lovbestemte funktioner eller til andre formål, der er fastsat i Section 2(2)(a) i Security Service Act 1989 eller Section 2(2)(a) og 4(2)(a) i Intelligence Services Act 1994 ([433]). Det er vigtigt at bemærke, at disse krav også gælder i tilfælde, hvor den nationale sikkerhedsundtagelse i henhold til Section 110 i DPA 2018 påberåbes, da Section 110 i DPA 2018 ikke opregner Section 109 i DPA 2018 som en af de bestemmelser, der kan fraviges, hvis en undtagelse fra visse bestemmelser er nødvendig for at beskytte den nationale sikkerhed.

(243) Som påpeget af ICO i sine retningslinjer om efterretningstjenesters behandling er en efterretningstjeneste, ud over de garantier, der er fastsat i Part 4 i DPA 2018, desuden, når den deler oplysninger med et tredjelands efterretningsenhed, også omfattet af garantier i henhold til andre lovgivningsmæssige foranstaltninger, der gælder for dem, for at sikre, at personoplysninger indsamles, deles og håndteres lovligt og ansvarligt ([434]). IPA 2016 indeholder eksempelvis yderligere garantier i forbindelse med overførsel til et tredjeland af materiale, der er indsamlet gennem målrettet aflytning ([435]), et målrettet indgreb i udstyr ([436]), masseaflytning ([437]), masseindsamling af kommunikationsdata ([438]) og masseindgreb i udstyr ([439]) (såkaldte »oversøiske oplysninger«). Den myndighed, der udsteder kendelsen, skal navnlig sikre, at der er truffet foranstaltninger til at sikre, at det tredjeland, der modtager oplysningerne, begrænser antallet af personer, der ser materialet, samt omfanget af videregivelsen og antallet af kopier af alt materiale til det minimum, som er nødvendigt til de godkendte formål, der er fastsat i IPA 2016 ([440]).

3.3.3. *Kontrol*

(244) Myndighedsadgang af hensyn til den nationale sikkerhed overvåges af en række forskellige organer. Information Commissioner fører kontrol med behandlingen af personoplysninger i henhold til DPA 2018 (for yderligere oplysninger om Information Commissioners uafhængighed, rolle vedrørende udpegelser og beføjelser henvises til betragtning 85-98), mens IPC fører uafhængig og retlig kontrol med anvendelsen af efterforskningsbeføjelser i

([430]) Section 87(1) i DPA 2018.

([431]) Section 87(3) i DPA 2018. Selv om dataansvarlige kan undtages fra dette princip i henhold til Section 110 i DPA 2018, i det omfang en sådan undtagelse er nødvendig af hensyn til den nationale sikkerhed, skal en sådan undtagelse vurderes fra sag til sag og kan kun påberåbes i det omfang, anvendelsen af en given bestemmelse ville have negative konsekvenser for den nationale sikkerhed (se betragtning 132). De nationale sikkerhedscertifikater for Det Forenede Kongeriges efterretningstjenester (findes på følgende link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) omfatter ikke Section 87(3) i DPA 2018. Da enhver behandling til et andet formål desuden skal være tilladt ved lov, skal efterretningstjenesterne have et klart retsgrundlag for den videre behandling.

([432]) Se fodnote 312 for yderligere oplysninger om formålene.

([433]) Jf. fodnote 312.

([434]) ICO's retningslinjer om efterretningstjenesters behandling (jf. fodnote 161).

([435]) Section 54 i IPA 2016.

([436]) Section 130 i IPA 2016.

([437]) Section 151 i IPA 2016.

([438]) Section 171(9) i IPA 2016.

([439]) Section 192 i IPA 2016.

([440]) Foranstaltningerne skal omfatte foranstaltninger til sikring af, at alle eksemplarer af det pågældende materiale opbevares på en sikker måde, så længe det opbevares. Materiale, der er fremskaffet på grundlag af en kendelse, og enhver kopi af et sådant materiale skal destrueres, så snart der ikke længere foreligger nogen relevante grunde til at opbevare det (se Section 150 (2), 150(5) og 151(2) i IPA 2016). Det er værd at bemærke, at lignende garantier i henhold til den tidligere retlige ramme (RIPA 2000) blev fundet i overensstemmelse med de krav, som Den Europæiske Menneskerettighedsdomstol havde fastsat for deling af materiale opnået ved masseaflytning med fremmede stater eller internationale organisationer (Den Europæiske Menneskerettighedsdomstol (Store Afdeling), Big Brother Watch m.fl. mod Det Forenede Kongerige, (jf. fodnote 279 ovenfor), præmis 362 og 399).

henhold til IPA 2016. IPC fører kontrol med, at både retshåndhævende myndigheder og nationale sikkerhedsmyndigheder anvender efterforskningsbeføjelserne i IPA 2016. Den politiske kontrol sikres af parlamentets Intelligence Service Committee (udvalg vedrørende efterretningstjenesterne).

3.3.3.1. Kontrol i henhold til Part 4 i DPA

(245) Den behandling af personoplysninger, der foretages af efterretningstjenesterne i henhold til Part 4 i DPA 2018, overvåges af Information Commissioner ([441]).

(246) Information Commissioners generelle opgaver i forbindelse med efterretningstjenesternes behandling af personoplysninger i henhold til Part 4 i DPA 2018 er fastlagt i Schedule 13 til DPA 2018. Opgaverne omfatter, men er ikke begrænset til, overvågning og håndhævelse af Part 4 i DPA 2018, fremme af offentlighedens bevidsthed, rådgivning af parlamentet, regeringen og andre institutioner om lovgivningsmæssige og administrative foranstaltninger, fremme af dataansvarliges og databehandleres kendskab til deres forpligtelser, underretning af den registrerede om udøvelsen af registreredes rettigheder og gennemførelse af undersøgelser osv.

(247) Information Commissioner har ligesom for Part 3 i DPA 2018 beføjelse til at underrette de dataansvarlige om en påstået overtrædelse og udstede advarsler om, at en behandling sandsynligvis vil udgøre en overtrædelse af reglerne, og udstede irettesættelser, når overtrædelsen bekræftes. Den kan også udstede enforcement og penalty notices for overtrædelser af visse bestemmelser i loven ([442]). I modsætning til for andre dele af DPA 2018 kan Information Commissioner imidlertid ikke udstede en assessment notice til et nationalt sikkerhedsagentur ([443]).

(248) Desuden indeholder Section 110 i DPA 2018 en undtagelse fra anvendelsen af visse af Information Commissioners beføjelser, når dette er nødvendigt af hensyn til beskyttelsen af den nationale sikkerhed. Dette omfatter Information Commissioners beføjelse til at udstede (enhver form for) notices i henhold til DPA (information, assessment, enforcement og penalty notices), beføjelse til at foretage inspektioner i overensstemmelse med internationale forpligtelser, ransagnings- og inspektionsbeføjelser samt reglerne om lovovertrædelser ([444]). Som forklaret i betragtning 126finder disse undtagelser kun anvendelse, hvis det er nødvendigt og forholdsmæssigt, og vurderes fra sag til sag.

(249) ICO og Det Forenede Kongeriges efterretningstjenester har undertegnet et Memorandum of Understanding ([445]), der fastlægger en ramme for samarbejde om en række spørgsmål, herunder anmeldelser af brud på datasikkerheden og behandling af klager fra registrerede. Det fastsætter navnlig, at ICO efter modtagelse af en klage vurderer, at anvendelsen af en eventuel undtagelse vedrørende den nationale sikkerhed er blevet anvendt korrekt. Svar på forespørgsler fra ICO i forbindelse med behandlingen af individuelle klager skal gives inden for 20 arbejdsdage af den berørte efterretningstjeneste ved hjælp af passende sikre kanaler, hvis der er tale om fortrolige oplysninger. ICO har fra april 2018 til dato modtaget 21 klager over efterretningstjenesterne fra enkeltpersoner. Hver klage er blevet vurderet, og resultatet er meddelt den registrerede ([446]).

([441]) Section 116 i DPA 2018.

([442]) I henhold til Schedule 13, paragraph 2, i DPA 2018 kan der udstedes påbud og afgørelser om sanktioner til en dataansvarlig eller databehandler i forbindelse med overtrædelser af Chapter 2 i Part 4 i DPA 2018 (behandlingsprincipper), en bestemmelse i Part 4 i DPA 2018, der giver den registrerede rettigheder, et krav om at underrette Information Commissioner om brud på persondatasikkerheden i henhold til Section 108 i DPA 2018 og principperne for videregivelse af personoplysninger til tredjelande, lande, der ikke er part i konventionen, og internationale organisationer i Section 109 i DPA 2018 (for yderligere oplysninger om håndhævelsesmeddelelser og sanktionsafgørelser, se betragtning 92).

([443]) I henhold til Section 147(6) i DPA 2018 kan Information Commissioner ikke udstede en assessment notice til et organ, der er nævnt i Section 23(3) i Freedom of Information Act 2000. Dette omfatter Security Service (sikkerhedstjenesten, MI5), Secret Intelligence Service (efterretningstjenesten, MI6) og Government Communications Headquarter (regeringens hovedkvarter for kommunikation)).

([444]) De bestemmelser, der kan indrømmes undtagelser fra, er: Section 108 (anmeldelse af brud på persondatasikkerheden til Information Commissioner), Section 119 (inspektion i overensstemmelse med internationale forpligtelser), Section 142-154 og Schedule 15 (Information Commissioner's notices og beføjelser vedrørende adgang og inspektion) og Section 170-173 (lovovertrædelser vedrørende personoplysninger). Endvidere så vidt angår behandling foretaget af efterretningstjenesterne i Schedule 13 (Information Commissioners øvrige generelle opgaver), paragraph 1(a) og (g) og 2.

([445]) Aftalememorandum mellem Information Commission's Office og Det Forenede Kongeriges efterretningstjeneste, jf. fodnote 165.

([446]) I syv af disse sager rådede ICO klageren til at gøre opmærksom på problemet over for den dataansvarlige (dette er tilfældet, når en person har gjort ICO opmærksom på et problem, men først burde have gjort den dataansvarlige opmærksom på det). I et af disse tilfælde gav ICO generel rådgivning til den dataansvarlige (dette sker, når den dataansvarliges handlinger ikke synes at have overtrådt lovgivningen, men hvor en forbedring af praksis kunne have forhindret, at problemet blev taget op over for ICO). I de øvrige 13 tilfælde krævedes der ingen indgriben fra den dataansvarlige (dette anvendes, når de problemer, som den pågældende person gør opmærksom på, hører under Data Protection Act 2018, fordi de vedrører behandling af personoplysninger, men hvor den dataansvarlige på grundlag af de forelagte oplysninger ikke synes at have overtrådt lovgivningen).

3.3.3.2. Kontrol med anvendelsen af efterforskningsbeføjelser under IPA 2016

(250) I henhold til Part 8 i IPA 2016 udøves kontrollen med anvendelsen af efterforskningsbeføjelserne af Investigatory Powers Commissioner (IPC). IPC bistås af andre Judicial Commissioners, der under ét benævnes »Judicial Commissioners« ([447]). IPA 2016 fastsætter de garantier, der beskytter Judicial Commissioners uafhængighed. Judicial Commissioners skal beklæde eller have varetaget en høj retslig funktion (dvs. de skal være eller have været medlem af de øverste domstole) ([448]), og som medlemmer af dommerstanden er de uafhængige af regeringen ([449]). I henhold til Section 227 i IPA 2016 skal premierministeren udnævne IPC og det antal Judicial Commissioners, som han anser for nødvendigt. Alle Commissioners, uanset om de er nuværende eller tidligere medlemmer af dommerstanden, kan kun udnævnes på grundlag af en fælles henstilling fra de tre Chief Justices for England & Wales, Skotland og Nordirland og Lord Chancellor ([450]). Secretary of State skal stille personale, indkvartering, udstyr og andre faciliteter og tjenester til rådighed for IPC ([451]). Judicial Commissioners' embedsperiode er tre år, og de kan genudnævnes ([452]). Judicial Commissioners kan som en yderligere garanti for deres uafhængighed kun afsættes fra embedet på strenge betingelser, der kræver en høj tærskel: enten af premierministeren under de særlige omstændigheder, der er anført udtømmende i Section 228(5) i IPA 2016 (såsom konkurs eller fængsling), eller hvis parlamentets to kamre har vedtaget en beslutning om godkendelse af afsættelsen ([453]).

(251) IPC og Judicial Commissioners støttes i deres roller af Investigatory Powers Commissioner's Office (kontoret for efterforskningsbeføjelser, IPCO). IPCO's personale omfatter et team af efterforskere, interne juridiske og tekniske eksperter og et Technology Advisory Panel (rådgivende teknologipanel), der yder ekspertrådgivning. Som det er tilfældet for de enkelte Judicial Commissioners, er IPCO's uafhængighed beskyttet. IPCO er et »armslængde-organ« under Home Office (indenrigsministeriet), dvs. det modtager finansiering fra indenrigsministeriet, men udfører sine opgaver uafhængigt ([454]).

(252) De vigtigste funktioner, som Judicial Commissioners varetager, er beskrevet i Section 229 i IPA 2016 ([455]). Navnlig har Judicial Commissioners en omfattende beføjelse til forudgående godkendelse, hvilket er en del af de garantier, der blev indført i Det Forenede Kongeriges retlige ramme med IPA 2016. Kendelser i forbindelse med målrettet aflytning, indgreb i udstyr, datasæt med massepersonoplysninger, masseindsamling af kommunikationsdata samt lagringsmeddelelser vedrørende kommunikationsdata skal alle godkendes af Judicial Commissioners ([456]). IPC skal også altid forhåndsgodkende indsamlingen af kommunikationsdata med henblik på retshåndhævelse ([457]). Hvis en Judicial Commissioner nægter at godkende en kendelse, kan Secretary of State appellere til Investigatory Powers Commissioner, hvis afgørelse er endelig.

([447]) I overensstemmelse med Section 227(7) og (8) i IPA 2016 er Investigatory Powers Commissioner en Judicial Commissioner, og Investigatory Powers Commissioner og de øvrige Judicial Commissioners kaldes under ét for Judicial Commissioners. Der er i øjeblikket 15 Judicial Commissioners.

([448]) I henhold til Section 60(2) i Part 3 af Constitutional Reform Act 2005 betyder en »høj retslig funktion« et embede som dommer ved en af følgende domstole: i) Supreme Court, ii) Court of Appeal i England og Wales, iii) High Court i England og Wales, iv) Court of Session, v) Court of Appeal i Nordirland, vi) High Court i Nordirland eller som Lord of Appeal in Ordinary.

([449]) Retsvæsenets uafhængighed er baseret på konvention og har været almindelig anerkendt siden Act of Settlement fra 1701.

([450]) Section 227(3) i IPA 2016. Judicial Commissioners skal også anbefales af Investigatory Powers Commissioner, jf. Section 227(4)(e) i IPA 2016.

([451]) Section 238 i IPA 2016.

([452]) Section 227(2) i IPA 2016.

([453]) Afsættelsesprocessen er identisk med afsættelsesprocessen for andre dommere i Det Forenede Kongerige (se f.eks. Section 11(3) i Senior Courts Act 1981 og Section 33 i Constitutional Reform Act 2005, som også kræver en beslutning efter godkendelse fra parlamentets to kamre). Indtil videre er ingen Judicial Commissioner blevet afsat fra sit embede.

([454]) Et armslængde-organ er en organisation eller et agentur, der modtager støtte fra en regering, men som er i stand til at handle uafhængigt (for en definition og flere oplysninger om armslængde-organer henvises til Handbook of the Cabinet Office on the classification of Public Bodies, som findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf og den første mødeprotokol fra 2014-2015 fra Public Administration Select Committee of the House of Commons, som findes på følgende link: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf) .

([455]) I henhold til Section 229 i IPA 2016 har Judicial Commissioner omfattende tilsynsbeføjelser, som også omfatter tilsyn med opbevaring og videregivelse af oplysninger indsamlet af efterretningstjenesterne.

([456]) Afgørelser om, hvorvidt Secretary of States afgørelse om at udstede en kendelse skal godkendes, træffes af Judicial Commissioners selv. Hvis en Judicial Commissioner nægter at godkende en kendelse, kan Secretary of State appellere til Investigatory Powers Commissioner, hvis afgørelse er endelig.

([457]) Der anmodes altid om IPC-godkendelse, når kommunikationsdata indsamles med henblik på retshåndhævelse (Section 60A i IPA 2016). Hvis kommunikationsdata indsamles af hensyn til den nationale sikkerhed, kan tilladelsen gives af IPC eller alternativt af en udpeget højtstående embedsmand fra den relevante offentlige myndighed (se Section 61 og 61A i IPA 2016 og betragtning 203).

(253) FN's særlige rapportør om retten til privatlivets fred udtrykte stor tilfredshed med indførelsen af Judicial Commissioners med IPA 2016, da »alle de mere følsomme eller indgribende anmodninger om at gennemføre overvågning skal godkendes af både en minister fra kabinettet og Investigatory Powers Commissioner's Office«. Han understregede navnlig, at »dette element af domstolskontrol [gennem IPC's rolle] bistået af et hold af erfarne efterforskere og teknologieksperter med flere ressourcer er en af de vigtigste nye beskyttelsesforanstaltninger, der er indført med IPA, der erstattede et tidligere fragmenteret system af kontrolmyndigheder og supplerer den rolle, som Intelligence and Security Committee of Parliament og Investigatory Powers Tribunal spiller« ([458]).

(254) IPC har desuden beføjelse til at føre *efterfølgende* kontrol, herunder ved hjælp af revision, inspektion og undersøgelse, med anvendelsen af efterforskningsbeføjelserne i henhold til IPA 2016 ([459]) og visse andre beføjelser og funktioner, der er fastsat i den relevante lovgivning ([460]). Resultaterne af en sådan *efterfølgende* kontrol indgår i den rapport, som IPC hvert år skal udarbejde og forelægge premierministeren ([461]), og som skal offentliggøres og forelægges parlamentet ([462]). Rapporten indeholder relevante statistikker og oplysninger om efterretningsagenturers og retshåndhævende myndigheders anvendelse af efterforskningsbeføjelserne samt anvendelsen af garantierne i forbindelse med materiale, der er omfattet af retten til fortrolighed mellem advokat og klient, fortroligt journalistisk materiale og kilder til journalistiske oplysninger, oplysninger om de foranstaltninger, der er truffet, og de operationelle formål, der anvendes i forbindelse med kendelser om masseindsamling. Endelig præciseres det i IPCO's årsberetning, på hvilket område der blev udstukket anbefalinger til de offentlige myndigheder, og hvordan de er blevet håndteret ([463]).

(255) I overensstemmelse med Section 231 i IPA 2016 skal IPC, hvis han eller hun får kendskab til en relevant fejl begået af offentlige myndigheder i forbindelse med udøvelsen af deres efterforskningsbeføjelser, underrette den pågældende person, hvis vedkommende mener, at fejlen er alvorlig, og det er i offentlighedens interesse, at personen underrettes ([464]). Navnlig præciseres det i Section 231 i IPA 2016, at når en person underrettes om en fejl, skal IPC fremlægge oplysninger om eventuelle rettigheder, som vedkommende har til at indbringe spørgsmålet for Investigatory Powers Tribunal, og fremlægge de oplysninger, som han eller hun anser for nødvendige for udøvelsen af disse rettigheder, og der er en offentlig interesse i videregivelsen ([465]).

([458]) End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland (jf. fodnote 281).

([459]) Section 229 i IPA 2016. Judicial Commissioners undersøgelses- og informationsbeføjelser er beskrevet i Section 235 i IPA 2016.

([460]) Dette omfatter overvågningsforanstaltninger i henhold til RIPA 2000, udøvelse af funktioner i henhold til Part 3 i Police Act 1997 (tilladelse til handling med hensyn til ejendom) og Secretary of States udøvelse af funktioner i henhold til Section 5-7 i Intelligence Services Act 1994 (kendelser til aflytning af trådløs telegrafi, adgang til og indtrængen på ejendom (Section 229 i IPA 2016).

([461]) Section 230 i IPA 2016. IPC kan også på eget initiativ aflægge rapport til premierministeren om ethvert spørgsmål vedrørende den pågældendes funktioner. IPC skal også aflægge rapport til premierministeren på dennes anmodning, og premierministeren kan pålægge IPC at gennemgå alle efterretningstjenesternes funktioner.

([462]) Nogle dele kan udelukkes, hvis det ville være i strid med den nationale sikkerhed at offentliggøre dem.

([463]) I IPCO's årsberetning for 2019 (paragraph 6.38) nævnes det f.eks., at MI5 blev anbefalet at ændre sin politik for opbevaring af datasæt med massepersonoplysninger, da man burde have anvendt en tilgang, hvor der blev taget hensyn til proportionaliteten af opbevaringen for alle områder af datasæt med massepersonoplysninger og for hvert af de opbevarede datasæt med massepersonoplysninger. Ved udgangen af 2018 fandt IPCO ikke, at denne anbefaling var blevet fulgt, og det blev i rapporten fra 2019 forklaret, at MI5 nu er ved at indføre en ny procedure for at opfylde dette krav. I årsberetningen for 2019 (paragraph 8.22) nævnes det også, at GHCQ modtog en række anbefalinger vedrørende registreringen af proportionaliteten af deres forespørgsler om massedata. Rapporten bekræfter, at der er sket forbedringer på dette område ved udgangen af 2018. Årsberetning fra Investigatory Powers Office 2019, som findes på følgende link: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Derudover, afsluttes hver IPCO-inspektion hos en offentlig myndighed med en rapport, der fremsendes til myndigheden, og som indeholder eventuelle anbefalinger, der følger af denne inspektion. IPCO påbegynder derefter hver efterfølgende inspektion med en gennemgang af eventuelle tidligere anbefalinger fra sidste gang, og det fremgår af den nye inspektionsrapport, om tidligere anbefalinger er blevet fulgt eller videreført.

([464]) En fejl betragtes som »alvorlig«, når IPC mener, at den har påført den pågældende væsentlig risiko eller skade (Section 231, stk. 2, i IPA 2016). I 2018 blev der indberettet 22 fejl, hvoraf otte blev anset for alvorlige og resulterede i, at den berørte person blev informeret. Jf. årsberetningen fra Investigatory Powers Office 2018, bilag C (se https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). I 2019 blev 14 fejl anset for at være alvorlige. Jf. årsberetningen fra Investigatory Powers Office 2019, bilag C, jf. fodnote 463.

([465]) Section 231 i IPA 2016 præciserer, at IPC, når han eller hun informerer en person om en fejl, skal give de oplysninger, som førstnævnte finder nødvendige for udøvelsen af disse rettigheder, navnlig under hensyntagen til, i hvilken udstrækning det ville være i strid med den offentlige interesse eller skade forebyggelsen eller afsløringen af grov kriminalitet, Det Forenede Kongeriges økonomiske velfærd eller den fortsatte udøvelse af efterretningstjenesternes funktioner.

3.3.3.3. Parlamentarisk kontrol med efterretningstjenesterne

(256) Den parlamentariske kontrol, der føres af Intelligence and Security Committee (ISC), har hjemmel i Justice and Security Act 2013 (JSA 2013) ([466]). Ved loven oprettes ISC som et udvalg under Det Forenede Kongeriges parlament. Siden 2013 har ISC fået større beføjelser, herunder kontrol med sikkerhedstjenesternes operationelle aktiviteter. I henhold til Section 2 i JSA 2013 har ISC til opgave at føre kontrol med de nationale sikkerhedsagenturers udgifter, administration, politik og drift. JSA 2013 præciserer, at ISC kan foretage undersøgelser af operationelle spørgsmål, når de ikke vedrører igangværende operationer ([467]). I det aftalememorandum, der er indgået mellem premierministeren og ISC ([468]), præciseres det nærmere, hvilke elementer der skal tages hensyn til, når det skal vurderes, hvorvidt en aktivitet ikke er en del af en igangværende operation ([469]). Premierministeren kan også anmode ISC om at undersøge igangværende operationer og gennemgå oplysninger, som agenturerne frivilligt fremlægger.

(257) I henhold til bilag 1 til JSA 2013 kan ISC anmode lederne af en af de tre efterretningstjenester om at videregive alle oplysninger. Agenturet skal stille disse oplysninger til rådighed, medmindre Secretary of State nedlægger veto mod dette ([470]). Ifølge de britiske myndigheders forklaringer tilbageholdes der i praksis meget få oplysninger fra ISC ([471]).

(258) ISC består af medlemmer, der tilhører parlamentets to kamre og udnævnes af premierministeren efter høring af oppositionslederen ([472]). ISC skal hvert år aflægge beretning til parlamentet om udøvelsen af sine funktioner og andre rapporter, som det finder hensigtsmæssige ([473]). Desuden har ISC ret til hver tredje måned at modtage listen over operationelle formål, der anvendes til at undersøge materiale, der er indsamlet som massedata ([474]). Premierministeren udveksler kopier af efterforskninger, inspektioner eller revisioner foretaget af Investigatory Power Commissioner med ISC, når emnet i rapporterne er relevant for udvalgets lovbestemte beføjelser ([475]). Endelig kan udvalget anmode IPC om at foretage en undersøgelse, og denne skal underrette ISC om sin beslutning om, hvorvidt der skal foretages en sådan undersøgelse ([476]).

(259) ISC kom også med input til udkastet til IPA 2016, hvilket resulterede i en række ændringer, som nu er afspejlet i IPA 2016 ([477]). ISC anbefalede navnlig en styrkelse af beskyttelsen af privatlivets fred ved at indføre et sæt beskyttelsesforanstaltninger for privatlivets fred, der gælder for hele rækken af

([466]) Som forklaret af de britiske myndigheder udvidede JSA Justeringen ISC's ansvarsområde til at omfatte en rolle i kontrollen med efterretningstjenesterne ud over de tre agenturer og mulighed for efterfølgende kontrol med agenturernes operationelle aktiviteter i spørgsmål af væsentlig national interesse.

([467]) Section 2 i JSA 2013.

([468]) Aftalememorandum mellem premierministeren og ISC findes på følgende link: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Memorandum of Understanding mellem premierministeren og ISC, paragraph 14, se fodnote 468.

([470]) Secretary of State kan kun nedlægge veto mod videregivelse af oplysninger af to grunde: Oplysningerne er følsomme og bør ikke videregives til ISC af hensyn til den nationale sikkerhed, eller der er tale om oplysninger af en sådan karakter, at Secretary of State (af grunde, der ikke er begrænset til den nationale sikkerhed) ville anse det for hensigtsmæssigt ikke at gøre dette, hvis Secretary of State blev anmodet om at fremlægge dem for et Departmental Select Committee (særligt ministerielt udvalg) i Underhuset (Schedule 1, paragraph 4(2) i JSA 2013).

([471]) UK Explanatory Framework for Adequacy Discussions, section H: National Security, s. 43, jf. fodnote 31.

([472]) Section 1 i JSA 2013. Ministre kan ikke være medlemmer. Medlemmerne sidder i ISC i den valgperiode, hvor de blev udnævnt. De kan fjernes ved en beslutning truffet af det kammer i parlamentet, som har udnævnt dem, eller hvis de ophører med at være parlamentsmedlem eller udnævnes til minister. Et medlem kan også træde tilbage.

([473]) Udvalgets beretninger og udtalelser er tilgængelige online via følgende link: https://isc.independent.gov.uk/publications/. I 2015 udsendte ISC rapporten »Privacy and Security: A modern and transparent legal framework« (se: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), hvor det behandlede de retlige rammer for de overvågningsteknikker, der anvendes af efterretningstjenesterne, og fremsatte en række henstillinger, som derefter blev overvejet og indarbejdet i Investigatory Powers Bill (lovforslag vedrørende efterforskningsbeføjelser), der blev gjort til lov, IPA 2016. Regeringens svar på Privacy and Security Report findes på følgende link: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) Section 142, 161 og 183 i IPA 2016.

([475]) Section 234 i IPA 2016.

([476]) Section 236 i IPA 2016.

([477]) Parlamentets Intelligence and Security Committee, rapport om forslaget til Investigatory Powers Bill, som findes på følgende link: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf.

efterforskningsbeføjelser ([478]). ISC foreslog også ændringer af den foreslåede kapacitet vedrørende indgreb i udstyr, datasæt med massepersonoplysninger og kommunikationsdata og anmodede om andre specifikke ændringer for at styrke begrænsningerne og garantierne i forbindelse med anvendelsen af efterforskningsbeføjelser ([479]).

3.3.4. *Klageadgang*

(260) På området myndighedsadgang af hensyn til den nationale sikkerhed skal de registrerede have mulighed for at anlægge sag ved en uafhængig og upartisk domstol for at få adgang til deres personoplysninger eller for at få dem berigtiget eller slettet ([480]). En sådan retsinstans skal navnlig have beføjelse til at træffe bindende afgørelser om efterretningstjenesten ([481]). Som forklaret i betragtning 261 til 271 giver en række retsmidler i Det Forenede Kongerige de registrerede mulighed for at anvende og få adgang til sådanne retsmidler.

3.3.4.1 Klagemekanismer i henhold til Part 4 i DPA

(261) I henhold til Section 165 i DPA 2018 har den registrerede ret til at indgive en klage til Information Commissioner, hvis den registrerede mener, at der i forbindelse med vedkommendes personoplysninger foreligger en overtrædelse af Part 4 i DPA 2018. Information Commissioner har beføjelse til at vurdere den dataansvarliges og databehandlerens overholdelse af DPA 2018 og kræve, at de tager de nødvendige skridt. I henhold til Part 4 i DPA 2018 har fysiske personer desuden ret til at anmode High Court (eller Court of Session i Skotland) om en kendelse, der pålægger den dataansvarlige at overholde retten til indsigt i oplysninger ([482]), at gøre indsigelse mod behandling ([483]) samt til berigtigelse eller sletning ([484]).

(262) Fysiske personer har også ret til at kræve erstatning for den skade, de har lidt som følge af den dataansvarliges eller databehandlerens overtrædelse af et krav i Part 4 i DPA 2018 ([485]). Skader omfatter både økonomiske tab og skader, der ikke indebærer økonomiske tab, såsom overlast ([486]).

3.3.4.2 Klagemekanismer i henhold til IPA 2016

(263) Enkeltpersoner kan få erstatning for overtrædelser af IPA 2016 ved Investigatory Powers Tribunal.

(264) Investigatory Powers Tribunal er oprettet ved RIPA 2000 og er uafhængig af den udøvende magt ([487]). I overensstemmelse med Section 65 i RIPA 2000 udnævnes medlemmerne af denne domstol af Kronen for en periode på fem år. Et medlem af domstolen kan afskediges af Kronen efter et forslag (»Address«) ([488]) fra begge parlamentets kamre ([489]).

([478]) Disse generelle forpligtelser vedrørende privatlivets fred er nu fastsat i Section 2, stk. 2, i IPA 2016, hvori det bestemmes, at en offentlig myndighed, der handler i henhold til IPA 2016, skal tage hensyn til, om det, der søges opnået med kendelsen, godkendelsen eller meddelelsen, med rimelighed kan opnås ved hjælp af andre, mindre indgribende midler, om det beskyttelsesniveau, der skal anvendes i forbindelse med indsamling af oplysninger i henhold til kendelsen, tilladelsen eller meddelelsen, er højere på grund af disse oplysningers særlige følsomhed, offentlighedens interesse i andre integritets- og sikkerhedsaspekter i telekommunikationssystemerne samt andre aspekter af offentlighedens interesse i beskyttelsen af personoplysninger.

([479]) Som følge af ISC's anmodning er antallet af dage, hvor en »hastekendelse« kan gælde, inden Judicial Commissioner skal godkende den, blevet reduceret fra fem til tre hverdage, og ISC fik beføjelse til at henvise sager til Investigatory Powers Commissioner med henblik på undersøgelse.

([480]) Schrems II-dommen, præmis 194.

([481]) Schrems II-dommen, præmis 197.

([482]) Section 94(11) i DPA 2018.

([483]) Section 99(4) i DPA 2018.

([484]) Section 100(1) i DPA 2018.

([485]) Section 169 i DPA 2018 tillader krav fra »en person, der lider skade som følge af overtrædelse af et krav i databeskyttelseslovgivningen«. Ifølge oplysningerne fra de britiske myndigheder vil et krav eller en klage mod efterretningstjenesterne i praksis sandsynligvis blive indbragt for Investigatory Powers Tribunal, som har bred kompetence, kan tilkende godtgørelse/erstatning, og når det ikke medfører omkostninger at indbringe et krav.

([486]) Section 169(5) i DPA 2018.

([487]) I henhold til Schedule 3 til RIPA 2000 skal medlemmerne have nærmere angivet juridisk erfaring og kan genudnævnes.

([488]) Et »Address« er et forslag, der forelægges Parlamentet, og som har til formål at gøre Kronen opmærksom på Parlamentets udtalelser om et bestemt emne.

([489]) Schedule 3, paragraph 1(5) i RIPA 2000.

(265) I henhold til Section 65 i RIPA 2000 er Investigatory Powers Tribunal den rette retsinstans for enhver klage fra en person, der er blevet krænket som følge af handlinger i henhold til IPA 2016, RIPA 2000 eller efterretningstjenesternes handlinger ([490]).

(266) For at anlægge sag ved Investigatory Powers Tribunal (opfylde kravet om søgsmålskompetence) skal en person i henhold til Section 65 i RIPA 2000 have en formodning om ([491]), at en efterretningstjeneste har udført aktiviteter vedrørende ham, et hvilket som helst af hans aktiver, enhver kommunikation, der er sendt af eller til ham eller er bestemt for ham, eller hans brug af en posttjeneste, en telekommunikationstjeneste eller et telekommunikationssystem ([492]). Desuden skal klageren have en formodning om, at aktiviteten har fundet sted under »anfægtelige omstændigheder« ([493]) eller »er udført af eller på vegne af efterretningstjenesterne« ([494]). Da navnlig denne »formodnings«-standard er blevet fortolket ret bredt ([495]), er indbringelse af en sag for retten underlagt lave krav til søgsmålskompetence.

(267) Når Investigatory Powers Tribunal behandler en klage, som er indbragt for den, er det dens opgave at undersøge, om de personer, der er genstand for en påstand i klagen, har udført handlinger i forhold til klageren, og at undersøge, hvilken myndighed der angiveligt har begået overtrædelserne, og om de påståede handlinger har fundet sted ([496]). Når Investigatory Powers Tribunal behandler en sag, skal den anvende de samme principper for at træffe afgørelse i denne sag, som en domstol ville anvende i forbindelse med en anmodning om domstolsprøvelse ([497]). Desuden har modtagerne af kendelser eller meddelelser i henhold til IPA 2016 og enhver anden person, der er ansat under Kronen, og som er ansat af politiet eller Police Investigations and Review Commissioner, pligt til at videregive eller fremlægge alle de dokumenter og oplysninger, som retten måtte have brug for, for at sætte dem i stand til at udøve deres kompetence ([498]).

(268) Investigatory Powers Tribunal skal underrette klageren om, hvorvidt vedkommende har fået medhold eller ej ([499]). I henhold til Section 67(6) og (7) i RIPA 2000 har Investigatory Powers Tribunal beføjelse til at udstede foreløbige kendelser og til at udstede enhver sådan tilkendelse af erstatning eller anden kendelse, som den finder passende. Dette kan omfatte en kendelse, der ophæver eller annullerer en kendelse eller tilladelse, og en kendelse om

([490]) Section 65(5) i RIPA 2000.

([491]) Med hensyn til standarden for »formodningstesten« henvises til sagen Human Rights Watch mod Secretary of State [2016] UKIPTrib15_165-CH, paragraph 41. I denne sag fastslog Investigatory Powers Tribunal med henvisning til Den Europæiske Menneskerettighedsdomstols retspraksis, at det passende kriterium er, om der for så vidt angår den påståede formodning om, at enhver handling, der henhører under Subsection 68(5) i RIPA 2000, er blevet udført af efterretningstjenesterne eller på vegne af en efterretningstjeneste, er grundlag for en sådan formodning, således at den pågældende kan påberåbe sig en krænkelse, der er fremkaldt af den blotte eksistens af hemmelige foranstaltninger eller lovgivning, der tillader hemmelige foranstaltninger, hvis han eller hun på grund af sin personlige situation kan påvise en sådan risiko.

([492]) Section 65(4)(a) i RIPA 2000.

([493]) Sådanne omstændigheder vedrører offentlige myndigheders handlinger, der finder sted med bemyndigelse (f.eks. en kendelse, en tilladelse/meddelelse om indsamling af kommunikation osv.), eller hvis omstændighederne er af en sådan art, at det (uanset om der foreligger en sådan bemyndigelse eller ej) ikke ville have været hensigtsmæssigt, at handlingerne fandt sted uden den, eller i det mindste uden at der var blevet taget behørigt hensyn til, om der skulle anmodes om en sådan bemyndigelse. Handlinger, der er godkendt af en Judicial Commissioner, anses for at have fundet sted under omstændigheder, der kan påklages (Section 65(7ZA) i RIPA 2000), mens andre handlinger, der finder sted med tilladelse fra en person, der varetager en retslig funktion, ikke anses for at have fundet sted under omstændigheder, der kan påklages (Section 65(7) og (8) i RIPA 2000).

([494]) Ifølge oplysningerne fra de britiske myndigheder viser den lave tærskel for indgivelse af en klage, at det ikke er usædvanligt, at Investigatory Powers Tribunal i sin undersøgelse fastslår, at klageren faktisk aldrig har været genstand for en offentlig myndigheds undersøgelse. Det fremgår af den seneste statistiske rapport fra Investigatory Powers Tribunal, at den i 2016 modtog 209 klager, hvoraf 52 % blev anset for at være useriøse eller chikanerende, mens 25 % førte til resultatet »ikke bestemt«. De britiske myndigheder forklarede, at dette enten betyder, at der ikke var blevet udøvet hemmelige aktiviteter/beføjelser over for klageren, eller at der var blevet anvendt skjulte teknikker, men at Investigatory Powers Tribunal fastslog, at aktiviteten var lovlig. Desuden blev 11 % kendt ugrundede, trukket tilbage eller kendt ikke gyldige, 5 % blev afvist på grund af overskridelse af tidsfristen, mens klageren fik medhold i 7 %. Statistisk rapport fra Investigatory Powers Tribunal 2016, tilgængelig via følgende link: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([495]) Se sagen Human Rights Watch mod Secretary of State [2016] UKIPTrib15_165-CH. I denne sag fastslog Investigatory Powers Tribunal med henvisning til Menneskerettighedsdomstolens retspraksis, at det passende kriterium med hensyn til formodningen om, at enhver handling, der falder ind under Subsection 68(5) i RIPA 2000, er blevet udført af eller på vegne af en efterretningstjeneste, kun er, om der er grundlag for en sådan formodning, herunder den omstændighed, at en person kan hævde at være offer for en krænkelse, der kan tilskrives den blotte eksistens af hemmelige foranstaltninger eller lovgivning, som tillader hemmelige foranstaltninger, hvis den pågældende kan påvise, at han eller hun på grund af sin personlige situation er udsat for sådanne foranstaltninger (se Human Rights Watch mod Secretary of State, præmis 41).

([496]) Section 67(3) i RIPA 2000.

([497]) Section 67(2) i RIPA 2000.

([498]) Section 68(6)-(7) i RIPA 2000.

([499]) Section 68(4) i RIPA 2000.

tilintetgørelse af ethvert register over oplysninger, der er indsamlet under udøvelse af beføjelser i henhold til en kendelse, tilladelse eller meddelelse, eller som en offentlig myndighed på anden måde er i besiddelse af over for en hvilken som helst person ([500]). I henhold til Section 67A i RIPA 2000 kan Investigatory Powers Tribunals afgørelse appelleres med forbehold af dens egen eller den relevante appeldomstols tilladelse.

(269) Endelig er det værd at bemærke, at Investigatory Powers Tribunals rolle er blevet drøftet i forbindelse med retssager ved Den Europæiske Menneskerettighedsdomstol ved flere lejligheder, navnlig i sagen *Kennedy mod Det Forenede Kongerige* ([501]) og senest i sagen *Big Brother Watch m.fl.* ([502]) mod Det Forenede Kongerige, hvor retten fastslog, at »IPT sikrede en solid klageadgang for alle med en mistanke om, at vedkommendes kommunikation var blevet aflyttet af efterretningstjenesterne« ([503]).

3.3.4.3. Andre tilgængelige klagemekanismer

(270) Som forklaret i betragtning 109 til 111 findes der også klagemuligheder i henhold til Human Rights Act 1998 og Den Europæiske Menneskerettighedsdomstol ([504]) vedrørende statens sikkerhed. Section 65(2) i RIPA 2000 giver Investigatory Powers Tribunal enekompetence i forbindelse med alle krav i Human Rights Act i forhold til efterretningsagenturerne ([505]). Dette betyder, som High Court har bemærket, at »hvorvidt der er sket en overtrædelse af HRA på grundlag af de faktiske omstændigheder i en bestemt sag, er noget, der i princippet kan rejses og afgøres af en uafhængig domstol, som kan få adgang til alt relevant materiale, herunder hemmeligt materiale. [...] Vi skal i denne forbindelse også huske på, at IPT nu selv er omfattet af muligheden for at appellere til en passende appeldomstol (i England og Wales ville dette være Court of Appeal), og at Supreme Court for nylig har afgjort, at IPT i princippet kan gøres til genstand for domstolsprøvelse: Se R (Privacy International) mod Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219« ([506]).

(271) Det følger af ovenstående, at når Det Forenede Kongeriges retshåndhævende myndigheder eller statslige sikkerhedsmyndigheder får adgang til personoplysninger, der er omfattet af denne afgørelse, er en sådan adgang underlagt love, der fastsætter betingelserne for adgang og sikrer, at adgangen til og den videre anvendelse af oplysningerne er begrænset til, hvad der er nødvendigt og står i et rimeligt forhold til det tilstræbte mål om retshåndhævelse eller statens sikkerhed. Desuden er en sådan adgang i de fleste tilfælde betinget af en forudgående tilladelse fra en retsinstans gennem godkendelse af en kendelse eller en editionskendelse og under alle omstændigheder uafhængig kontrol. Når de offentlige myndigheder har fået adgang til data, er behandlingen heraf, herunder videreformidling og videreoverførsel, omfattet af specifikke databeskyttelsesgarantier i henhold til Part 3 i DPA 2018, som afspejler dem, der er fastsat i direktiv (EU) 2016/680, med henblik på retshåndhævende myndigheders behandling og Part 4 i DPA 2018 med henblik på efterretningstjenesternes behandling. Endelig har registrerede på dette område ret til effektiv administrativ og retslig prøvelse, herunder adgang til deres oplysninger eller berigtigelse eller sletning af sådanne oplysninger.

(272) I betragtning af betydningen af sådanne betingelser, begrænsninger og garantier i forbindelse med denne afgørelse vil Kommissionen nøje overvåge anvendelsen og fortolkningen af Det Forenede Kongeriges regler om statslig adgang til oplysninger. Dette vil omfatte relevant udvikling inden for lovgivning, regulering og retspraksis samt ICO's og andre tilsynsmyndigheders aktiviteter på dette område. Der vil også blive lagt stor vægt på Det Forenede Kongeriges

([500]) Et eksempel på anvendelsen af disse beføjelser er sagen Liberty & Others mod. the Security Service, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2. Retten gav to klagere medhold, fordi deres kommunikationsdata i den ene sag blev opbevaret ud over de fastsatte frister, og i den anden fordi undersøgelsesproceduren ikke blev fulgt i henhold til GCHQ's interne regler. I den første sag pålagde retten efterretningstjenesterne at destruere de data, der blev opbevaret længere end den relevante frist. I den anden sag blev der ikke udstedt en destruktionskendelse, fordi dataene ikke blev opbevaret.

([501]) Kennedy, jf. fodnote 129.

([502]) Den Europæiske Menneskerettighedsdomstol, Big Brother Watch m.fl. mod Det Forenede Kongerige (jf. fodnote 268 ovenfor), præmis 413-415.

([503]) Den Europæiske Menneskerettighedsdomstol, Big Brother Watch, præmis 425.

([504]) Som det f.eks. fremgår af Den Europæiske Menneskerettighedsdomstols Store Afdelings nylige dom i sagen Big Brother Watch m.fl. mod Det Forenede Kongerige (se fodnote 279 ovenfor), giver dette mulighed for en effektiv domstolskontrol — i lighed med den, som EU's medlemsstater er underlagt — ved en international domstol med hensyn til offentlige myndigheders overholdelse af grundlæggende rettigheder i forbindelse med adgang til personoplysninger. Endvidere er fuldbyrdelsen af Den Europæiske Menneskerettighedsdomstols domme underlagt Europarådets specifikke tilsyn.

([505]) I sagen Belhaj & others [2017] UKSC 3 var konstateringen af, at opsnapningen af materiale, der var omfattet af fortroligheden mellem advokat og klient, var ulovlig, direkte baseret på artikel 8 i EMRK (se præmis 11).

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

gennemførelse af relevante domme fra Den Europæiske Menneskerettighedsdomstol, herunder foranstaltninger, der er angivet i de »handlingsplaner« og »handlingsrapporter«, der forelægges Ministerkomitéen i forbindelse med tilsynet med overholdelsen af Domstolens afgørelser.

4. **KONKLUSION**

(273) Kommissionen mener, at UK GDRP og DPA 2018 sikrer et beskyttelsesniveau for personoplysninger, der overføres fra Den Europæiske Union, som i det væsentlige svarer til det, der er garanteret ved forordning (EU) 2016/679.

(274) Kommissionen finder desuden ud fra en samlet betragtning, at kontrolmekanismerne og domstolsadgangen i det Forenede Kongerige i praksis gør det muligt at identificere og sanktionere overtrædelser, og at de sikrer den registrerede retsmidler til at opnå adgang til personoplysninger, som vedrører den pågældende, og til efterfølgende at få sådanne oplysninger berigtiget eller slettet.

(275) Endelig finder Kommissionen på grundlag af de tilgængelige oplysninger om Det Forenede Kongeriges retsorden, at ethvert indgreb i de grundlæggende rettigheder for de personer, hvis personoplysninger overføres fra Den Europæiske Union til Det Forenede Kongerige af Det Forenede Kongeriges offentlige myndigheder af hensyn til den offentlige interesse, navnlig retshåndhævelse og statens sikkerhed, vil være begrænset til, hvad der er strengt nødvendigt for at nå det pågældende legitime mål, og at der findes en effektiv retsbeskyttelse mod et sådant indgreb.

(276) I lyset af konklusionerne i denne afgørelse bør det derfor besluttes, at Det Forenede Kongerige sikrer et tilstrækkeligt beskyttelsesniveau som omhandlet i artikel 45 i forordning (EU) 2016/679, fortolket i lyset af Den Europæiske Unions charter om grundlæggende rettigheder.

(277) Denne konklusion er baseret på både den relevante nationale ordning i Det Forenede Kongerige og dets internationale forpligtelser, navnlig overholdelsen af den europæiske menneskerettighedskonvention og Den Europæiske Menneskerettighedsdomstols jurisdiktion. Fortsat overholdelse af sådanne internationale forpligtelser er derfor et særligt vigtigt element i den vurdering, som denne afgørelse er baseret på.

5. **VIRKNINGERNE AF DENNE AFGØRELSE OG DATABESKYTTELSESMYNDIGHEDERNES HANDLINGER**

(278) Medlemsstaterne og deres organer er forpligtet til at træffe de nødvendige foranstaltninger for at efterkomme EU-institutionernes retsakter, idet sidstnævnte formodes at være lovlige og derfor afføder retsvirkninger, indtil de udløber, trækkes tilbage, annulleres som følge af et annullationssøgsmål eller erklæres ugyldige som følge af en præjudiciel forelæggelse eller en ulovlighedsindsigelse.

(279) En afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 er således bindende for alle de organer i medlemsstaterne, som den er rettet til, herunder deres uafhængige tilsynsmyndigheder. I denne afgørelses gyldighedsperiode kan overførsler fra en dataansvarlig eller databehandler i Den Europæiske Union til dataansvarlige eller databehandlere i Det Forenede Kongerige finde sted uden yderligere godkendelse.

(280) Det bør bemærkes, at i henhold til artikel 58, stk. 5, i forordning (EU) 2016/679, og som Domstolen forklarede i *Schrems*-dommen ([507]), skal den nationale lovgivning, når en national databeskyttelsesmyndighed, herunder efter en klage, sætter spørgsmålstegn ved, om en afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet er forenelig med den enkeltes grundlæggende ret til privatlivets fred og databeskyttelse, giver den pågældende mulighed for at indbringe disse indsigelser for en national domstol, som kan være forpligtet til at forelægge Domstolen et præjudicielt spørgsmål ([508]).

([507]) Schrems-sagen, præmis 65.

([508]) Schrems-sagen, præmis 65: »I denne henseende påhviler det den nationale lovgiver at tilvejebringe retsmidler, der gør det muligt for den pågældende nationale tilsynsmyndighed at indbringe de klagepunkter, som den finder begrundede, for de nationale domstole, således at disse, såfremt de deler myndighedens tvivl vedrørende gyldigheden af Kommissionens afgørelse, kan foretage en præjudiciel forelæggelse med henblik på en efterprøvelse af denne afgørelses gyldighed.«

6. OVERVÅGNING, SUSPENSION, OPHÆVELSE ELLER ÆNDRING AF DENNE AFGØRELSE

(281) I henhold til artikel 45, stk. 4, i forordning (EU) 2016/679 skal Kommissionen løbende overvåge den relevante udvikling i Det Forenede Kongerige efter vedtagelsen af denne afgørelse for at vurdere, om den stadig sikrer et i det væsentlige tilsvarende beskyttelsesniveau. En sådan overvågning er særlig vigtig i dette tilfælde, da Det Forenede Kongerige vil forvalte, anvende og håndhæve en ny databeskyttelsesordning, som ikke længere er underlagt EU-retten og muligvis kan udvikle sig. I den forbindelse vil der blive lagt særlig vægt på den praktiske anvendelse af Det Forenede Kongeriges regler om overførsel af personoplysninger til tredjelande og den indvirkning, det kan have på beskyttelsesniveauet for oplysninger, der overføres i henhold til denne afgørelse, effektiviteten af udøvelsen af individuelle rettigheder, herunder enhver relevant udvikling inden for lovgivning og praksis vedrørende undtagelser fra eller begrænsninger af sådanne rettigheder (navnlig den undtagelse, der vedrører opretholdelse af en effektiv indvandringskontrol), samt overholdelse af begrænsningerne og garantierne med hensyn til statslig adgang. Blandt andre elementer vil udviklingen i retspraksis og ICO's og andre uafhængige organers tilsyn danne grundlag for Kommissionens tilsyn.

(282) For at lette dette tilsyn bør Det Forenede Kongeriges myndigheder straks underrette Kommissionen om enhver væsentlig ændring af Det Forenede Kongeriges retsorden, som har indvirkning på den retlige ramme, der er genstand for denne afgørelse, samt enhver udvikling i praksis i forbindelse med behandling af personoplysninger, der vurderes i denne afgørelse, både hvad angår dataansvarliges og databehandleres behandling af personoplysninger i henhold til UK GDPR og de begrænsninger og garantier, der gælder for offentlige myndigheders adgang til personoplysninger. Dette bør omfatte udviklingen med hensyn til de elementer, der er nævnt i betragtning 281.

(283) For at gøre det muligt for Kommissionen at udøve sin overvågningsfunktion effektivt bør medlemsstaterne desuden underrette Kommissionen om alle relevante foranstaltninger, der træffes af de nationale databeskyttelsesmyndigheder, navnlig vedrørende forespørgsler eller klager fra registrerede i EU vedrørende overførsel af personoplysninger fra Unionen til dataansvarlige eller databehandlere i Det Forenede Kongerige. Kommissionen bør også underrettes om eventuelle indikationer på, at Det Forenede Kongeriges myndigheder med ansvar for forebyggelse, efterforskning, afsløring og retsforfølgelse på det strafferetlige område eller for statens sikkerhed, herunder alle tilsynsmyndigheder, handler på en måde, der ikke sikrer det krævede beskyttelsesniveau.

(284) Hvis tilgængelige oplysninger, navnlig oplysninger fra overvågningen af denne afgørelse eller fra Det Forenede Kongeriges eller medlemsstaternes myndigheder, viser, at det beskyttelsesniveau, som Det Forenede Kongerige yder, måske ikke længere er tilstrækkeligt, bør Kommissionen straks underrette de kompetente myndigheder i Det Forenede Kongerige herom og anmode om, at der træffes passende foranstaltninger inden for en nærmere fastsat tidsramme, som ikke må overstige tre måneder. Denne periode kan om nødvendigt forlænges med et nærmere fastsat tidsrum under hensyntagen til arten af det pågældende spørgsmål og/eller de foranstaltninger, der skal træffes. En sådan procedure vil f.eks. blive udløst i tilfælde, hvor videreoverførsler, herunder på grundlag af nye bestemmelser om tilstrækkeligheden af beskyttelsesniveauet vedtaget af Secretary of State eller internationale aftaler indgået af Det Forenede Kongerige, ikke længere gennemføres under garantier, der sikrer kontinuitet i beskyttelsen som omhandlet i artikel 44 i forordning (EU) 2016/679.

(285) Hvis Det Forenede Kongeriges kompetente myndigheder ved udløbet af den fastsatte tidsramme ikke træffer disse foranstaltninger eller på anden måde på tilfredsstillende vis godtgør, at denne afgørelse fortsat er baseret på et passende beskyttelsesniveau, indleder Kommissionen proceduren i artikel 93, stk. 2, i forordning (EU) 2016/679 med henblik på helt eller delvis at suspendere eller ophæve denne afgørelse.

(286) Alternativt vil Kommissionen indlede denne procedure med henblik på at ændre afgørelsen, navnlig ved at underkaste dataoverførsler yderligere betingelser eller ved at begrænse omfanget af konstateringen af et tilstrækkeligt beskyttelsesniveau til kun at omfatte dataoverførsler, for hvilke der fortsat sikres et tilstrækkeligt beskyttelsesniveau.

(287) I behørigt begrundede særligt hastende tilfælde vil Kommissionen gøre brug af muligheden for efter proceduren i artikel 93, stk. 3, i forordning (EU) 2016/679 at vedtage gennemførelsesretsakter, der finder anvendelse straks, og som suspenderer, ophæver eller ændrer afgørelsen.

7. VARIGHED OG FORLÆNGELSE AF DENNE AFGØRELSE

(288) Kommissionen bør tage i betragtning, at Det Forenede Kongerige med udløbet af den overgangsperiode, der er fastsat i udtrædelsesaftalen, og så snart den midlertidige bestemmelse i artikel 782 i handels- og samarbejdsaftalen mellem EU og Det Forenede Kongerige ophører med at finde anvendelse, vil forvalte, anvende og håndhæve en ny databeskyttelsesordning, der kan sammenlignes med den, der var gældende, da landet var bundet af EU-retten. Dette kan navnlig indebære ændringer eller ændringer af den databeskyttelsesramme, der vurderes i denne afgørelse, samt andre relevante udviklinger.

(289) Det bør derfor fastsættes, at denne afgørelse finder anvendelse i en periode på fire år fra dens ikrafttræden.

(290) Hvis navnlig oplysninger som følge af overvågningen af denne afgørelse viser, at konklusionerne vedrørende tilstrækkeligheden af det beskyttelsesniveau, der sikres i Det Forenede Kongerige, stadig er faktuelt og retligt begrundede, bør Kommissionen senest seks måneder inden denne afgørelses ophør indlede proceduren for ændring af denne afgørelse ved i princippet at forlænge dens gyldighedsperiode med yderligere fire år. En sådan gennemførelsesretsakt om ændring af denne afgørelse skal vedtages efter proceduren i artikel 93, stk. 2, i direktiv (EU) 2016/679.

8. **AFSLUTTENDE BETRAGTNINGER**

(291) Det Europæiske Databeskyttelsesråd har offentliggjort sin udtalelse ([509]), som er blevet taget i betragtning ved udarbejdelsen af denne afgørelse.

(292) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 93 i forordning (EU) 2016/679 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

1. Med henblik på artikel 45 i forordning (EU) 2016/679 sikrer Det Forenede Kongerige et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres inden for rammerne af forordning (EU) 2016/679 fra Den Europæiske Union til Det Forenede Kongerige.

2. Denne afgørelse vedrører ikke personoplysninger, der videregives med henblik på indvandringskontrol i Det Forenede Kongerige, eller som på anden måde falder ind under anvendelsesområdet for undtagelsen fra visse registreredes rettigheder med henblik på opretholdelse af en effektiv indvandringskontrol i henhold til paragraph 4(1) i Schedule 2 til DPA 2018.

Artikel 2

Når de kompetente tilsynsmyndigheder i medlemsstaterne med henblik på at beskytte fysiske personer i forbindelse med behandling af deres personoplysninger udøver deres beføjelser i henhold til artikel 58 i forordning (EU) 2016/679 med hensyn til videregivelse af oplysninger, der er omfattet af anvendelsesområdet i artikel 1, underretter den berørte medlemsstat straks Kommissionen herom.

Artikel 3

1. Kommissionen overvåger løbende anvendelsen af den retlige ramme, som denne afgørelse er baseret på, herunder betingelserne for videreoverførsel, udøvelse af individuelle rettigheder og Det Forenede Kongeriges offentlige myndigheders adgang til oplysninger, der overføres på baggrund af denne afgørelse, med henblik på at vurdere, om Det Forenede Kongerige fortsat sikrer et tilstrækkeligt beskyttelsesniveau i henhold til artikel 1.

2. Medlemsstaterne og Kommissionen underretter hinanden om tilfælde, hvor Information Commissioner eller en anden kompetent myndighed i Det Forenede Kongerige ikke sikrer overholdelse af den retlige ramme, som denne afgørelse er baseret på.

3. Medlemsstaterne og Kommissionen underretter hinanden, hvis der er tegn på, at Det Forenede Kongeriges myndigheders indgriben i den enkeltes ret til beskyttelse af sine personoplysninger går videre, end hvad der er strengt nødvendigt, eller på, at der ikke er en effektiv retsbeskyttelse mod sådanne indgreb.

4. Hvis Kommissionen ser tegn på, at et tilstrækkeligt beskyttelsesniveau ikke længere er sikret, underretter Kommissionen de kompetente myndigheder i Det Forenede Kongerige herom og kan suspendere, ophæve eller ændre denne afgørelse.

([509]) Udtalelse 14/2021 om Kommissionens udkast til gennemførelsesafgørelse i henhold til forordning (EU) 2016/679 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Det Forenede Kongerige, som findes på følgende link: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Kommissionen kan suspendere, ophæve eller ændre denne afgørelse, hvis Det Forenede Kongeriges regerings manglende samarbejdsvilje forhindrer Kommissionen i at afgøre, om konklusionen i artikel 1, stk. 1, er berørt.

Artikel 4

Denne afgørelse udløber den 27. juni 2025, medmindre den forlænges efter proceduren i artikel 93, stk. 2, i forordning (EU) 2016/679.

Artikel 5

Denne afgørelse er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 28. juni 2021.

På Kommissionens vegne
Didier REYNDERS
Medlem af Kommissionen