KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2021/1773

af 28. juni 2021

i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2016/680 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Det Forenede Kongerige

(meddelt under nummer C(2021) 4801)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til 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 ([1]), særlig artikel 36, stk. 3, og

ud fra følgende betragtninger:

1. INDLEDNING

(1) I Europa-Parlamentets og Rådets direktiv (EU) 2016/680 fastsættes regler for overførsel af personoplysninger fra kompetente myndigheder i Unionen til tredjelande og internationale organisationer, i det omfang sådanne overførsler falder ind under dets anvendelsesområde. Reglerne om kompetente myndigheders internationale overførsler af oplysninger er fastsat i kapitel V i direktiv (EU) 2016/680, nærmere bestemt i artikel 35-40. Selv om strømmen af personoplysninger til og fra lande uden for Den Europæiske Union er afgørende for et effektivt retshåndhævelsessamarbejde, skal det sikres, at beskyttelsesniveauet for personoplysninger i Den Europæiske Union ikke undermineres af sådanne overførsler ([2]).

(2) I henhold til artikel 36, stk. 3, i direktiv (EU) 2016/680 kan Kommissionen i form af en gennemførelsesretsakt beslutte, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland eller en international organisation har et tilstrækkeligt beskyttelsesniveau. På denne betingelse kan overførsler af personoplysninger til et tredjeland finde sted uden yderligere tilladelse (bortset fra tilfælde, hvor en anden medlemsstat, hvorfra oplysningerne er indsamlet, skal give sin tilladelse til overførslen), jf. artikel 35, stk. 1, og betragtning 66 i direktiv (EU) 2016/680.

(3) Som anført i artikel 36, stk. 2, i direktiv (EU) 2016/680 skal vedtagelsen af en afgørelse om beskyttelsesniveauets tilstrækkelighed baseres på en omfattende analyse af tredjelandets retsorden. I sin vurdering skal Kommissionen afgøre, om det pågældende tredjeland giver garantier, der sikrer et beskyttelsesniveau, som »i det væsentlige svarer til« det, der sikres i Den Europæiske Union (betragtning 67 i direktiv (EU) 2016/680). Den standard, som den »væsentlige ækvivalens« vurderes i forhold til, er den, der er fastsat i EU-lovgivningen, navnlig direktiv (EU) 2016/680, samt Den Europæiske Unions Domstols retspraksis ([3]). Det Europæiske Databeskyttelsesråds reference vedrørende et tilstrækkeligt beskyttelsesniveau er også af betydning i denne henseende ([4]).

(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 anvendes 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 kopieres punkt for punkt. Testen består snarere i, om det udenlandske system som helhed på grundlag af indholdet af rettigheder vedrørende privatlivets fred og gennem effektiv gennemførelse, overvågning og håndhævelse heraf sikrer det krævede beskyttelsesniveau ([7]).

([1]) EUT L 119 af 4.5 2016, s. 89.
([2]) Se betragtning 64 i direktiv (EU) 2016/680.
([3]) Se senest sag C-311/18, *Maximilian Schrems mod Data Protection Commissioner* (»*Schrems II*«), ECLI:EU:C:2020:559.
([4]) Se henstilling 01/2021 om henvisning til tilstrækkelighed i henhold til direktivet om retshåndhævelse, som blev vedtaget i februar 2021 og kan findes på følgende link: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_da
([5]) Sag C-362/14, *Maximilian Schrems mod Data Protection Commissioner* (»Schrems«), ECLI:EU:C:2015:650, præmis 73.
([6]) *Schrems*, præmis 74.
([7]) 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, findes på følgende link: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52017DC0007&from=EN).

(5) Kommissionen har nøje analyseret den relevante lovgivning og praksis i Det Forenede Kongerige (UK). På grundlag af nedenstående konklusioner konstaterer Kommissionen, at Det Forenede Kongerige sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres af kompetente myndigheder i Unionen og er omfattet af direktiv (EU) 2016/680, til kompetente myndigheder i Det Forenede Kongerige, der er omfattet af Part 3 i Data Protection Act 2018 (DPA 2018) (lov om databeskyttelse af 2018) ([8]).

(6) Det fastsættes ved denne afgørelse, at sådanne overførsler kan finde sted for en periode på fire år, uden at der behøves yderligere tilladelser med forbehold af en eventuel forlængelse, jf. dog betingelserne i artikel 35 i direktiv (EU) 2016/680.

2. REGLER FOR KOMPETENTE MYNDIGHEDERS BEHANDLING AF PERSONOPLYSNINGER MED HENBLIK PÅ STRAFFERETLIG HÅNDHÆVELSE

2.1. De forfatningsmæssige rammer

(7) Det Forenede Kongerige er et parlamentarisk demokrati. Det har et suverænt parlament, som står over alle andre regeringsinstitutioner, en udøvende magt, der udgår fra og er ansvarlig over for parlamentet, og et uafhængigt retsvæsen. Den udøvende magts myndighed følger af dens evne til at opnå det valgte Underhus' tillid, og den er ansvarlig over for begge kamre i parlamentet (Underhuset og Overhuset), som har ansvar for at kontrollere regeringen og drøfte og vedtage love. Det Forenede Kongeriges parlament har overdraget ansvaret for lovgivning om visse nationale anliggender i Skotland, Wales og Nordirland til henholdsvis det skotske parlament, det walisiske parlament (Senedd Cymru) og Nordirlands parlament. Selv om databeskyttelse er et anliggende, der er forbeholdt Det Forenede Kongeriges parlament, dvs. at den samme lovgivning finder anvendelse i hele landet, er andre politikområder af relevans for denne afgørelse blevet decentraliseret. F.eks. er strafferetssystemerne, herunder politiets aktiviteter i Skotland og Nordirland, overdraget til henholdsvis det skotske parlament og Nordirlands parlament ([9]).

(8) Selv om Det Forenede Kongerige ikke har en kodificeret forfatning i form af et permanent, konstituerende dokument, har landets forfatningsmæssige principper udviklet sig over tid, navnlig på grundlag af retspraksis og konventioner. Den forfatningsmæssige værdi af visse love, såsom Magna Carta, Bill of Rights 1689 (rettighedslov) og Human Rights Act 1998 (menneskerettighedslov), er blevet anerkendt. Den enkeltes grundlæggende rettigheder er som en del af forfatningen blevet udviklet gennem sædvaneret, 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]).

(9) Human Rights Act 1998 indarbejder rettighederne fra EMRK i Det Forenede Kongeriges lovgivning. Loven indrømmer enhver person de grundlæggende rettigheder og frihedsrettigheder, der er fastsat i EMRK's artikel 2-12 og 14 samt i artikel 1-3 i den første protokol og i artikel 1 i den trettende protokol hertil, sammenholdt med EMRK's artikel 16-18. Dette omfatter retten til respekt for privatliv og familieliv, hvilket igen omfatter retten til databeskyttelse og retten til en retfærdig rettergang ([11]). I henhold til EMRK's artikel 8 må en offentlig myndighed navnlig kun lovmedholdeligt gribe ind i retten til privatlivets fred, 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 forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og frihedsrettigheder.

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

([9]) UK Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement, som kan findes på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Principperne i konvention 108 er oprindelig gennemført i Det Forenede Kongeriges lovgivning gennem Data Protection Act fra 1984, som blev erstattet af DPA 1998 og senere DPA 2018 (sammenholdt med UK GDPR, Det Forenede Kongeriges databeskyttelseslov). I 2018 undertegnede Det Forenede Kongerige desuden protokollen om ændring af konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (betegnet konvention 108+), og der arbejdes i øjeblikket på ratificeringen af konventionen.

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

(10) I henhold til Human Rights Act 1998 skal enhver handling fra offentlige myndigheders side være forenelig med en rettighed, der er sikret ved EMRK ([12]). Desuden skal primær og underordnet lovgivning fortolkes og gennemføres på en måde, der er forenelig med disse rettigheder ([13]). Hvis en person mener, at hans eller hendes rettigheder, herunder retten til privatlivets fred og databeskyttelse, er blevet krænket af offentlige myndigheder, kan vedkommende opnå erstatning ved de britiske domstole i henhold til Human Rights Act 1998 og i sidste instans, når de nationale retsmidler er udtømt, indbringe sagen for Den Europæiske Menneskerettighedsdomstol for krænkelser af de rettigheder, der er garanteret i henhold til EMRK.

2.2. **Det Forenede Kongeriges databeskyttelsesrammer**

(11) 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. Inden udtrædelsen og i overgangsperioden bestod de lovgivningsmæssige rammer for beskyttelse af personoplysninger i Det Forenede Kongerige, for så vidt angår kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed, af relevante dele af Data Protection Act 2018, som gennemførte direktiv (EU) 2016/680.

(12) Som forberedelse til udtrædelsen af EU vedtog Det Forenede Kongeriges regering European Union (Withdrawal) Act 2018 (EUWA) (lov om udtrædelse af Den Europæiske Union) ([15]), som indarbejdede umiddelbart gældende EU-lovgivning i Det Forenede Kongeriges lovgivning og bestemte, at den såkaldte »EU-afledte nationale lovgivning« fortsat har virkning efter overgangsperiodens udløb. Part 3 i DPA 2018 ([16]), som gennemfører direktiv (EU) 2016/680 i national lovgivning, udgør »afledt EU-lovgivning« i henhold til EUWA. I overensstemmelse med EUWA skal den uændrede nationale lovgivning, der er afledt af EU-retten, fortolkes af domstolene i Det Forenede Kongerige i overensstemmelse med den relevante retspraksis fra Den Europæiske Unions Domstol (EU-Domstolen) og de generelle principper i EU-retten, således som de havde virkning umiddelbart inden overgangsperiodens udløb (benævnt henholdsvis »bibeholdt EU-retspraksis« og »bibeholdte generelle principper fra EU-retten«) ([17]).

(13) I henhold til EUWA har Det Forenede Kongeriges ministre beføjelse til at indføre afledt ret via bekendtgørelser med henblik på at indføre de nødvendige ændringer i den bibeholdte EU-ret, der følger af Det Forenede Kongeriges udtræden af Unionen. Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations) ([18]) er et resultat af denne beføjelse. Disse love ændrer den britiske databeskyttelseslovgivning, herunder DPA 2018, så den passer til den nationale kontekst ([19]).

([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 (»udtrædelsesaftalen«), der findes på følgende link: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=DA.
([15]) European Union (Withdrawal) Act 2018, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2018/16/contents
([16]) Data Protection Act 2018, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2018/12/contents
([17]) Section 6 i EUWA 2018.
([18]) 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 2020, der findes på følgende link: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.
([19]) Disse Exit Regulations indeholder en række ændringer af Part 3 i DPA 2018. Mange af dem er tekniske ændringer, f.eks. fjernelse af henvisninger til »medlemsstat« eller erstatning af »retshåndhævelsesdirektivet« (se f.eks. Section 48(8) eller Section 73(5)(a)) i DPA 2018 med »national lovgivning«, således at Part 3 fungerer effektivt som national lovgivning efter overgangsperiodens udløb. Nogle steder var der behov for andre typer ændringer, f.eks. med hensyn til »hvem« der vedtager »afgørelser om beskyttelsesniveauets tilstrækkelighed« med henblik på Det Forenede Kongeriges retlige databeskyttelsesrammer (se Section 74A i DPA 2018), dvs. Secretary of State (indenrigsministeren) i stedet for Europa-Kommissionen.

(14) De retlige standarder for kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, opdage eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed i Det Forenede Kongerige efter overgangsperioden i henhold til udtrædelsesaftalen, vil derfor blive bibeholdt i relevante dele af DPA 2018, men som ændret ved DPPEC-lovene, navnlig i Part 3 i nævnte lov. United Kingdom General Data Protection Regulation (UK GDPR) finder ikke anvendelse på denne form for behandling.

(15) Part 3 i DPA 2018 indeholder regler for behandling af personoplysninger med henblik på strafferetlig håndhævelse, herunder databeskyttelsesprincipper, retsgrundlag for behandling (lovlighed), de registreredes rettigheder, de kompetente myndigheders forpligtelser som dataansvarlige og begrænsninger for videreoverførsel. Samtidig findes de gældende regler om kontrol, håndhævelse og klageadgang i retshåndhævelsessektoren i Part 5 og 6 i DPA 2018.

(16) Desuden bør der i lyset af politistyrkernes relevante rolle i retshåndhævelsessektoren tages hensyn til reglerne for politiarbejde. Da politiarbejde er et decentralt anliggende, finder forskellige retsakter, hvis indhold dog ofte ligner hinanden, anvendelse på politiarbejdet i a) England og Wales, b) Skotland og c) Nordirland ([20]). Desuden indeholder forskellige typer vejledninger yderligere præciseringer af, hvordan politiets beføjelser bør anvendes. Der findes tre hovedformer for politivejledning: 1) lovbestemt vejledning udstedt i henhold til lovgivning såsom Code of Ethics (etiske regler) ([21]) og Code of Practice on the Management of Police Information (MoPI Code of Practice) (adfærdskodeks for forvaltning af politioplysninger)) ([22]) udstedt i henhold til Police Act 1996 (politiloven af 1996) ([23]) eller PACE Codes ([24]) udstedt i henhold til Police and Criminal Evidence Act (lov om politiets og strafferettens bevismateriale) ([25]), 2) Authorised Professional Practice on the Management of Police Information (APP Guidance on the Management of Police Information) (autoriseret vejledning i forvaltning af politioplysninger, APP)) ([26]) udarbejdet af College of Policing (politiakademiet) og 3) operationel vejledning (offentliggjort af politiet selv). National Police Chiefs Council (det nationale politichefråd, et koordinerende organ for alle britiske politistyrker) offentliggør operationelle retningslinjer, som alle politistyrker har godkendt, og som derfor finder anvendelse på nationalt plan ([27]). Formålet med denne vejledning er at sikre sammenhæng i politistyrkernes behandling af information ([28]).

(17) MoPI Code of Practice blev udstedt af Secretary of State i 2005 i medfør af de beføjelser, der er fastsat i Section 39A i Police Act 1996 ([29]). Enhver adfærdskodeks, der udstedes i henhold til Police Act, skal godkendes af Secretary of State og er genstand for en høring i National Crime Agency (det nationale kontor for kriminalitet), inden den forelægges parlamentet. I henhold til Section 39A(7) i Police Act skal politiet tage behørigt hensyn til kodekser udstedt i

([20]) En mere detaljeret redegørelse for politistyrkerne og deres beføjelser i Det Forenede Kongerige findes i: UK Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement (se fodnote 9).

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

([22]) Code of Practice on the Management of Police Information, der findes på følgende link: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) Police Act 1996, der findes på følgende link: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Police and Criminal Evidence Act 1984 (PACE) med adfærdskodekser, som kan findes på følgende link: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) Police and Criminal Evidence Act 1984, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Authorised Professional Practice on the Management of Police Information, der findes på følgende link: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Data Protection Manual for Police Data Protection Professionals, som kan findes på følgende link: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) F.eks. finder MoPI Code of Practice (se fodnote 22) anvendelse på opbevaring af operationelle politioplysninger (se betragtning (47) i denne afgørelse).

([29]) Ifølge oplysningerne fra de britiske myndigheder var College of Policing i den periode, hvor drøftelserne om beskyttelsesniveauets tilstrækkelighed fandt sted, i færd med at udarbejde en Information and Records Management Code of Practice til erstatning for MoPI. Udkastet til kodeksen blev offentliggjort til offentlig høring den 25. januar 2021 og findes på følgende link: https://beta.college.police.uk/article/information-records-management-consultation. https://www.college.police.uk/article/information-records-management-consultation

henhold til loven, og politiet forventes derfor at overholde sådanne ([30]). Desuden skal en ikke-lovfæstet vejledning (såsom APP Guidance on the Management of Police Information) altid være i overensstemmelse med MoPI Code of Practice, som har forrang for den ([31]). Selv om der kan være visse konkrete situationer, hvor politiet er nødt til at afvige fra denne vejledning, er de under alle omstændigheder stadig forpligtet til at overholde kravene i Part 3 i DPA 2018 ([32]).

(18) Yderligere vejledning om Det Forenede Kongeriges databeskyttelseslovgivning for behandling i retshåndhævelsessektoren gives af Information Commissioner (»Information Commissioner« eller »ICO«) ([33]) (yderligere oplysninger om ICO findes i betragtning (93) til (109)). Selv om vejledningen ikke er juridisk bindende, vil domstolene i en retssag være forpligtede til at tage hensyn til enhver overtrædelse af den, da den har fortolkningsmæssig betydning og viser, hvordan databeskyttelseslovgivningen fortolkes og håndhæves af Information Commissioner i praksis ([34]).

(19) Endelig skal de britiske retshåndhævende myndigheder som nævnt i betragtning (8)-(10) sikre overholdelse af EMRK og konvention 108.

(20) Med hensyn til struktur og hovedelementer er den retlige ramme for britiske strafferetlige myndigheders behandling af oplysninger således meget lig den, der gælder i EU. Dette vil blandt andet sige, at en sådan ramme ikke kun er baseret på forpligtelser, der er fastsat i national ret, 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, samt at den er underlagt Den Europæiske Menneskerettighedsdomstols jurisdiktion. Disse forpligtelser, der følger af retligt bindende internationale instrumenter, navnlig vedrørende beskyttelse af personoplysninger, er derfor et særligt vigtigt element i den retlige ramme, der vurderes i denne afgørelse.

2.3. **Materielt og territorialt anvendelsesområde**

(21) Det materielle anvendelsesområde for DPA 2018, Part 3, falder sammen med anvendelsesområdet for direktiv 2016/680 som præciseret i direktivets artikel 2, stk. 2. Part 3 finder anvendelse på en kompetent myndigheds behandling af personoplysninger, der helt eller delvist sker automatisk, og en kompetent myndigheds behandling på anden måde end ved hjælp af elektronisk databehandling af personoplysninger, der er eller vil blive lagret i et register.

(22) For at falde ind under anvendelsesområdet for Part 3 skal den dataansvarlige desuden være en »kompetent myndighed«, og behandlingen skal foretages med henblik på retshåndhævelse. Den databeskyttelsesordning, der vurderes i denne afgørelse, finder derfor anvendelse på alle disse kompetente myndigheders retshåndhævelsesaktiviteter.

(23) 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. 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), Welsh Revenue Authority (Wales' afgiftsmyndighed), Competition and Markets Authority (konkurrence- og markedsmyndigheden) eller Her Majesty's Land Register (ejendomsregistret)), anklagemyndigheder, andre strafferetlige

([30]) I sag R mod Commission of Police of the Metropolis [2014] EWCA Civ 585 blev den retlige status for MoPI Code of Practice bekræftet, og Lord Justice Laws erklærede, at Metropolitan Police Commissioner er forpligtet til at tage hensyn til MoPI Code of Practice og APP Guidance on Management of Police Information i henhold til Section 39A i Police Act 1996.

([31]) Politiets overholdelse af MoPI Code of Practice kontrolleres af Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS).

([32]) Se i denne forbindelse udtalelsen fra College of Policing om overholdelse af APP-vejledningen om alle aspekter af politiarbejde, hvoraf det fremgår, at APP er godkendt af det professionelle politikorps (College of Policing) som den officielle kilde til professionel praksis for politiarbejde. Betjente og personale forventes at tage hensyn til APP i forbindelse med varetagelsen af deres opgaver. Der kan dog være situationer, hvor der er en legitim operationel grund til, at en styrke afviger fra APP, forudsat at der er en klar begrundelse herfor. Det er op til styrken at bære ansvaret for enhver lokal og national risiko for at operere uden for nationalt fastsatte retningslinjer, og hvis en hændelse indtræffer, eller der skal foretages en efterforskning som følge heraf (f.eks. af Independent Office of Police Conduct (den uafhængige politianklagemyndighed)), er styrken ansvarlig for enhver risiko. Udtalelsen findes på følgende link: https://www.app.college.police.uk/faq-page/

([33]) Guide to Law Enforcement Processing findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Se sag *Bridges mod Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), hvor High Court, selv om den bemærkede, at Information Commissioners vejledning ikke er lovfæstet, fastslog, at hvis en dataansvarlig har opfyldt forpligtelsen i henhold til Section 64 [til at foretage en konsekvensanalyse vedrørende databeskyttelse i forbindelse med behandling af høj risiko], vil en domstol tage hensyn til den vejledning, som er udstedt af Information Commissioner med hensyn til konsekvensanalyser vedrørende databeskyttelse.

myndigheder og tilsvarende eller organisationer, der udfører retshåndhævelsesaktiviteter ([35]). Part 3 i DPA 2018 finder også anvendelse på retter og domstole, når de udøver deres judicielle funktioner, bortset fra den del, der vedrører den registreredes rettigheder og Information Commissioner's kontrol ([36]). Listen over kompetente myndigheder i Schedule 7 er ikke endelig og kan ajourføres af Secretary of State ved Regulations under hensyntagen til ændringerne i tilrettelæggelsen af offentlige kontorer ([37]).

(24) Den pågældende behandling skal også have et »retshåndhævelsesformål«, der defineres som forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed ([38]). En kompetent myndigheds behandling er ikke omfattet af Part 3 i DPA 2018, hvis den ikke har et retshåndhævelsesformål. Dette vil f.eks. være tilfældet, når Competition and Markets Authority undersøger sager, der ikke er strafbare (f.eks. fusioner mellem virksomheder). I så fald vil UK GDPR og Part 2 i DPA 2018 finde anvendelse, da de kompetente myndigheders behandling af personoplysninger foretages til andre formål end retshåndhævelsesformål. For at afgøre, hvilken databeskyttelsesordning der finder anvendelse (Part 3 eller Part 2 i DPA 2018) på behandlingen af personoplysninger, skal den kompetente myndighed, dvs. den dataansvarlige, overveje, om det »primære formål« med en sådan behandling er et af retshåndhævelsesformålene i henhold til DPA 2018.

(25) Hvad angår det territoriale anvendelsesområde for Part 3 i DPA 2018, bestemmes det i Section 207(2), at DPA finder anvendelse på behandling af personoplysninger i forbindelse med aktiviteter, der udføres af en person, som har et forretningssted i hele Det Forenede Kongeriges område. Dette omfatter offentlige myndigheder i England, Wales, Skotland og Nordirland, som er omfattet af det materielle anvendelsesområde for Part 3 i DPA 2018 ([39]).

2.3.1. *Definition af personoplysninger og behandling*

(26) Nøglebegreberne personoplysninger og behandling er defineret i Section 3 i DPA 2018 og gælder i hele DPA. Definitionerne følger nøje de tilsvarende definitioner i artikel 3 i direktiv 2016/680. I henhold til DPA 2018 forstås ved personoplysninger enhver form for oplysning om en identificeret eller identificerbar levende person ([40]). I henhold til Section 3(3) i DPA 2018 kan en person identificeres, hvis vedkommende direkte eller indirekte kan identificeres ud fra oplysningerne, herunder ved henvisning til et navn eller en identifikator eller ved henvisning til et eller flere elementer, der er særlige for personens fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet. Ved »behandling« forstås en eller flere operationer, der udføres på grundlag af oplysninger eller sæt af oplysninger, såsom a) indsamling, registrering, organisering, strukturering eller opbevaring, b) tilpasning eller ændring, c) udtræk, konsultation eller brug, d) offentliggørelse ved videregivelse, formidling eller tilgængeliggørelse på anden vis, e) justering eller kombination eller f) begrænsning, sletning eller tilintetgørelse. Desuden forstås ved »følsom behandling« i loven a) behandling af personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, b) behandling af genetiske eller biometriske data med det formål entydigt at identificere en fysisk person, c) behandling af helbredsoplysninger, d) behandling af oplysninger om en persons seksuelle forhold eller seksuelle orientering ([41]). I den forbindelse indeholder Section 205 i DPA 2018 en definition af »biometriske data« ([42]), »helbredsoplysninger ([43])« og »genetiske data« ([44]).

([35]) 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.

([36]) Section 43(3) i DPA 2018.

([37]) Section 30(3) i DPA 2018. Efterretningstjenesterne (Secret Intelligence Service, Security Service og Government Communications Headquarters) er ikke kompetente myndigheder (se også Section 30(2) i DPA 2018), og Part 3 i DPA 2018 finder ikke anvendelse på deres aktiviteter. Deres aktiviteter er omfattet af Part 4 i DPA 2018.

([38]) Section 31 i DPA 2018.

([39]) Det betyder, at DPA 2018 og derfor også denne afgørelse ikke finder anvendelse på de territorier, der hører under den britiske krone, og andre af Det Forenede Kongeriges oversøiske territorier såsom f.eks. Falklandsøerne og Gibraltar.

([40]) personoplysninger vedrørende afdøde falder ikke ind under DPA 2018.

([41]) Section 35(8) i DPA 2018.

([42]) »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.

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

([44]) »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.

(27) I Section 32 i DPA 2018 præciseres definitionerne af »dataansvarlig« og »databehandler« i forbindelse med behandling af personoplysninger med henblik på retshåndhævelse, der nøje følger de tilsvarende definitioner i direktiv 2016/680. Den dataansvarlige er den kompetente myndighed, som afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. Hvis behandlingen er påkrævet i henhold til lovgivningen, er den dataansvarlige den kompetente myndighed, som denne lov pålægger en sådan forpligtelse. En databehandler defineres som enhver person, der behandler personoplysninger på vegne af den dataansvarlige (bortset fra en person, der er ansat hos den dataansvarlige).

2.4. **Garantier, rettigheder og forpligtelser**

2.4.1. *Behandlingens lovlighed og rimelighed*

(28) I henhold til Section 35 i DPA 2018 skal behandlingen af personoplysninger være lovlig og rimelig på en måde, der svarer til artikel 4, stk. 1, litra a), i direktiv (EU) 2016/680. I henhold til Section 35(2) i DPA 2018 er behandling af personoplysninger til et hvilket som helst retshåndhævelsesformål kun lovlig, hvis den er hjemlet ved lov, og enten den registrerede har givet sit samtykke til behandlingen til dette formål, eller behandlingen er nødvendig for, at en kompetent myndighed kan udføre en opgave med henblik herpå.

2.4.1.1. Behandling på grundlag af loven

(29) I lighed med artikel 8 i direktiv (EU) 2016/680 skal en sådan behandling, for at sikre lovligheden af en behandling, der er omfattet af Part 3 i DPA 2018, være »baseret på lov«. Ved »lovlig« behandling forstås behandling, der er tilladt i henhold til enten lov, sædvaneret eller kongelige beføjelser ([45]).

(30) De kompetente myndigheders beføjelser er generelt reguleret ved lov, hvilket betyder, at deres funktioner og beføjelser er klart fastlagt i lovgivning vedtaget af parlamentet ([46]). I visse tilfælde kan politiet og andre kompetente myndigheder, der er opført i Schedule 7 til DPA 2018, basere sig på sædvaneret for at behandle data ([47]). Sædvaneret er udviklet gennem præcedens i form af domstolsafgørelser. Sædvaneretten er relevant i forbindelse med de beføjelser, som politiet har adgang til, idet politiet i henhold til denne retskilde har en central forpligtelse til at beskytte offentligheden ved at afsløre og forebygge kriminalitet ([48]). Politistyrkerne har

([45]) Forklarende bemærkninger til DPA 2018, paragraph 181, findes på følgende link: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) National Crime Agency udleder f.eks. sine beføjelser af Crime and Courts Act 2013, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2013/22/contents. Tilsvarende er Food Standards Agencys beføjelser fastsat i Food Standards Act 1999, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/1999/28/contents. Andre eksempler er Prosecution of Offenders Act 1985, hvorved Crown Prosecution Service blev oprettet (se https://www.legislation.gov.uk/ukpga/1985/23/contents); Commissioners for Revenue and Customs Act 2005, hvorved Her Majesty's Revenue and Customs blev oprettet (se https://www.legislation.gov.uk/ukpga/2005/11/contents); Criminal Procedure (Scotland) Act 1995, hvorved Scottish Criminal Cases Review Commission blev nedsat (se https://www.legislation.gov.uk/ukpga/1995/46/contents); Justice (Northern Ireland) Act 2002, hvorved Public Prosecution Service blev oprettet (se https://www.legislation.gov.uk/ukpga/2002/26/contents), og Serious Fraud Office blev oprettet og fik beføjelser i henhold til Criminal Justice Act 1987 (se https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Ifølge oplysningerne fra de britiske myndigheder udleder Lord Advocate, der er ansvarlig for retsforfølgningen af sager i Skotland inden for Crown Office and Procurator Fiscal Service, f.eks. sine beføjelser til at efterforske dødsfald og retsforfølge lovovertrædelser på grundlag af sædvaneret, mens en del af hans funktion er fastlagt ved lov. Desuden udleder Kronen og i forlængelse heraf forskellige regeringer, departementer og ministre også deres beføjelser af en kombination af lovgivning, sædvaneret og kongelige beføjelser (det drejer sig om sædvaneretlige beføjelser, der er tillagt Kronen, men som udøves af ministrene).

([48]) UK Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement, s. 8 (se fodnote 9).

dog beføjelser i henhold til både sædvaneret og lovgivning ([49]) til at udføre en sådan forpligtelse. Når politiet har lovfæstede beføjelser, træder dette i stedet for sædvaneretlige beføjelser ([50]).

(31) Domstolene har anerkendt, at politibetjentes beføjelser og forpligtelser i henhold til sædvaneret omfatter »alle de skridt, som betjente finder nødvendige for at bevare freden, forebygge kriminalitet eller beskytte formuegoder mod kriminel skade« ([51]). Sædvaneretlige beføjelser er ikke uden forbehold. De er underlagt en række begrænsninger, herunder dem, der er fastsat af domstolene ([52]) og i lovgivningen, navnlig Human Rights Act 1998 og Equality Act 2010 (lov om ligeret) ([53]). For kompetente myndigheder, der behandler data i henhold til Part 3 i DPA 2018, omfatter dette desuden udøvelse af sædvaneretlige beføjelser i overensstemmelse med kravene i DPA 2018 ([54]). Desuden skal en beslutning om at gennemføre enhver form for databehandling tage hensyn til kravene i gældende vejledning, såsom MoPI Code of Practice samt vejledninger, der er specifikke for et af landene i Det Forenede Kongerige ([55]). Regeringen og politiet udsteder en række vejledninger for at sikre, at politibetjente udøver deres beføjelser inden for de grænser, der er fastsat i sædvaneret eller den relevante lov ([56]).

(32) De kongelige prærogativer udgør en anden del af »loven« og henviser til visse beføjelser, der er tillagt Kronen og kan udøves af den udøvende magt, og som ikke er baseret på lov, men udspringer af monarkens suverænitet ([57]). Der er meget få eksempler på beføjelser, som er relevante i forbindelse med retshåndhævelse. De omfatter f.eks. rammen for gensidig retshjælp, der gør det muligt for Secretary of State at dele data med tredjelande med henblik på

([49]) De primære retsakter om politiets vigtigste beføjelser (anholdelse, ransagning, tilladelse til fortsat tilbageholdelse, fingeraftryk, udtagning af blod-, urin-, sæd- eller vævsprøver o.l., aflytninger og adgang til kommunikationsdata) er: i) for England og Wales, Police and Criminal Evidence Act 1984 (PACE), der findes på følgende link https://www.legislation.gov.uk/ukpga/1984/60/contents (som ændret ved Protection of Freedoms Act 2012 (PoFA)), som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2012/9/contents) og Investigatory Powers Act 2016 (IPA), der findes på følgende link:https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) for Skotland, Criminal Justice (Scotland) Act 2016, der findes på følgende link: https://www.legislation.gov.uk/asp/2016/1/contents og Criminal Procedure (Scotland) Act 1995, der findes på følgende link: https://www.legislation.gov.uk/ukpga/1995/46/contents), iii) for Nordirland, Police and Criminal Evidence (Northern Ireland) Order 1989, der findes på følgende link: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) De britiske myndigheder har forklaret, at den almindelige lovs forrang er en lang tradition i Det Forenede Kongerige og går så langt tilbage som til dommen i sagen *Entick mod Carrington* [1765] EWHC KB J98, som anerkendte, at der var grænser for den udøvende magts udøvelse af beføjelser, og fastsatte princippet om, at universal- og regeringsbeføjelser er underordnet lovgivningen på området.

([51]) Se sag *Rice mod Connolly* [1966] 2 QB 414.

([52]) Se sag *R (Catt) mod Association of Chief Police Officers* [2015] AC 1065, hvor Lord Sumption i forbindelse med politiets beføjelse til indsamling og opbevaring af oplysninger om en person (der havde begået en forbrydelse) fastslog, at politiet i henhold til sædvaneretten har beføjelse til at indsamle og opbevare oplysninger til politimæssige formål, dvs. i bred forstand til at sikre opretholdelse af den offentlige orden og forebyggelse og afsløring af kriminalitet. Disse beføjelser tillader ikke indgribende metoder til indsamling af oplysninger, såsom indtrængen på privat ejendom eller handlinger (bortset fra anholdelse i henhold til sædvaneretlige beføjelser), som ville udgøre et angreb. Dommeren fandt, at sædvaneretlige beføjelser i den foreliggende sag i høj grad var tilstrækkelige til at tillade indsamling og opbevaring af de pågældende offentlige oplysninger om disse appeller.

([53]) Equality Act 2010, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Et eksempel på en sag, hvor politiets sædvaneretlige beføjelser vurderes inden for rammerne af DPA 1998, findes i High Courts afgørelse i sagen *Bridges mod Chief Constable of South Wales Police* (se fodnote 33). Se også sagerne Vidal-Hall mod Google Inc [2015] EWCA Civ 311 og Richard mod BBC [2018] EWHC 1837 (Ch).

([55]) Se f.eks. vejledningen fra Police Service of Northern Ireland om forvaltning af journaler, som kan findes på følgende link: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf

([56]) Underhuset har offentliggjort et briefingdokument, som beskriver den vigtigste sædvaneret og lovfæstede beføjelser for politiet i England og Wales (se https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Det fremgår f.eks. af dette dokument, at selv om beføjelserne til at opretholde »Kronens fred« er afledt af sædvaneretten, hvilket også gælder »magtanvendelse«, er »visitations-beføjelser« altid afledt af lovgivningen. Desuden giver den skotske regering oplysninger på sit websted om politiets beføjelser vedrørende anholdelse og visitation (se https://www.gov.scot/policies/police/police-powers/).

([57]) Ifølge oplysningerne fra de britiske myndigheder omfatter regeringens beføjelser f.eks. udarbejdelse og ratifikation af traktater, diplomatiske funktioner og brug af de væbnede styrker i Det Forenede Kongerige til at opretholde freden til støtte for politiet.

retshåndhævelse, og beføjelsen til at udveksle data på denne måde er ikke altid fastsat ved lov ([58]). Kongelige prærogativer er omfattet af sædvaneretlige principper ([59]) og underlagt loven og er derfor omfattet af de begrænsninger, der er fastsat i Human Rights Act 1998 og DPA 2018 ([60]).

(33) I lighed med artikel 8 i direktiv (EU) 2016/680 kræver det britiske system, at de kompetente myndigheder for at overholde legalitetsprincippet skal sikre, at behandlingen, når den er baseret på loven, også er »nødvendig« for den opgave, der udføres med henblik på retshåndhævelse. ICO's vejledning i denne henseende præciserer, at »behandlingen skal være en målrettet og forholdsmæssig måde at opfylde formålet på. Retsgrundlaget gælder ikke, hvis man med rimelighed kan opfylde formålet med andre mindre indgribende midler. Det er ikke tilstrækkeligt at anføre, at behandling er nødvendig, fordi man har valgt at drive sin virksomhed på en bestemt måde. Spørgsmålet er, om behandlingen er nødvendig til det angivne formål« ([61]).

2.4.1.2. Behandling på grundlag af den registreredes »samtykke«

(34) Som nævnt i betragtning (28) giver Section 35(2) i DPA 2018 mulighed for at behandle personoplysninger på grundlag af den fysiske persons »samtykke«.

(35) Samtykke ser imidlertid ikke ud til at være et retsgrundlag, der er relevant for de behandlingsaktiviteter, som er omfattet af denne afgørelse. De behandlingsaktiviteter, der er omfattet af denne afgørelse, vil faktisk altid vedrøre data, som er overført i henhold til direktiv (EU) 2016/680 af en kompetent myndighed i en medlemsstat til en kompetent myndighed i Det Forenede Kongerige. De vil derfor typisk ikke omfatte den type direkte samspil (indsamling) mellem en offentlig myndighed og registrerede, som kan baseres på samtykke i henhold til Section 35(2)(a) i DPA 2018.

(36) Selv om samtykke derfor ikke anses for at være relevant for den vurdering, der foretages i henhold til denne afgørelse, er det for fuldstændighedens skyld værd at bemærke, at behandling i en retshåndhævelsessammenhæng aldrig udelukkende er baseret på samtykke, da en kompetent myndighed altid skal have en underliggende beføjelse, der sætter den i stand til at behandle oplysningerne ([62]). Mere specifikt og i lighed med, hvad der er tilladt i henhold til direktiv (EU) 2016/680 ([63]) betyder dette, at samtykke fungerer som en yderligere betingelse for at muliggøre visse begrænsede og specifikke behandlingsaktiviteter, der ellers ikke ville kunne foretages, f.eks. indsamling og behandling af en DNA-prøve fra en person, der ikke er mistænkt. I så fald vil behandlingen ikke blive foretaget, hvis samtykket ikke er givet eller trækkes tilbage ([64]).

([58]) Jf. i den forbindelse vurderingen af Det Forenede Kongeriges ordning for videreoverførsel i betragtning (74)-(87).

([59]) Jf. sagen *Bancoult mod Secretary of State for Foreign and Commonwealth Affairs* [2008] UKHL 61, hvor domstolene fastslog, at beføjelsen til at udstede Orders in Council (ministerielle bekendtgørelser) også var underlagt almindelig domstolsprøvelse.

([60]) Se sag *Attorney-General mod De Keyser's Royal Hotel Ltd* [1920] [1920] AC 508, hvor domstolen fastslog, at prærogative beføjelser ikke kan anvendes, når lovmæssige beføjelser erstatter dem; sagen Laker Airways Ltd mod Department of Trade 1977] QB 643,], hvor retten fandt, at prærogative beføjelser ikke har forrang for lovgivningen, sagen R mod Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3, hvor retten fastslog, at prærogative beføjelser ikke kan anvendes, hvis de er i strid med vedtaget lovgivning, selv ikke hvis den vedtagne lovgivning endnu ikke er trådt i kraft, sagen R (Miller) mod Secretary of State for Exiting the European Union [2017] UKSC 5, hvor domstolen bekræftede, at lovlovgivning kan tilpasse og tilsidesætte prærogative beføjelser. En generel oversigt over forholdet mellem de kongelige prærogativer og beføjelser i henhold til lovgivningen eller sædvaneret findes i Underhusets briefingdokument på følgende link: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Guide to Law Enforcement Processing, »What is the first principle about?«, der findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Dette følger af ordlyden i den relevante bestemmelse i DPA 2018, hvor det hedder, at behandling af personoplysninger til et hvilket som helst retshåndhævelsesformål kun er lovlig, hvis og i det omfang »den er baseret på lov«, og enten at a) den registrerede har givet samtykke til behandlingen med henblik herpå, eller b) at behandlingen er nødvendig for, at en kompetent myndighed kan udføre en opgave med henblik herpå«.

([63]) Jf. betragtning 35-37 i direktiv (EU) 2016/680.

([64]) De britiske myndigheder har forklaret, at et eksempel på, hvornår samtykke kan være et passende grundlag for behandling, er, hvor politiet indsamler en DNA-prøve i forbindelse med en forsvundet person for at matche et lig, hvis et sådan er blevet fundet. Under sådanne omstændigheder ville det være upassende for politiet at tvinge den registrerede til at fremlægge en prøve. Politiet vil i stedet anmode personen om frivilligt at give sit samtykke, som til enhver tid kan trækkes tilbage. Hvis samtykket trækkes tilbage, kan oplysningerne ikke længere behandles, medmindre der er fastlagt et nyt retsgrundlag for fortsat behandling af prøven (f.eks. hvis den registrerede er mistænkt). Et andet eksempel kan være, når politiet efterforsker en forbrydelse, hvor et offer (det kan være offer for røveri, seksuel forbrydelse, vold i hjemmet, slægtninge til et drab eller et andet offer for en forbrydelse) kan blive henvist til Victim Support (en uafhængig velgørende organisation, der støtter personer, som er berørt af kriminalitet og traumatiske hændelser). Under sådanne omstændigheder vil politiet kun videregive personlige oplysninger såsom navn og kontaktoplysninger til Victim Support med ofrets samtykke.

(37) I tilfælde, hvor der kræves samtykke fra den pågældende, skal et sådant være utvetydigt og indeholde en klar bekræftelse ([65]). Politiet skal have en databeskyttelsesmeddelelse, der bl.a. skal indeholde de nødvendige oplysninger om gyldig brug af samtykke. Desuden offentliggør nogle politistyrker yderligere materiale om, hvordan de overholder databeskyttelseslovgivningen, herunder hvordan og hvornår de vil anvende samtykke som retsgrundlag ([66]).

2.4.1.3. Behandling af følsomme oplysninger

(38) Der bør være specifikke garantier, når »særlige kategorier« af oplysninger behandles. I lighed med hvad der er fastsat i artikel 10 i direktiv (EU) 2016/680, giver Part 3 i DPA 2018 i denne henseende stærkere garantier for såkaldt »følsom behandling« ([67]).

(39) I henhold til Section 35(3) i DPA 1998 må de kompetente myndigheder kun behandle følsomme oplysninger til retshåndhævelsesformål i to tilfælde: 1) Den registrerede har givet sit samtykke til behandlingen med henblik på retshåndhævelse, og på det tidspunkt, hvor behandlingen foretages, har den dataansvarlige udarbejdet et passende politikdokument ([68]), eller 2) behandlingen er strengt nødvendig af hensyn til retshåndhævelsesformålet, behandlingen opfylder mindst en af betingelserne i Schedule 8 til DPA 2018, og på det tidspunkt, hvor behandlingen foretages, har den dataansvarlige udarbejdet et passende politikdokument ([69]).

(40) For så vidt angår det første tilfælde og som forklaret i betragtning 38 anses anvendelsen af samtykke ikke for relevant i den type overførselssituation, der er omfattet af denne afgørelse ([70]).

(41) Når behandlingen af følsomme oplysninger ikke er baseret på samtykke, kan den foretages på en af betingelserne i Schedule 8 til DPA 2018. Disse betingelser vedrører behandling, der er nødvendig i henhold til loven, retsplejen, beskyttelse af den registreredes eller en anden persons vitale interesser, beskyttelse af børn og udsatte personer, retskrav, retsakter, forebyggelse af svig, arkivering, og hvis personoplysninger åbenlyst offentliggøres af den registrerede. Bortset fra det tilfælde, hvor oplysningerne åbenlyst offentliggøres, er alle betingelserne i Schedule 8 underlagt en »streng nødvendighedstest«. Som præciseret af ICO betyder »strengt nødvendigt« i denne forbindelse, at

([65]) Der findes ingen særskilt definition af »samtykke« med henblik på behandling af personoplysninger i henhold til Part 3 i DPA 2018. ICO's vejledning om begrebet »samtykke« i Part 3 i DPA 2018 præciserer, at det har samme betydning som og bør bringes i overensstemmelse med definitionen i GDPR, navnlig at »samtykke skal gives frivilligt, specifikt og informeret, og der skal være et reelt valg om at acceptere de oplysninger, der behandles« (Guide to Law Enforcement Processing, »What is the first principle about?« (se fodnote 64) og Guide to Data Protection on consent, som kan findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Se f.eks. oplysningerne på webstedet for Lincolnshire Police (se https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) eller på webstedet for West Yorkshire Police (se https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Section 35(8) i DPA 2018.

([68]) Section 35(4) i DPA 2018.

([69]) Section 35(5) i DPA 2018.

([70]) For fuldstændighedens skyld er det værd at bemærke, at når behandlingen er baseret på samtykke, skal dette gives frivilligt, det skal være specifikt og informeret, og der skal være et specifikt valg med hensyn til at give samtykke til behandling af de pågældende oplysninger. Desuden skal den dataansvarlige, når behandlingen sker på grundlag af den registreredes samtykke, have et »passende politikdokument«. I Section 42 i DPA 2018 beskrives de krav, som politikdokumentet skal opfylde. Det præciseres, at der i dokumentet som minimum skal gøres rede for den dataansvarliges procedurer for at sikre overholdelse af databeskyttelsesprincipperne og dens politik med hensyn til opbevaring og sletning af personoplysninger. I henhold til Section 42 i DPA 2018 betyder dette, at den dataansvarlige skal fremlægge et dokument, som a) beskriver dennes procedurer for sikring af overholdelse af databeskyttelsesprincipperne og b) beskriver dennes politik med hensyn til opbevaring og sletning af personoplysninger, der behandles på grundlag af den registreredes samtykke, eller en angivelse af, hvor længe sådanne personoplysninger sandsynligvis vil blive opbevaret. Det skal navnlig fremgå af politikdokumentet, at den dataansvarlige under overholdelse af sin pligt til at registrere behandlingsaktiviteterne altid skal medtage de elementer, der er nævnt i a) og b). ICO har offentliggjort et standarddokument (Guide to Law Enforcement Processing, »Conditions for sensitive processing«), der findes på følgende link: Https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing, og denne kan træffe håndhævelsesforanstaltninger, hvis den dataansvarlige ikke opfylder disse krav. Politikdokumentet gennemgås også af domstolene i forbindelse med vurderingen af potentielle overtrædelser af DPA 2018. I den nylige sag R (Bridges) mod Chief Constable of South Wales Police gennemgik domstolene f.eks. den dataansvarliges politikdokument og fandt, at det var tilstrækkeligt, men at det med fordel kunne have været mere detaljeret. Som følge heraf gennemgik Southern Wales Police politikdokumentet og ajourførte det i overensstemmelse med ICO's nye retningslinjer (se fodnote 33). Endvidere bør den dataansvarlige i henhold til Section 42(3) i DPA 2018 regelmæssigt revidere politikdokumentet. Endelig er den dataansvarlige som en yderligere sikkerhedsforanstaltning i henhold til Section 42(4) i DPA 2018 forpligtet til at føre en udvidet fortegnelse over behandlingsaktiviteter, herunder yderligere elementer i forhold til den dataansvarliges generelle forpligtelse til at føre registre over behandlingsaktiviteterne i Section 61 i DPA 2018.

behandlingen skal vedrøre et presserende socialt behov, og at man ikke med rimelighed kan opfylde formålet ved hjælp af mindre indgribende midler ([71]). Desuden er nogle af betingelserne underlagt yderligere begrænsninger. For at påberåbe sig betingelsen om »lovfæstede formål« og »beskyttelsesklausulen« (Schedule 8, paragraph 1 og paragraph 4) er der f.eks. et yderligere kriterium af væsentlig samfundsmæssig interesse, som skal opfyldes. Hvad angår betingelserne for beskyttelse af børn (Schedule 8, paragraph 4), skal den registrerede desuden have en bestemt alder og anses for at være i fare. Desuden kan den dataansvarlige kun anvende betingelsen i Schedule 8, paragraph 4, under særlige omstændigheder ([72]). Tilsvarende er der begrænsninger for betingelserne for »retslige handlinger« og »forebyggelse af svig« (Schedule 8, henholdsvis paragraph 7 og 8). Begge gælder kun for bestemte dataansvarlige. I tilfælde af retsakter kan kun en domstol eller en anden judiciel myndighed anvende en sådan betingelse, og i tilfælde af forebyggelse af svig kan kun dataansvarlige, der er organisationer til bekæmpelse af svig, påberåbe sig den.

(42) Endelig gælder det, at når behandlingen er baseret på en af betingelserne i Schedule 8 og i overensstemmelse med Section 42 i DPA 2018, skal der foreligge et »passende politikdokument«, som beskriver den dataansvarliges procedurer for at sikre overholdelse af databeskyttelsesprincipperne og den dataansvarliges politik med hensyn til opbevaring og sletning af personoplysninger, og en skærpet registreringspligt.

2.4.2. *Formålsbegrænsning*

(43) Personoplysninger skal behandles til et specifikt formål og efterfølgende udelukkende bruges, såfremt dette ikke er uforeneligt med behandlingsformålet. Dette databeskyttelsesprincip er sikret ved Section 36 i DPA 2018. I lighed med artikel 4, stk. 1, litra b), i direktiv (EU) 2016/680 kræver denne bestemmelse, at a) det retshåndhævelsesformål, hvortil personoplysninger indsamles, skal præciseres samt være udtrykkeligt og legitimt, og at b) de således indsamlede personoplysninger ikke må behandles på en måde, der er uforenelig med det formål, hvortil de blev indsamlet.

(44) Hvis de kompetente myndigheder behandler data med henblik på retshåndhævelse, kan dette omfatte arkivering, videnskabelig eller historisk forskning og statistiske formål ([73]). I disse tilfælde præciseres det også i DPA 2018, at arkivering (eller behandling til videnskabelige eller historiske forskningsformål og statistiske formål) ikke er tilladt, hvis den foretages i forbindelse med afgørelser, der træffes vedrørende en bestemt registreret, eller hvis det kan forvolde den pågældende væsentlig skade eller lidelse ([74]).

2.4.3. *Nøjagtighed og dataminimering*

(45) Oplysningerne skal være nøjagtige og holdes ajour. De skal også være tilstrækkelige, relevante og ikke for omfattende i forhold til de formål, hvortil de behandles. I lighed med artikel 4, stk. 1, litra c), d) og e), i direktiv (EU) 2016/680 er disse principper sikret i Section 37 og 38 i DPA 2018. Der skal tages ethvert rimeligt skridt til at sikre, at urigtige personoplysninger ([75]) straks

([71]) Guide to Law Enforcement Processing, »Conditions for sensitive processing« (se fodnote 70).

([72]) Behandlingen foretages uden den registreredes samtykke, når: a) den registrerede ikke kan give sit samtykke til behandlingen, b) den dataansvarlige ikke med rimelighed kan forventes at indhente den registreredes samtykke til behandlingen, c) behandlingen skal foretages uden den registreredes samtykke, fordi indhentning heraf ville være til skade for den beskyttelse, der er nævnt i sub-paragraph (1)(a).

([73]) Jf. Section 41(1) i DPA 2018.

([74]) Jf. Section 41(2) i DPA 2018.

([75]) I Section 205 i DPA 2018 defineres udtrykket »unøjagtige« som »ukorrekte eller vildledende« personoplysninger. Det Forenede Kongeriges myndigheder har forklaret, at oplysninger vedrørende strafferetlige efterforskninger typisk ofte vil være ufuldstændige, men at de uanset dette kan være nøjagtige.

slettes eller berigtiges ([76]) under hensyntagen til det retshåndhævelsesformål, hvortil de behandles ([77]), og til at sikre, at personoplysninger, der er ukorrekte, ufuldstændige eller ikke længere ajourførte, ikke videregives eller stilles til rådighed med henblik på retshåndhævelse ([78]).

(46) I lighed med artikel 7 i direktiv (EU) 2016/680 præciserer Det Forenede Kongeriges databeskyttelsesordning desuden, at der så vidt muligt skal sondres mellem personoplysninger baseret på fakta og personoplysninger baseret på personlige vurderinger ([79]). Hvor det er relevant og så vidt muligt, skal der skelnes klart mellem personoplysninger vedrørende forskellige kategorier af registrerede, såsom mistænkte, personer, der er dømt for en strafbar handling, ofre for en strafbar handling, og vidner ([80]).

2.4.4. *Begrænsning af opbevaring*

(47) I henhold til artikel 5 i direktiv (EU) 2016/680 må oplysningerne i princippet ikke opbevares i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil personoplysningerne behandles. I henhold til Section 39 i DPA 2018 og i lighed med direktivets artikel 5 er det forbudt at opbevare personoplysninger, der behandles til et hvilket som helst retshåndhævelsesformål, i et længere tidsrum end det, der er nødvendigt i forhold til det formål, hvortil de behandles. Det Forenede Kongeriges retssystem kræver, at der fastsættes passende tidsfrister for regelmæssig revision af behovet for fortsat opbevaring af personoplysninger med henblik på retshåndhævelse. Yderligere regler om praksis i forbindelse med opbevaring af personoplysninger og de gældende tidsfrister er fastsat i den relevante lovgivning og vejledning om politiets beføjelser og funktionsmåde. I England og Wales udgør College of Policings MoPI Code of Practice sammen med APP Guidance on the Management of Police Information f. eks. en ramme til sikring af en konsekvent risikobaseret opbevarings-, revisions- og bortskaffelsesproces i forbindelse med forvaltningen af operationelle politioplysninger ([81]). Denne ramme fastsætter klare forventninger på tværs af tjenesten til, hvordan oplysninger bør skabes, deles, anvendes og forvaltes inden for og mellem de enkelte politistyrker og andre agenturer ([82]). Politiet forventes at overholde adfærdskodeksen, og overholdelsen kontrolleres af Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services ([83]).

(48) Police Service of Northern Ireland (PSNI) er ikke ved lov forpligtet til at følge MoPI Code of Practice. MoPI-rammen, der blev vedtaget i 2011, suppleres dog af en håndbog udarbejdet af PSNI ([84]), der beskriver politikker og procedurer for anvendelsen af adfærdskodeksen i Nordirland.

([76]) Section 38(1)(b) i DPA 2018.

([77]) Ifølge Det Forenede Kongeriges Explanatory Framework for Adequacy Discussion sikrer dette, at både de registreredes rettigheder og de retshåndhævende myndigheders operationelle behov anerkendes. Ovenstående punkt blev nøje overvejet i forbindelse med udarbejdelsen af databeskyttelsesloven, da der kan være specifikke og begrænsede operationelle årsager til, at data ikke kan berigtiges. Dette vil højst sandsynligt være tilfældet, hvis de pågældende unøjagtige personoplysninger skal bevares i deres oprindelige form med henblik på bevisførelse (jf. UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, side 21, jf. fodnote 9).

([78]) Section 38(4) i DPA 2018. I henhold til Section 38(5) i DPA 2018 skal kvaliteten af personoplysningerne desuden efterprøves, inden de videregives eller stilles til rådighed; ved enhver videregivelse af personoplysninger skal de oplysninger, der er nødvendige for, at modtageren kan vurdere, i hvor høj grad oplysningerne er korrekte, fuldstændige og pålidelige, og i hvilket omfang de er ajourførte, medtages, og hvis det efter videregivelsen af personoplysningerne viser sig, at oplysningerne var ukorrekte, eller at videregivelsen var ulovlig, skal modtageren straks underrettes.

([79]) Section 38(2) i DPA 2018.

([80]) Section 38(3) i DPA 2018.

([81]) Rammen sikrer konsekvens i opbevaringen af de indsamlede personoplysninger. Vurderingsperioden afhænger af overtrædelserne, der er inddelt i fire grupper: 1) visse spørgsmål vedrørende beskyttelse af offentligheden, 2) andre alvorlige forbrydelser og seksuelle overgreb, 3) alle andre lovovertrædelser, 4) diverse. Yderligere oplysninger findes i APP Guidance on the Management of Police Information (se fodnote 26).

([82]) Ifølge oplysningerne fra de britiske myndigheder kan andre organisationer frit følge principperne i MoPI Code of Practice, hvis de ønsker det, f.eks. har Her Majesty's Revenue and Customs og National Crime Agency frivilligt indarbejdet mange af principperne for at sikre konsekvens i retshåndhævelsen. Generelt udleverer de fleste organisationer specifikke politikker og vejledning til alle medarbejdere om, hvordan de håndterer personoplysninger i deres arbejde, som er skræddersyet til den specifikke organisation. Dette vil normalt også omfatte obligatorisk uddannelse.

([83]) MoPI Code of Practice blev udstedt under anvendelse af de beføjelser, der er fastsat i Police Act 1996, som giver College of Policing mulighed for at udstede adfærdskodekser, der gør politiarbejdet mere effektivt. Enhver adfærdskodeks, der udarbejdes i henhold til loven, skal godkendes af Secretary of State og høres af National Crime Agency, inden den vedtages i parlamentet. I henhold til Section 39A(7) i Police Act 1996 skal politiet tage behørigt hensyn til de kodekser, der er udstedt i henhold til denne lov.

([84]) PSNI MoPI Handbook, kapitel 1-6.

(49) I Skotland baserer politiet sig på Record Retention Standard Operating Procedure (SOP) (standardprocedure for registrering) ([85]), som understøtter det skotske politis Records Management Policy (politik for forvaltning af registre) ([86]). SOP fastsætter specifikke opbevaringsregler for de registre, som føres af politiet i Skotland.

(50) Ud over det overordnede krav om gennemgang af registre, der gælder i hele Det Forenede Kongerige, findes der yderligere oplysninger i lokale regler. For at give nogle få eksempler er det sådan, at for så vidt angår England og Wales indeholder Police and Criminal Evidence Act (PACE) (politiloven), som ændret ved Freedom Protection Act 2012 (PoFA) (lov om beskyttelse af frihedsrettigheder), bestemmelser om opbevaring af fingeraftryk og DNA-profiler samt en særlig ordning for personer, der ikke er dømt ([87]). Med PoFA oprettedes også stillingen som Commissioner for the Retention and Use of Biometric Material (»Biometrics Commissioner«) (kommissær for opbevaring af biomometrisk materiale) ([88]). Særlige regler om fotos af varetægtsfængslede findes i 2017 Custody Image Review (revision af bestemmelserne om fotos af varetægtsfængslede) ([89]). Med hensyn til Skotland indeholder Criminal Procedure (Scotland) Act 1995 (Skotlands strafferetsplejelov) regler for indsamling og opbevaring af fingeraftryk og biologiske prøver ([90]). Som for England og Wales regulerer lovgivningen opbevaring af biometriske data i forskellige situationer ([91]).

2.4.5. *Datasikkerhed*

(51) Personoplysninger skal behandles på en måde, der garanterer deres sikkerhed, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse. Med henblik herpå skal de offentlige myndigheder træffe passende tekniske eller organisatoriske foranstaltninger for at beskytte personoplysninger mod mulige trusler. Disse foranstaltninger skal vurderes under hensyntagen til det aktuelle tekniske niveau og de dermed forbundne omkostninger.

(52) Disse principper afspejles i Section 40 i DPA 2018, der bestemmer, at personoplysninger, som behandles med henblik på retshåndhævelse, i lighed med artikel 4, stk. 1, litra f), i direktiv (EU) 2016/680 skal behandles på en måde, der garanterer en passende sikkerhed for personoplysningerne ved hjælp af passende tekniske eller organisatoriske foranstaltninger. Dette omfatter beskyttelse af oplysningerne mod uautoriseret eller ulovlig

([85]) Record Retention Standard Operating Procedure (SOP), som kan findes på følgende link: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Yderligere oplysninger om forvaltning af registreringer findes på følgende link om Skotlands nationale registre: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Opbevaringsperioderne varierer afhængigt af, om en person er blevet dømt eller ikke (Section 63I-63KI i PACE 1984). Hvis der f.eks. er tale om en voksen, som er dømt for en lovovertrædelse, der kan registreres, kan vedkommendes fingeraftryk og DNA-profil opbevares på ubestemt tid (Section 63I(2) i PACE 1984), mens opbevaringen er tidsbegrænset, hvis den domfældte er under 18 år, lovovertrædelsen er en »mindre« lovovertrædelse, der kan registreres, og personen ikke er tidligere dømt (Section 63K i PACE 1984). Opbevaringsperioden for data om en person, der er anholdt eller tiltalt, men ikke dømt, er tidsbegrænset til tre år (Section 63F i PACE 1984). Forlængelse af denne opbevaringsperiode skal godkendes af den judicielle myndighed (Section 63F(7) i PACE 1984). I tilfælde af personer, der er anholdt eller anklaget, men ikke dømt for mindre lovovertrædelser, kan deres data ikke opbevares (Section 63D og Section 63H i PACE 1984).

([88]) Ved Section 20 i PoFA 2012 oprettes stillingen som Biometrics Commissioner. 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). Biometric Commissioner udnævnes i henhold til Code for Public Appointments (kodeks for udnævnelser i den offentlige sektor) (kodeksen findes på følgende link: Governance Code for Public Appointments - GOV.UK (www.gov.uk)), og det fremgår klart af udnævnelsesbetingelserne, at den pågældende alene kan fjernes fra embedet af Home Secretary og på baggrund af et snævert sæt af forhold, såsom at den pågældende ikke udfører sine funktioner i en periode på tre måneder, er dømt for en forbrydelse eller ikke overholder betingelserne for udnævnelsen.

([89]) Review of the Use and Retention of Custody Images, findes på følgende link: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Section 18 ff. i Criminal Procedure (Scotland) Act 1995.

([91]) Opbevaringsperioderne afhænger af, om personen er blevet dømt (Section 18(3) i Criminal Procedure (Scotland) Act 1995), eller om vedkommende er mindreårig. I sidstnævnte tilfælde er opbevaringsperioden tre år fra domsafsigelsen (Section 18E(8) i Criminal Procedure (Scotland) Act 1995). Oplysninger om personer, der er anholdt, men ikke dømt, må ikke opbevares (Section 18(3) i Criminal Procedure (Scotland) Act 1995) undtagen i særlige tilfælde og afhængigt af forbrydelsens alvor (Section 18A i Criminal Procedure (Scotland) Act 1995). Ved Scottish Biometrics Commissioner Act 2020 (se https://www.legislation.gov.uk/asp/2020/8/contents) oprettes stillingen som Biometrics Commissioner. Denne skal udarbejde og revidere adfærdskodekser (godkendt af det skotske parlament) vedrørende indsamling, opbevaring, anvendelse og destruktion af biometriske data til strafferetlige og politimæssige formål (Section 7 i Scottish Biometrics Commissioner Act 2020).

behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse ([92]). I Section 66 i DPA 2018 præciseres endvidere, at hver dataansvarlig og hver databehandler skal gennemføre hensigtsmæssige tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, som er passende i forhold til de risici, der opstår som følge af behandlingen af personoplysninger. Ifølge de forklarende bemærkninger skal den dataansvarlige vurdere risiciene og gennemføre passende sikkerhedsforanstaltninger på grundlag af denne evaluering, f.eks. kryptering eller specifikke sikkerhedsgodkendelsesniveauer for personale, der behandler oplysningerne ([93]). I evalueringen skal der også tages hensyn til f.eks. arten af de behandlede oplysninger og andre relevante faktorer eller omstændigheder, der kan påvirke behandlingssikkerheden.

(53) Ordningen for overholdelse af principperne for datasikkerhed svarer meget til den, der er fastsat i artikel 29-31 i direktiv (EU) 2016/680. Navnlig i tilfælde af brud på persondatasikkerheden i forbindelse med personoplysninger, som den dataansvarlige er ansvarlig for, skal denne i henhold til Section 67(1) i DPA 2018 uden unødig forsinkelse og om muligt inden for 72 timer efter at have fået kendskab til bruddet på persondatasikkerheden anmelde dette til Information Commissioner ([94]). Underretningspligten finder ikke anvendelse, når bruddet på persondatasikkerheden sandsynligvis ikke vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder ([95]). Den dataansvarlige skal dokumentere de faktiske omstændigheder i forbindelse med ethvert brud på persondatasikkerheden, dets virkninger og de afhjælpende foranstaltninger, der er truffet, på en sådan måde, at Information Commissioner kan kontrollere, at databeskyttelsesloven overholdes ([96]). Hvis en databehandler bliver opmærksom på et sikkerhedsbrud, skal denne underrette den dataansvarlige uden unødig forsinkelse ([97]).

(54) I henhold til Section 68(1) i DPA 2018 skal den dataansvarlige, hvis et brud på persondatasikkerheden sandsynligvis udgør en høj risiko for fysiske personers rettigheder og frihedsrettigheder, uden unødig forsinkelse underrette den registrerede om bruddet ([98]). Underretningen skal indeholde de samme oplysninger som meddelelsen til Information Commissioner, der er beskrevet i betragtning (53). Denne forpligtelse gælder ikke, hvis den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, som er blevet anvendt på de personoplysninger, der er berørt af bruddet. Den finder heller ikke anvendelse, hvis den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for registreredes rettigheder og frihedsrettigheder sandsynligvis ikke længere vil bestå. Endelig er den dataansvarlige ikke forpligtet til at underrette den registrerede, hvis dette ville indebære en uforholdsmæssig stor indsats ([99]). I så fald skal oplysningerne stilles til rådighed for den registrerede på en anden lige så effektiv måde, f.eks. gennem en offentlig meddelelse ([100]). Hvis den dataansvarlige ikke har underrettet den registrerede om bruddet, kan Information Commissioner efter at være blevet underrettet i henhold til Section 67 i DPA og efter at have overvejet sandsynligheden for, at bruddet medfører en høj risiko, kræve, at den dataansvarlige underretter den registrerede om bruddet ([101]).

([92]) I overensstemmelse med de forklarende bemærkninger til DPA 2018 (se fodnote 45) skal den dataansvarlige navnlig: udforme og tilrettelægge deres sikkerhed, så dette passer til arten af de personoplysninger, de er i besiddelse af, og den skade, der kan opstå som følge af et brud på sikkerheden, være klar over, hvem i deres organisation der er ansvarlig for at garantere informationssikkerheden, sikre sig, at de har den rette fysiske og tekniske sikkerhed, understøttet af robuste politikker og procedurer samt pålideligt, veluddannet personale og være rede til at reagere hurtigt og effektivt på ethvert brud på sikkerheden.

([93]) Paragraph 221 i de forklarende bemærkninger til DPA 2018 (se fodnote 45).

([94]) I Section 67(4) i DPA 2018 fastsættes, at underretningen skal indeholde en beskrivelse af karakteren af bruddet på persondatasikkerheden (herunder om muligt kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger), navn og kontaktoplysninger på et kontaktpunkt, en beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden og en beskrivelse af de foranstaltninger, som den dataansvarlige har truffet eller foreslået at træffe for at afhjælpe bruddet på persondatasikkerheden (herunder, hvor det er relevant, foranstaltninger til at afbøde de mulige skadevirkninger).

([95]) Section 67(2) i DPA 2018.

([96]) Section 67(6) i DPA 2018.

([97]) Section 67(9) i DPA 2018.

([98]) I henhold til Section 68(7) i DPA 2018 kan den dataansvarlige helt eller delvist begrænse underretningen af den registrerede, i det omfang og så længe begrænsningen, under hensyn til den registreredes grundlæggende rettigheder og legitime interesser, er en nødvendig og forholdsmæssig foranstaltning for at a) undgå at hindre en officiel eller retlig undersøgelse, efterforskning eller procedure, b) undgå at hindre forebyggelse, opdagelse, efterforskning eller retsforfølgning af strafbare handlinger, c) beskytte den offentlige sikkerhed, d) beskytte statens sikkerhed, e) beskytte andres rettigheder og frihedsrettigheder.

([99]) Section 68(3) i DPA 2018.

([100]) Section 68(5) i DPA 2018.

([101]) Section 68(6) i DPA 2018 med forbehold af den begrænsning, der er fastsat i Section 68(8) i DPA 2018.

2.4.6. *Gennemsigtighed*

(55) De registrerede skal informeres om de vigtigste elementer i behandlingen af deres personoplysninger. Dette databeskyttelsesprincip afspejles i Section 44 i DPA 2018, som i lighed med artikel 13 i direktiv (EU) 2016/680 bestemmer, at den dataansvarlige har en generel forpligtelse til at stille oplysninger om behandlingen af deres personoplysninger til rådighed for de registrerede (enten ved at gøre oplysningerne alment tilgængelige for offentligheden eller på anden måde) ([102]). De oplysninger, der skal stilles til rådighed, omfatter a) den dataansvarliges identitet og kontaktoplysninger, b) databeskyttelsesrådgiverens kontaktoplysninger, hvis det er relevant, c) de formål, hvortil den dataansvarlige behandler personoplysninger, d) de registreredes ret til at anmode den dataansvarlige om indsigt i personoplysninger, berigtigelse af personoplysninger og sletning af personoplysninger eller begrænsning af behandlingen heraf og e) retten til at indgive en klage til Information Commissioner og kontaktoplysninger for denne ([103]).

(56) Den dataansvarlige skal også i særlige tilfælde med henblik på at gøre det muligt for en registreret at udøve sine rettigheder i henhold til DPA 2018 (f.eks. når de personoplysninger, der behandles, blev indsamlet uden den registreredes vidende) give den registrerede oplysninger om a) retsgrundlaget for behandlingen, b) oplysninger om det tidsrum, hvori personoplysningerne opbevares, eller, hvis dette ikke er muligt, om de kriterier, der anvendes til at fastsætte denne periode, c) i givet fald oplysninger om kategorierne af modtagere af personoplysningerne (herunder modtagere i tredjelande eller internationale organisationer), d) yderligere oplysninger, der er nødvendige for at gøre det muligt den registrerede at udøve sine rettigheder i henhold til Part 3 i DPA 2018 ([104]).

2.4.7. *Individuelle rettigheder*

(57) De registrerede skal have en række rettigheder, som kan håndhæves. Chapter 3, Part del 3 i DPA 2018 giver fysiske personer ret til indsigt, berigtigelse, sletning og begrænsning ([105]), som svarer til, hvad der er fastsat i kapitel 3 i direktiv (EU) 2016/680.

(58) Retten til indsigt er fastsat i Section 45 i DPA 2018. For det første har en fysisk person ret til at få en bekræftelse fra den dataansvarlige om, hvorvidt vedkommendes personoplysninger behandles eller ikke ([106]). For det andet har den registrerede, når personoplysningerne behandles, ret til at få adgang til disse oplysninger og modtage følgende oplysninger om behandlingen: a) formålet med og retsgrundlaget for behandlingen, b) de pågældende kategorier af oplysninger, c) den modtager, som oplysningerne er videregivet til, d) det tidsrum, hvori personoplysningerne skal opbevares, e) den registreredes ret til berigtigelse og sletning af personoplysninger, f) retten til klageadgang og g) oplysninger om de pågældende personoplysningers oprindelse ([107]).

(59) I henhold til Section 46 i DPA 2018 har den registrerede ret til at kræve, at den dataansvarlige berigtiger urigtige personoplysninger om vedkommende. Den dataansvarlige skal uden unødig forsinkelse berigtige (eller, hvis oplysningerne er ukorrekte, fordi de er ufuldstændige, supplere) oplysningerne. Hvis personoplysningerne skal opbevares med henblik på bevisførelse, skal den dataansvarlige (i stedet for at berigtige personoplysningerne) begrænse behandlingen heraf ([108]).

([102]) Guide to Law Enforcement Processing indeholder følgende eksempel: »Der er en generel meddelelse om databeskyttelse på dit websted, som indeholder grundlæggende oplysninger om organisationen, formålet med behandlingen af personoplysninger, en registrerets rettigheder og dennes ret til at klage til Information Commissioner. Du har modtaget oplysninger om, at en person var til stede, da en forbrydelse fandt sted. Under din første samtale med denne person skal du give de generelle oplysninger og yderligere supplerende oplysninger for at gøre det muligt for den pågældende at udøve sine rettigheder. Du har kun ret til at begrænse dine oplysninger om rimelig behandling, hvis de vil påvirke dine undersøgelser negativt« (Guide to Law Enforcement Processing, »What information should we supply to an individual?«, som kan findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) I vejledningen Guide to Law Enforcement Processing hedder det, at de oplysninger, der gives om behandling af personoplysninger, skal være koncise, forståelige og let tilgængelige. De skal være skrevet i et klart og forståeligt sprog og være tilpasset sårbare personers, f.eks. børns, behov, og de skal være gratis (Guide to Law Enforcement Processing, »How should we provide this information?«, findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Section 44(2) i DPA 2018.

([105]) En detaljeret analyse af de registreredes rettigheder findes i: Guide to Law Enforcement Processing on individual rights, der er tilgængelig på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) Section 45(1) i DPA 2018.

([107]) Section 45(2) i DPA 2018.

([108]) Section 46(4) i DPA 2018.

(60) Section 47 i DPA 2018 giver fysiske personer ret til sletning og begrænsning af behandlingen. Den dataansvarlige skal ([109]) slette personoplysninger uden unødig forsinkelse, hvis behandlingen af personoplysningerne vil være i strid med databeskyttelsesprincipperne, retsgrundlaget for behandlingen eller garantierne i forbindelse med arkivering og følsom behandling. Den dataansvarlige skal slette oplysningerne, hvis der består en retlig forpligtelse hertil. Hvis personoplysningerne skal opbevares med henblik på bevisførelse, skal den dataansvarlige (i stedet for at berigtige personoplysningerne) begrænse behandlingen heraf ([110]). Den dataansvarlige skal begrænse behandlingen af personoplysninger, hvis en registreret anfægter rigtigheden af personoplysningerne, men det ikke er muligt at fastslå, om de er korrekte eller ej ([111]).

(61) Hvis en registreret anmoder om berigtigelse eller sletning af personoplysninger eller begrænsning af behandlingen heraf, skal den dataansvarlige skriftligt underrette den registrerede om, hvorvidt anmodningen er imødekommet, og, hvis den er blevet afvist, oplyse den registrerede om årsagerne til afslaget og om tilgængelige klagemuligheder (den registreredes ret til at indgive en anmodning til Information Commissioner om at undersøge, om begrænsningen er blevet anvendt lovligt, retten til at indgive en klage til Information Commissioner og retten til at anmode en domstol om at efterkomme afgørelsen) ([112]).

(62) Hvis den dataansvarlige berigtiger personoplysninger, der er modtaget fra en anden kompetent myndighed, skal denne underrette den anden myndighed ([113]). Hvis den dataansvarlige berigtiger, sletter eller begrænser behandlingen af personoplysninger, der er videregivet af den dataansvarlige, skal den dataansvarlige underrette modtagerne, og modtagerne skal ligeledes berigtige, slette eller begrænse behandlingen af personoplysningerne (for så vidt de bevarer ansvaret for dem) ([114]).

(63) Desuden har den registrerede ret til uden unødig forsinkelse at blive underrettet af den dataansvarlige om brud på persondatasikkerheden, når dette sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder ([115]).

(64) I forbindelse med alle den registreredes rettigheder og i lighed med, hvad der er fastsat i artikel 12 i direktiv (EU) 2016/680, er den dataansvarlige forpligtet til at sikre, at alle oplysninger til den registrerede gives i en kortfattet, letforståelig og lettilgængelig form ([116]), og at de så vidt muligt gives i samme form som anmodningen ([117]). Den dataansvarlige skal efterkomme en anmodning fra den registrerede uden unødig forsinkelse eller under alle omstændigheder inden udløbet af en frist på en måned fra anmodningen ([118]). Hvis den dataansvarlige nærer rimelig tvivl om en persons identitet, kan vedkommende anmode om yderligere oplysninger og udsætte behandlingen af anmodningen, indtil identiteten er fastslået. Den dataansvarlige kan kræve et rimeligt gebyr eller nægte at handle, hvis den anser anmodningen for at være åbenbart grundløs ([119]). ICO har udarbejdet en vejledning om, hvornår en anmodning anses for at være åbenbart grundløs eller overdreven, og hvornår der kan anmodes om et gebyr ([120]).

(65) I henhold til Section 53(4) i DPA 2018 kan Secretary of State desuden ved bekendtgørelse fastsætte det maksimale gebyrbeløb.

([109]) En registreret kan anmode den dataansvarlige om at slette personoplysninger eller begrænse behandlingen heraf (men den dataansvarliges pligt til at slette oplysningerne eller begrænse behandlingen heraf gælder, uanset om der fremsættes en sådan anmodning).

([110]) Section 46(4) og 47(2) i DPA 2018.

([111]) Section 47(3) i DPA 2018.

([112]) Section 48(1) i DPA 2018.

([113]) Section 48(7) i DPA 2018.

([114]) Section 48(9) i DPA 2018.

([115]) Section 68 i DPA 2018.

([116]) Section 52(1) i DPA 2018.

([117]) Section 52(3) i DPA 2018.

([118]) Section 54 i DPA 2018 definerer betydningen af »gældende tidsperiode«, dvs. den periode på en måned eller en længere periode, som måtte være fastsat i bestemmelser, begyndende med det relevante tidspunkt (når den dataansvarlige modtager den pågældende anmodning, når den dataansvarlige modtager de (eventuelle) oplysninger, der anmodes om i forbindelse med en anmodning i henhold til databeskyttelsesmyndighedens Section 52(4), eller når det (eventuelle) gebyr, der opkræves i forbindelse med anmodningen i henhold til Section 53 i DPA, betales.

([119]) Section 53(1) i DPA 2018.

([120]) I henhold til ICO's vejledning kan en dataansvarlig beslutte at opkræve et gebyr af en registreret, hvis vedkommendes anmodning er åbenbart grundløs eller overdreven, men stadig vælger at besvare den. Gebyret skal være rimeligt, og omkostningerne skal kunne begrundes. Guide to Law Enforcement Processing »Manifestly unfounded and excessive requests«, der findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

2.4.7.1. Begrænsninger i den registreredes rettigheder og gennemsigtighedsforpligtelser

(66) En kompetent myndighed kan under visse omstændigheder begrænse visse af den registreredes rettigheder: retten til indsigt ([121]), til at blive informeret ([122]), til at få kendskab til et brud på persondatasikkerheden ([123]) og til at blive informeret om årsagen til et afslag på en anmodning om berigtigelse eller sletning ([124]). I lighed med ordningen i kapitel III i direktiv (EU) 2016/680 kan den kompetente myndighed kun anvende begrænsningen, hvis den under hensyn til den registreredes grundlæggende rettigheder og legitime interesser er nødvendig og står i et rimeligt forhold til følgende: a) undgå at hindre en officiel eller retlig undersøgelse, efterforskning eller procedure, b) undgå at hindre forebyggelse, opdagelse, efterforskning eller retsforfølgning af strafbare handlinger, c) beskytte den offentlige sikkerhed, d) beskytte statens sikkerhed, e) beskytte andres rettigheder og frihedsrettigheder.

(67) ICO har udarbejdet en vejledning om anvendelsen af disse begrænsninger. I henhold til denne vejledning skal dataansvarlige foretage en analyse fra sag til sag for at finde en balance mellem den enkeltes rettigheder og den skade, som videregivelse ville forårsage. De skal navnlig begrunde enhver begrænsning, der anvendes som nødvendig og forholdsmæssig, og må kun begrænse, hvad der er fastsat, hvis det ville skade ovennævnte formål ([125]).

(68) Der findes også en række andre vejledninger fra kompetente myndigheder, som giver detaljerede oplysninger om alle aspekter af databeskyttelseslovgivningen, herunder om anvendelsen af begrænsningerne i de registreredes rettigheder ([126]). I forbindelse med Section 45(4) hedder det f.eks. i Data Protection Manual of the National Police Chief's Counsel: »Det er vigtigt at bemærke, at begrænsningerne kun kan anvendes, i det omfang det er nødvendigt, og at de kun kan anvendes, så længe det er nødvendigt. Følgelig er en generel anvendelse af begrænsningen til alle en ansøgers personoplysninger eller permanent anvendelse af begrænsningen ikke tilladt. Med hensyn til sidstnævnte punkt er det ofte sådan, at personoplysninger, der er indsamlet uden den registreredes kendskab, og denne er mistænkt og indgår i en efterforskning, i første omgang skal beskyttes mod videregivelse til den registrerede for at undgå at skade efterforskningen, mens denne pågår, men på et senere tidspunkt vil der ikke være nogen skade ved videregivelsen, hvis personoplysningerne var blevet videregivet til den pågældende under en afhøring. Politiet skal indføre procedurer, der sikrer, at anvendelsen af disse begrænsninger kun sker, i det omfang det er nødvendigt, og kun så længe det er nødvendigt« ([127]). Denne vejledning indeholder også eksempler på, hvornår hver af begrænsningerne sandsynligvis vil blive anvendt ([128]).

(69) Hvad angår muligheden for at begrænse en hvilken som helst af ovennævnte rettigheder med henblik på beskyttelse af »statens sikkerhed«, kan en dataansvarlig desuden anmode om et certifikat underskrevet af en Cabinet Minister eller af Attorney General (eller Advocate General for Scotland), der bekræfter, at en begrænsning af sådanne rettigheder er en nødvendig og forholdsmæssig foranstaltning til beskyttelse af den nationale sikkerhed ([129]). Den britiske regering har udstedt retningslinjer for nationale sikkerhedscertifikater i henhold til DPA 2018, hvori det navnlig understreges, at enhver begrænsning af registreredes rettigheder med henblik på at beskytte statens sikkerhed skal være forholdsmæssig og nødvendig ([130]) (yderligere oplysninger om de nationale sikkerhedscertifikater findes i betragtning (131)-(134)).

([121]) Section 45(4) i DPA 2018.
([122]) Section 44(4) i DPA 2018.
([123]) Section 68(7) i DPA 2018.
([124]) Section 48(3) i DPA 2018.
([125]) Se f.eks. Guide to Law Enforcement Processing on the right of access, som kan findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Se f.eks. Data Protection Manual for Police Data Protection Professional udgivet af National Police Chief Counsel (se fodnote 27) eller vejledningen fra Serious Fraud Office, som kan findes på følgende link: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Data protection Manual of the National Police Chief Counsel, side 140 (se fodnote 27).
([128]) Data protection Manual of the National Police Chief Counsel fastsætter, at formålet »undgå at hindre en officiel eller retlig undersøgelse, efterforskning eller procedure« sandsynligvis vil være relevant ved personoplysninger, der behandles i forbindelse med henvendelser, familieretlige sager, interne disciplinærundersøgelser og undersøgelser som f.eks. den uafhængige undersøgelse af seksuelt misbrug af børn, mens »beskytte andres rettigheder og frihedsrettigheder« er relevant for personoplysninger, der også vedrører andre personer og den, der fremsætter anmodningen« (Data Protection Manual of the National Police Chief Counsel, side 140, se fodnote 27).
([129]) Section 79 i DPA 2018.
([130]) UK Government Guidance on National Security Certificates 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

(70) Hvis en registrerets rettighed begrænses, skal den kompetente myndighed desuden uden unødig forsinkelse underrette den registrerede om, at vedkommendes rettigheder er blevet begrænset, om årsagerne til begrænsningen og om de tilgængelige klagemuligheder, medmindre det vil undergrave begrundelsen for at anvende begrænsningen, hvis denne oplysning blev meddelt ([131]). Som en yderligere garanti mod misbrug af begrænsninger skal den dataansvarlige registrere årsagerne til begrænsningen af oplysninger og efter anmodning stille registreringen til rådighed for Information Commissioner ([132]).

(71) Hvis den dataansvarlige nægter at give yderligere oplysninger om gennemsigtighed eller indsigt eller afviser en anmodning om berigtigelse, sletning eller begrænsning af behandling, kan den pågældende anmode Information Commissioner om at undersøge, om den dataansvarlige har anvendt begrænsningen på lovlig vis ([133]). Den berørte person kan også indgive en klage til Information Commissioner eller anmode en domstol om at pålægge den dataansvarlige at efterkomme anmodningen ([134]).

2.4.7.2. Automatiske afgørelser

(72) Section 49 og 50 i DPA 2018 dækker henholdsvis rettighederne i forbindelse med automatiske afgørelser og de garantier, der skal anvendes ([135]). I lighed med artikel 11 i direktiv (EU) 2016/680 kan den dataansvarlige kun træffe en væsentlig afgørelse, der alene er baseret på automatisk behandling af personoplysninger, hvis det kræves eller er tilladt ved lov ([136]). En afgørelse er væsentlig, hvis den vil få en negativ retsvirkning for den registrerede eller i væsentlig grad påvirke den registrerede ([137]).

(73) Hvis den dataansvarlige ved lov er forpligtet eller bemyndiget til at træffe en væsentlig afgørelse, fastsætter Section 50 i DPA 2018 de garantier, der gælder for en sådan afgørelse (der defineres som en »kvalificeret væsentlig afgørelse«). Så snart det er praktisk muligt, underretter den dataansvarlige den registrerede om, at der er truffet en sådan afgørelse. Den registrerede kan derefter inden for en måned anmode den dataansvarlige om at tage afgørelsen op til fornyet overvejelse eller træffe en ny afgørelse, der ikke udelukkende er baseret på automatisk behandling. Den dataansvarlige skal behandle anmodningen og underrette den registrerede om resultatet af denne overvejelse. DPA 2018 giver Secretary of State beføjelse til at vedtage bestemmelser om yderligere beskyttelsesforanstaltninger ([138]). Der er endnu ikke vedtaget sådanne bestemmelser.

2.4.8. *Videreoverførsel*

(74) Beskyttelsesniveauet for personoplysninger, der overføres fra en retshåndhævende myndighed i en medlemsstat til en retshåndhævende myndighed i Det Forenede Kongerige, må ikke undermineres af videreoverførslen af sådanne oplysninger til modtagere i et tredjeland. Sådanne »videreoverførsler«, som set fra en britisk retshåndhævelsesmyndigheds 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.

([131]) Section 44(5) og (6), Section 45(5) og (6), Section 48(4) i DPA 2018.
([132]) Section 44(7), Section 45(7), Section 48(6) i DPA 2018.
([133]) Section 51 i DPA 2018.
([134]) Section 167 i DPA 2018.
([135]) Med hensyn til omfanget af automatisk behandling af personoplysninger hedder det i de forklarende bemærkninger til DPA 2018, at: »disse bestemmelser vedrører fuldautomatiske afgørelser og ikke automatisk behandling. Automatisk behandling (herunder profilering) sker, når der udføres en operation på data uden behov for menneskelig indgriben. Dette anvendes regelmæssigt i forbindelse med retshåndhævelse til at filtrere store datasæt ned til håndterbare mængder, som en menneskelig operatør så kan bruge. Automatiske afgørelser er en form for automatisk behandling og kræver, at den endelige afgørelse træffes uden menneskelig indblanding«. (Forklarende noter til DPA, paragraph 204, se fodnote 45).
([136]) Ud over de former for beskyttelse, der er omfattet af DPA, findes der andre begrænsninger fastsat ved lov i Det Forenede Kongeriges lovgivning, som finder anvendelse på retshåndhævelsesinstanser, og som hindrer automatisk behandling (herunder profilering), som resulterer i ulovlig diskriminering. The Human Rights Act 1998 omsætter de rettigheder, der er fastlagt i ECHR, til Det Forenede Kongeriges lovgivning, herunder rettigheden i konventionens artikel 14, forbud mod diskriminering. På samme måde forbyder Equality Act 2010 diskriminering af personer med beskyttede kendetegn (såsom køn, race, handicap osv.).
([137]) Section 49(2) i DPA 2018.
([138]) Section 50(4) i DPA 2018.

(75) Det Forenede Kongeriges ordning om internationale overførsler er reguleret i Chapter 5, Part 3 i DPA 2018 ([139]) og afspejler tilgangen i kapitel V i direktiv (EU) 2016/680. For at overføre personoplysninger til et tredjeland skal en kompetent myndighed navnlig opfylde tre betingelser: a) overførslen skal være nødvendig med henblik på retshåndhævelse, b) overførslen skal baseres på: i) en bestemmelse om beskyttelsesniveauets tilstrækkelighed i forhold til tredjelandet, ii) hvis den ikke er baseret på en bestemmelse om beskyttelsesniveauets tilstrækkelighed, tilstedeværelsen af passende garantier, eller iii) hvis den ikke er baseret på en afgørelse om beskyttelsesniveauets tilstrækkelighed eller de fornødne garantier, skal den være baseret på særlige omstændigheder, og c) modtageren af overførslen skal være: i) en relevant myndighed (dvs. svarende til en kompetent myndighed) i tredjelandet, ii) en »relevant international organisation«, f.eks. et internationalt organ, der varetager funktioner svarende til et hvilket som helst retshåndhævelsesformål eller iii) en anden person end en relevant myndighed, men kun hvis overførslen er strengt nødvendig for at opfylde et af retshåndhævelsesformålene, der ikke er nogen grundlæggende rettigheder og frihedsrettigheder for den pågældende registrerede, som vejer tungere end de samfundsinteresser, der nødvendiggør overførslen, en overførsel af personoplysninger til en relevant myndighed i tredjelandet ville være ineffektiv eller uhensigtsmæssig og modtageren underrettes om de formål, hvortil oplysningerne kan behandles ([140]).

(76) Regler om beskyttelsesniveauets tilstrækkelighed med hensyn til et tredjeland, et område eller en sektor i et tredjeland, en international organisation eller en beskrivelse ([141]) af et sådant land, område, sektor eller organisation fastlægges af Secretary of State. Med hensyn til den standard, der skal opfyldes, skal Secretary of State vurdere, om et sådant område/en sådan sektor/organisation sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger. I Section 74A(4) i DPA 2018 præciseres det, at Secretary of State med henblik herpå skal tage hensyn til en række elementer, der afspejler dem, der er anført i artikel 36 i direktiv 2016/680/EU ([142]). I denne henseende har Part 3 i DPA 2018 siden overgangsperiodens udløb været »afledt national EU-lovgivning«, der som forklaret vil blive fortolket af de britiske domstole i overensstemmelse med relevant retspraksis fra EU-Domstolen, som ligger forud for Det Forenede Kongeriges udtræden af Unionen, og de generelle principper i EU-retten, som de havde virkning umiddelbart inden overgangsperiodens udløb. Dette omfatter standarden for »væsentlig ækvivalens«, som således vil finde anvendelse på de vurderinger af tilstrækkeligheden, der foretages af de britiske myndigheder.

(77) Med hensyn til proceduren er bestemmelserne underlagt de »generelle« procedurekrav, der er fastsat i Section 182 i DPA 2018. I henhold til denne procedure skal Secretary of State rådføre sig med Information Commissioner, når han fremsætter forslag til udarbejdelse af fremtidige britiske bestemmelser om tilstrækkeligheden af beskyttelses-

([139]) Denne nye ramme trådte i kraft ved overgangsperiodens udløb, herunder Secretary of States beføjelse til at udstede bestemmelser om beskyttelsesniveauets tilstrækkelighed. DPPEC-forordningerne (navnlig paragraph 10-12 i Schedule 21, som disse bestemmelser indfører i DPA 2018) fastsætter imidlertid, at visse overførsler af personoplysninger fra og efter overgangsperiodens udløb behandles, som om de er baseret på bestemmelser om tilstrækkelighed. Disse overførsler omfatter overførsler til tredjelande, der er omfattet af en EU-afgørelse om beskyttelsesniveauets tilstrækkelighed ved overgangsperiodens udløb, og til EU-medlemsstater, EFTA-stater og Gibraltar i kraft af deres anvendelse af retshåndhævelsesdirektivet på behandling af retshåndhævelsesoplysninger (EFTA-staterne anvender direktiv 2016/680/EU som følge af deres forpligtelser i henhold til Schengenreglerne). Det betyder, at overførslerne til disse lande ved overgangsperiodens udløb kan fortsætte som før Det Forenede Kongeriges udtræden af EU. Efter overgangsperiodens udløb og inden for fire år skal Secretary of State gennemgå konklusionerne om tilstrækkeligheden.

([140]) Section 73 og 77 i DPA 2018.

([141]) De britiske myndigheder har forklaret, at beskrivelsen af et land eller en international organisation henviser til en situation, hvor det vil være nødvendigt at foretage en specifik og delvis fastlæggelse af tilstrækkeligheden med fokuserede begrænsninger (f.eks. en bestemmelse om tilstrækkeligheden af beskyttelsesniveauet kun i forbindelse med visse typer af dataoverførsler).

([142]) Se Section 74A(4) i DPA 2018, hvori det bestemmes, at ved vurderingen af beskyttelsesniveauets tilstrækkelighed »skal Secretary of State navnlig tage hensyn til a) retsstatsprincippet, respekten for menneskerettighederne og de grundlæggende frihedsrettigheder, den relevante lovgivning, herunder vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og strafferet og offentlige myndigheders adgang til personoplysninger, samt gennemførelsen af en sådan lovgivning, databeskyttelsesregler, faglige regler og sikkerhedsforanstaltninger, herunder regler om videregivelse af personoplysninger til et andet tredjeland eller en international organisation, som overholder disse regler og sikkerhedsforanstaltninger, retspraksis samt effektive rettigheder for registrerede, som kan håndhæves, og effektiv administrativ og retslig prøvelse for de registrerede, hvis personoplysninger overføres, b) tilstedeværelsen af en eller flere velfungerende uafhængige tilsynsmyndigheder i tredjelandet, eller som den internationale organisation er underlagt, med ansvar for at sikre og håndhæve, at databeskyttelsesregler overholdes, herunder tilstrækkelige håndhævelsesbeføjelser, for at bistå og rådgive de registrerede, når de udøver deres rettigheder, og for samarbejde med Information Commissioner, og c) de internationale forpligtelser, som tredjelandet eller den internationale organisation har påtaget sig, eller andre forpligtelser, der følger af retligt bindende konventioner eller instrumenter og af landets eller organisationens deltagelse i multilaterale eller regionale systemer, navnlig vedrørende beskyttelse af personoplysninger«.

niveauet ([143]). Når disse bestemmelser er fastlagt af Secretary of State, forelægges de for parlamentet og er underlagt den »negative beslutningsprocedure«, i henhold til hvilken begge kamre i parlamentet kan gennemgå bestemmelserne og har mulighed for at vedtage et forslag om annullering af bestemmelserne inden for en frist på 40 dage ([144]).

(78) I henhold til Section 74B(1) i DPA 2018 skal tilstrækkelighedsbestemmelserne 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 tilstrækkeligheden af beskyttelsesniveauet eller om at ændre eller ophæve sådanne bestemmelser. Hvis Secretary of State bliver opmærksom på, at et givet land eller en organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, skal han i det omfang, det er nødvendigt, ændre eller ophæve bestemmelserne og indlede drøftelser med det pågældende tredjeland eller den pågældende internationale organisation for at afhjælpe manglen på et tilstrækkeligt beskyttelsesniveau.

(79) I lighed med, hvad der er fastsat i artikel 37 i direktiv (EU) 2016/680, vil det i mangel af bestemmelser om tilstrækkeligheden af beskyttelsesniveauet være muligt at overføre personoplysninger inden for rammerne af retshåndhævelsessektoren, når der er indført passende sikkerhedsforanstaltninger. Sådanne sikkerhedsforanstaltninger sikres ved hjælp af enten a) et retligt bindende instrument, der indeholder de fornødne garantier for beskyttelse af personoplysninger, eller b) en vurdering foretaget af den dataansvarlige, som efter at have vurderet alle omstændighederne i forbindelse med videregivelsen konkluderer, at der foreligger de fornødne sikkerhedsforanstaltninger til at beskytte oplysningerne ([145]). Når overførsler er baseret på passende sikkerhedsforanstaltninger, fastsættes det i DPA 2018 desuden, at de kompetente myndigheder ud over ICO's normale tilsynsrolle skal fremlægge specifikke oplysninger om overførslerne til ICO ([146]).

(80) Hvis en overførsel ikke er baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller de fornødne sikkerhedsforanstaltninger, kan den kun finde sted under visse, nærmere angivne omstændigheder, benævnt »særlige omstændigheder« ([147]). 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 forebygge en umiddelbar og alvorlig trussel mod et tredjelands offentlige sikkerhed, d) i individuelle sager til et hvilket som helst retshåndhævelsesformål eller e) for at opnå et retligt formål i individuelle sager (f.eks. i forbindelse med retssager eller for at indhente juridisk rådgivning) ([148]). Det skal bemærkes, at litra d) og e) ikke finder anvendelse, hvis den registreredes rettigheder og frihedsrettigheder går forud for samfundets interesse i overførslen ([149]). Disse omstændigheder svarer til de særlige situationer og betingelser, der kan betegnes som »undtagelser« i henhold til artikel 38 i direktiv (EU) 2016/680.

(81) Under disse omstændigheder skal dato, klokkeslæt og begrundelse for overførslen, navnet på og alle andre relevante oplysninger om modtageren samt en beskrivelse af de overførte personoplysninger dokumenteres og på anmodning udleveres til Information Commissioner ([150]).

(82) I Section 78 i DPA 2018 reguleres scenariet med »efterfølgende overførsler«, dvs. når personoplysninger, der er blevet overført fra Det Forenede Kongerige til et tredjeland, efterfølgende overføres til et andet tredjeland eller en international organisation. I overensstemmelse med Section 78) 1) skal den overførende dataansvarlige stille som betingelse, at oplysningerne ikke må videregives til et tredjeland uden den overførende dataansvarliges tilladelse. I overensstemmelse med Section 78(3) og svarende til bestemmelserne i artikel 35, stk. 1, litra e) i direktiv (EU) 2016/680 finder en række omfattende krav anvendelse, hvis en sådan tilladelse er påkrævet. Mere specifikt skal en

([143]) Jf. Memorandum of Understanding (aftalememorandum) mellem Secretary of State for the Department for Digital, Culture, Media and Sport (ministeren for det digitale område, kultur, medier og idræt, DCMS) og Information Commissioner's Office om ICO's rolle i relation til en ny vurdering af Det Forenede Kongeriges tilstrækkelighed, der 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.

([144]) I denne periode på 40 dage har begge kamre i parlamentet mulighed for, hvis de ønsker det, at stemme imod bestemmelserne. Hvis der er flertal for det ved en sådan afstemning, vil bestemmelserne i sidste ende ophøre med at have yderligere retsvirkning.

([145]) Section 75 i DPA 2018.

([146]) Section 75(3) i DPA 2018 bestemmer, at når videregivelse af oplysninger sker på grundlag af de fornødne sikkerhedsforanstaltninger: a) skal overførslen dokumenteres, b) skal dokumentationen efter anmodning udleveres til Information Commissioner, og c) skal dokumentationen navnlig omfatte i) dato og tidspunkt for overførslen, ii) navnet på og alle andre relevante oplysninger om modtageren, iii) begrundelsen for overførslen og iv) en beskrivelse af de overførte personoplysninger.

([147]) Guide to Law Enforcement Processing, »Are there any special circumstances?«, som kan findes på følgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) Section 76 i DPA 2018.

([149]) Section 76 i DPA 2018.

([150]) Section 76(3) i DPA 2018.

kompetent myndighed, når den træffer afgørelse om, hvorvidt overførslen skal godkendes eller ej, sikre sig, at den videre overførsel er nødvendig til retshåndhævelsesformål, og bl.a. tage hensyn til a) alvoren af de omstændigheder, der førte til anmodningen om tilladelse, b) det formål, hvortil personoplysningerne oprindeligt blev overført, og c) de standarder for beskyttelse af personoplysninger, der gælder i det tredjeland eller den internationale organisation, som personoplysningerne overføres til.

(83) Hvis de oplysninger, der overføres videre fra Det Forenede Kongerige, oprindeligt blev overført fra EU, finder yderligere beskyttelsesforanstaltninger anvendelse.

(84) For det første fastsættes det i Section 73(1)(b) i DPA) 2016/2018 — på samme måde som i artikel 35, stk. 1, litra c) i direktiv (EU) 2016/680 — at i tilfælde, hvor personoplysningerne oprindeligt blev videregivet eller på anden måde stillet til rådighed for den dataansvarlige eller en anden kompetent myndighed af en medlemsstat, skal den pågældende medlemsstat eller enhver person, der er etableret i den pågældende medlemsstat, og som er en kompetent myndighed i henhold til direktiv (EU) 2016/680, have givet tilladelse til videregivelsen i overensstemmelse med medlemsstatens lovgivning.

(85) I lighed med artikel 35, stk. 2, i direktiv (EU) 2016/680 kræves der imidlertid ikke en sådan tilladelse, hvis a) overførslen er nødvendig for at forebygge en umiddelbar og alvorlig trussel mod enten en medlemsstats eller et tredjelands offentlige sikkerhed eller mod en medlemsstats væsentlige interesser, og b) godkendelsen ikke kan opnås i tide. I så fald skal den myndighed i medlemsstaten, som ville have været ansvarlig for at beslutte, om der skal gives tilladelse til overførslen, straks underrettes ([151]).

(86) For det andet finder samme tilgang anvendelse, hvis oplysninger, som oprindeligt blev overført fra EU til Det Forenede Kongerige, overføres videre fra Det Forenede Kongerige til et tredjeland, som efterfølgende overfører dem videre til et tredjeland. I medfør af Section 78(4) kan Det Forenede Kongeriges myndighed i så fald ikke give sin tilladelse til sidstnævnte overførsel under Section 78(1), medmindre »den medlemsstat [som oprindeligt overførte de pågældende oplysninger], eller en person med hjemsted i den pågældende medlemsstat, som er en kompetent myndighed i overensstemmelse med retshåndhævelsesdirektivet, har givet tilladelse til overførslen i overensstemmelse med lovgivningen i denne medlemsstat«. Disse beskyttelsesforanstaltninger er vigtige, fordi de gør det muligt for medlemsstaternes myndigheder at sikre kontinuitet i beskyttelsen i overensstemmelse med EU's databeskyttelseslov i hele »overførselskæden«.

(87) Denne nye ramme for internationale overførsler trådte i kraft ved overgangsperiodens udløb ([152]). Paragraph 10-12 i Schedule 21 (indført ved DPPC Regulations) 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 medlemsstat, en EFTA-stat, et tredjeland, der er omfattet af en EU-afgørelse om tilstrækkeligheden af beskyttelsesniveauet ved overgangsperiodens udløb, og Gibraltar. Overførslerne til disse lande kan derfor fortsætte som før Det Forenede Kongeriges udtræden af Unionen. Efter overgangsperiodens udløb skal Secretary of State foretage en gennemgang af disse konklusioner om tilstrækkeligheden i en periode på fire år, dvs. inden udgangen af december 2024. Selv om ministeriet skal foretage denne gennemgang inden udgangen af december 2024, indeholder overgangsbestemmelserne ifølge de britiske myndigheder 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.

2.4.9. *Ansvarlighed*

(88) I henhold til ansvarlighedsprincippet skal offentlige myndigheder, der behandler data, indføre passende tekniske og organisatoriske foranstaltninger for effektivt at opfylde deres databeskyttelsesforpligtelser og kunne påvise en sådan overholdelse, navnlig over for den kompetente tilsynsmyndighed.

(89) Dette princip afspejles i Section 56 i DPA 2018, som indfører en generel ansvarlighedsforpligtelse for den dataansvarlige, dvs. en forpligtelse til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og være i stand til at påvise, at behandlingen af personoplysninger er i overensstemmelse med kravene i Part 3 i DPA 2018. De gennemførte foranstaltninger skal revideres og ajourføres, hvor det er nødvendigt, og, hvis det står i rimeligt forhold til behandlingen, omfatte passende databeskyttelsespolitikker.

([151]) Section 73(5) i DPA 2018.

([152]) Anvendelsen af denne nye ramme skal ses 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 af 31.12.2020, s 14) (»TCA EU-UK«), som kan findes på følgende link: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN.

(90) I overensstemmelse med kapitel IV i direktiv (EU) 2016/680 indeholder Section 55-71 i DPA 2018 forskellige mekanismer til at sikre ansvarlighed og give dataansvarlige og databehandlere mulighed for at påvise overensstemmelse. Dataansvarlige skal navnlig gennemføre databeskyttelsesforanstaltninger gennem design og gennem standardindstillinger, dvs. sikre, at databeskyttelsesprincipperne gennemføres effektivt, og de skal føre registre over alle kategorier af behandlingsaktiviteter, som den dataansvarlige er ansvarlig for (herunder oplysninger om den dataansvarliges identitet, kontaktoplysninger for databeskyttelsesrådgiver, formålene med behandlingen, kategorierne af modtagere af oplysninger og en beskrivelse af kategorierne af registrerede og personoplysninger), og efter anmodning stille disse registre til rådighed for Information Commissioner. Den dataansvarlige og databehandleren skal også føre logfiler for visse behandlingsaktiviteter og stille dem til rådighed for Information Commissioner ([153]). Dataansvarlige skal også specifikt samarbejde med Information Commissioner om udførelsen af dennes opgaver.

(91) DPA 2018 fastsætter også yderligere krav til behandling, som sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Disse omfatter en forpligtelse til at foretage konsekvensanalyser vedrørende databeskyttelse og til at rådføre sig med Information Commissioner forud for behandlingen, hvis en sådan vurdering viser, at behandlingen vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder (hvis der ikke træffes foranstaltninger til at mindske risikoen).

(92) Dataansvarlige skal endvidere udpege en databeskyttelsesrådgiver, medmindre den dataansvarlige er en domstol eller en anden judiciel myndighed, der handler i sin judicielle egenskab ([154]). Den dataansvarlige skal sikre, at den databeskyttelsesansvarlige er involveret i alle spørgsmål vedrørende beskyttelse af personoplysninger, har de nødvendige ressourcer og adgang til personoplysninger og behandlingsaktiviteter og kan udføre sine opgaver uafhængigt. Den databeskyttelsesansvarliges opgaver er beskrevet i Section 71 i DPA 2018, herunder information og rådgivning, overvågning af overholdelsen samt samarbejde med og varetagelse af funktionen som kontaktpunkt for Information Commissioner. Den databeskyttelsesansvarlige skal ved udførelsen af sine opgaver tage hensyn til de risici, der er forbundet med behandlingsaktiviteter, under hensyntagen til behandlingens art, omfang, kontekst og formål.

2.5. **Kontrol og håndhævelse**

2.5.1. *Uafhængig kontrol*

(93) For at garantere, at der også i praksis sikres et tilstrækkeligt databeskyttelsesniveau, skal der oprettes en uafhængig tilsynsmyndighed, der har beføjelser til at overvåge og håndhæve overholdelsen af databeskyttelsesreglerne. Denne myndighed skal handle fuldstændig uafhængigt og upartisk ved udførelsen af sine opgaver og udøvelsen af sine beføjelser.

(94) I Det Forenede Kongerige varetages tilsynet med og håndhævelsen af UK GDPR og DPA 2018 af Information Commissioner ([155]). Information Commissioner fører også kontrol med de kompetente myndigheders behandling af personoplysninger, der er omfattet af Part 3 i DPA 2018 ([156]). Information Commissioner er en »Corporation Sole«: en særskilt juridisk enhed, der består af en enkelt person. Information Commissioner bistås i sit arbejde af et kontor. Den 31. marts 2020 havde Information Commissioner's kontor 768 fastansatte medarbejdere ([157]). Information Commissioner er underlagt Department for Digital, Culture, Media and Sport ([158]).

([153]) Section 62 i DPA 2018.
([154]) Section 69 i DPA 2018.
([155]) Artikel 36, stk. 2, litra b), i direktiv (EU) 2016/680.
([156]) Section 116 i DPA 2018.
([157]) Information Commissioner's 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.
([158]) Forholdet mellem de to er fastlagt i en forvaltningsaftale. DCMS's centrale ansvarsområder som ansvarligt ministerium omfatter navnlig: sikring af, at ICO råder over tilstrækkelige økonomiske midler og ressourcer, at repræsentere ICO's interesser over for parlamentet og andre ministerier, at sikre, at der findes en solid national databeskyttelsesramme og at yde vejledning og støtte til ICO om driftsmæssige spørgsmål såsom ejendomsspørgsmål, lejemål og offentlige indkøb (Management Agreement 2018-2021 findes på følgende link: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).).

(95) Information Commissioners uafhængighed er udtrykkeligt fastsat i artikel 52 i UK GDPR, som afspejler kravene i artikel 52, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([159]). 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 med disse opgaver og beføjelser og hverken søge eller modtage instrukser fra nogen. Information Commissioner skal også afholde sig fra enhver handling, der er uforenelig med hans eller hendes hverv, og vedkommende må under udøvelsen af sit hverv ikke udøve nogen form for lønnet eller ulønnet uforenelig beskæftigelse.

(96) Betingelserne for udpegelse og afskedigelse af Information Commissioner er fastsat i Schedule 12 til DPA 2018. Information Commissioner udnævnes af dronningen efter indstilling fra regeringen efter en fair og åben udvælgelsesprøve. Ansøgeren skal have relevante kvalifikationer, færdigheder og kompetencer. I overensstemmelse med reglerne om offentlige udnævnelser (Governance Code on Public Appointments) ([160]) udarbejder et rådgivende vurderingsudvalg en liste over kandidater, der kan udnævnes. Inden Secretary of State 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 ([161]).

(97) Information Commissioner har en mandatperiode på op til syv år. Dronningen kan afskedige Information Commissioner på forslag fra begge parlamentets kamre. ([162]) En anmodning om afskedigelse af Information Commissioner kan ikke indgives til nogen af parlamentets kamre, medmindre en minister har forelagt det pågældende kammer en rapport, hvoraf det fremgår, at han eller hun finder det godtgjort, at Information Commissioner har begået en alvorlig forseelse, og/eller at Information Commissioner ikke længere opfylder de nødvendige betingelser for at varetage sine opgaver som Information Commissioner ([163]).

(98) Finansieringen af Information Commissioner kommer fra tre kilder: i) gebyrer for databeskyttelse betalt af dataansvarlige, som er fastsat i en ministeriel bekendtgørelse ([164]), og som udgør 85-90 % af kontorets årlige budget ([165]), ii) tilskud, som regeringen kan udbetale til Information Commissioner, og som hovedsagelig anvendes til at finansiere Information Commissioners driftsomkostninger i forbindelse med opgaver, der ikke vedrører databeskyttelse ([166]), og iii) gebyrer for tjenesteydelser ([167]). På nuværende tidspunkt opkræves der ikke sådanne gebyrer.

(99) Information Commissioners generelle opgaver i forbindelse med behandling af personoplysninger, der er omfattet af Part 3 i DPA 2018, er fastlagt i Schedule 13 til DPA 2018. Opgaverne omfatter overvågning og håndhævelse af Part 3 i DPA 2018, styrkelse af offentlighedens bevidsthed, rådgivning af parlamentet, regeringen og andre institutioner om lovgivningsmæssige og administrative foranstaltninger, fremme af de dataansvarliges og databehandlernes kendskab til deres forpligtelser, underretning af registrerede om udøvelsen af registreredes rettigheder og

([159]) 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) (EUT L 119 af 4.5.2016, s. 1).

([160]) Governance Code on Public Appointments kan findes på følgende link: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) 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.

([162]) Der er tale om et forslag, som forelægges Parlamentet, og som har til formål at gøre monarken opmærksom på Parlamentets holdning vedrørende et bestemt emne.

([163]) Schedule 12, paragraph 3, til DPA 2018.

([164]) Section 137 i DPA 2018.

([165]) Section 137 og 138 i DPA 2018 indeholder en række garantier, der skal sikre, at disse afgifter fastsættes på et passende niveau. Navnlig opregnes i Section 137(4) i DPA 2018 de forhold, som Secretary of State skal tage hensyn til, når denne udsteder bestemmelser, der fastsætter det beløb, som forskellige organisationer skal betale. Section 138(1) og Section 182 i DPA 2018 indeholder 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 fremlægges, således at der kan tages hensyn til deres synspunkter. I henhold til Section 138(2) i DPA 2018 skal Information Commissioner desuden føre tilsyn med, hvordan gebyrbestemmelserne fungerer, og 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 hvilket 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.

([166]) I forvaltningsaftalen præciseres det, at »ministeriet 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, se fodnote 158).

([167]) Section 134 i DPA 2018.

gennemførelse af undersøgelser. For at bevare retsvæsenets uafhængighed har Information Commissioner ikke bemyndigelse til at udøve sine funktioner i forbindelse med behandling af personoplysninger foretaget af en person, der handler i en judiciel egenskab, eller en ret eller en domstol, der handler i sin judicielle egenskab. Tilsynet med retsvæsenet varetages imidlertid af specialiserede organer, jf. nedenfor.

2.5.1.1 Håndhævelse, herunder sanktioner

(100) Information Commissioner har generelle undersøgelses-, korrektions-, godkendelses- og rådgivningsbeføjelser i forbindelse med behandling af personoplysninger, som Part 3 i DPA 2018 finder anvendelse på. Information Commissioner har beføjelse til at underrette den dataansvarlige eller databehandleren om en påstået overtrædelse af Part 3, til at udstede advarsler til en dataansvarlig eller databehandler om, at planlagte behandlingsaktiviteter sandsynligvis vil være i strid med bestemmelserne i Part 3, og til at udstede irettesættelser til en dataansvarlig eller databehandler, hvis behandlingsaktiviteter har overtrådt bestemmelserne i Part 3. Desuden kan Information Commissioner på eget initiativ eller efter anmodning afgive udtalelser til Det Forenede Kongeriges parlament, regeringen eller andre institutioner og organer samt offentligheden om ethvert spørgsmål vedrørende beskyttelse af personoplysninger ([168]).

(101) Desuden har Information Commissioner beføjelser til at:

— 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«) ([169]),

— foretage undersøgelser og revisioner ved at udstede et assessment notice (vurderingsvarsel), 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 (»assessment notice«) ([170])

— på anden måde få adgang til dataansvarliges og databehandleres dokumenter og adgang til deres lokaler i overensstemmelse med Section 154 i DPA 2018 (»powers of entry and inspection«, beføjelser til at skaffe sig adgang og foretage inspektion)

— udøve korrigerende beføjelser, herunder ved hjælp af advarsler og irettesættelser, eller udstede påbud ved hjælp af en enforcement notice (håndhævelsesmeddelelse), som pålægger dataansvarlige/databehandlere at tage eller undlade at tage bestemte skridt (»enforcement notice«) ([171]) og

— udstede administrative bøder i form af et »penalty notice« (bødeforlæg) ([172]).

(102) ICO's Regulatory Action Policy fastsætter de omstændigheder, hvorunder Information Commissioner vil udstede henholdsvis en information, assessment, enforcement og penalty notice ([173]). Enforcement notice kan indeholde krav, som Information Commissioner finder hensigtsmæssige med henblik på at afhjælpe den manglende overholdelse. Penalty notice pålægger den pågældende at betale et beløb, der er angivet i afgørelsen, til Information Commissioner. Der kan udstedes en penalty notice, hvis visse bestemmelser i DPA 2018 ([174]) er blevet overtrådt, eller den kan rettes til en en dataansvarlig eller en databehandler der ikke har efterkommet en information notice, en assessment notice eller en enforcement notice.

(103) Mere specifikt skal Information Commissioner ved afgørelsen af, om der skal udstedes en penalty notice til en dataansvarlig eller en databehandler, og fastsættelsen af bødens størrelse, tage hensyn til de forhold, der er anført i Section 155(3) i DPA 2018, herunder arten og alvoren af den manglende overholdelse, den forsætlige eller uagtsomme karakter af den manglende overholdelse, enhver foranstaltning, som den dataansvarlige eller databehandleren har truffet for at begrænse den skade, som de registrerede har lidt, omfanget af den dataansvarliges

([168]) Paragraph 2 i Schedule 13 til DPA 2018.
([169]) Section 142 i DPA 2018 (med forbehold af begrænsningerne i Section 143 i DPA 2018).
([170]) Section 146 i DPA 2018 (med forbehold af begrænsningerne i Section 147 i DPA 2018).
([171]) Section 149-151 i DPA 2018 (med forbehold af begrænsningerne i Section 152 i DPA 2018).
([172]) Section 155 i DPA 2018 (med forbehold af begrænsningerne i Section 156 i DPA 2018).
([173]) Regulatory Action Policy kan findes på følgende link: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) ICO kan navnlig udstede en penalty notice for manglende overholdelse som fastsat i Section 149(2), (3), (4) eller (5) i DPA 2018.

eller databehandlerens ansvar (under hensyntagen til de tekniske og organisatoriske foranstaltninger, som den dataansvarlige eller databehandleren har gennemført), eventuelle relevante tidligere fejl fra den dataansvarliges eller databehandlerens side, de kategorier af personoplysninger, der berøres af den manglende overholdelse, og hvorvidt sanktionen vil være effektiv, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

(104) Maksimumsbeløbet for den sanktion, der kan pålægges ved en penalty notice, er a) 17 500 000 GBP for manglende overholdelse af databeskyttelsesprincipperne (Section 35, 36, 37, 38(1), 39(1) og 40 i DPA 2018), gennemsigtighedsforpligtelser og individuelle rettigheder (Section 44, 45, 46, 47, 48, 49 og 52 i DPA 53) og principper for internationale overførsler af personoplysninger (Section 73, 75, 76, 77 eller 77 i DPA 2018), og b) 8 700 000 GBP i øvrigt ([175]). For så vidt angår manglende efterkommelse af en information notice, en assessment notice eller en enforcement notice er maksimumsbeløbet for den sanktion, der kan pålægges ved en bødeafgørelse 17 500 000 GBP.

(105) I henhold til sine seneste årsberetninger (2018-2019 ([176]), 2019-2020 ([177])) har Information Commissioner gennemført en række undersøgelser i forbindelse med strafferetsretshåndhævende myndigheders behandling af personoplysninger. Information Commissioner gennemførte f.eks. en undersøgelse og offentliggjorde i oktober 2019 en udtalelse om brugen af ansigtsgenkendelsesteknologi på offentlige steder i forbindelse med retshåndhævelse. Undersøgelsen fokuserede især på brugen af live-ansigtsgenkendelse hos South Wales Police og Metropolitan Police Service (MPS). Desuden undersøgte Information Commissioner MPS's »Gangs matrix« ([178]) og konstaterede en række alvorlige overtrædelser af databeskyttelseslovgivningen, som sandsynligvis ville undergrave offentlighedens tillid til matricen og anvendelsen af dataene.

(106) I november 2018 udstedte Information Commissioner en enforcement notice, og MPS tog efterfølgende de nødvendige skridt til at øge sikkerheden og ansvarligheden og sikre, at dataene blev anvendt forholdsmæssigt.

(107) Et andet eksempel på en nylig håndhævelsesforanstaltning er den bøde på 325 000 GBP, som Information Commissioner udstedte i maj 2018 til Crown Prosecution Service for at have mistet ukrypterede DVD'er med optagelser af politiafhøringer. Desuden gennemførte Information Commissioner undersøgelser af bredere emner, f. eks. i første halvdel af 2020 om brugen af dataudtræk fra mobiltelefoner til politimæssige formål og politiets behandling af ofrenes data.

(108) Ud over de håndhævelsesbeføjelser, som Information Commissioner har, udgør visse overtrædelser af databeskyttelseslovgivningen overtrædelser af straffeloven og kan derfor gøres til genstand for strafferetlige sanktioner (Section 196 i DPA 2018). Dette gælder f.eks. indsamling eller videregivelse af personoplysninger uden den dataansvarliges samtykke og videregivelse af personoplysninger til en anden person uden den dataansvarliges samtykke ([179]), genidentifikation af oplysninger, der er anonymiserede personoplysninger, uden samtykke fra den dataansvarlige, som er ansvarlig for anonymiseringen af personoplysningerne ([180]), forsætligt at hindre Information Commissioner i at udøve sine beføjelser i forbindelse med kontrol af personoplysninger i overensstemmelse med internationale forpligtelser ([181]), afgivelse af falske erklæringer i forbindelse med svar på en information notice eller tilintetgørelse af oplysninger i forbindelse med information og assessment notices ([182]).

(109) I henhold til Section 139 i DPA 2018 har Information Commissioner også pligt til at forelægge hvert af parlamentets kamre en generel beretning om udøvelsen af sine funktioner i henhold til loven ([183]).

([175]) Section 157 i DPA 2018.

([176]) Information Commissioner's årsberetning og årsregnskab for 2018-2019 kan findes på følgende link: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Information Commissioners årsberetning 2019-2020 (se fodnote 157).

([178]) En database med oplysninger om påståede bandemedlemmer og ofre for banderelaterede forbrydelser.

([179]) Section 170 i DPA 2018.

([180]) Section 171 i DPA 2018.

([181]) Section 119 i DPA 2018.

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

([183]) Som fastsat i Management Agreement skal årsberetningen: i) omfatte alle selskaber, datterselskaber eller joint ventures, som ICO har bestemmende indflydelse på, ii) overholde finansministeriets Financial Reporting Manual (håndbog for rapportering af finansielle oplysninger, FReM), iii) indeholde en forvaltningserklæring, som beskriver, hvordan regnskabsføreren har forvaltet og kontrolleret de ressourcer, der anvendes i organisationen i løbet af året, og som viser, hvor godt organisationen håndterer risici med hensyn til opfyldelsen af sine formål og mål, og iv) skitsere de vigtigste aktiviteter og resultater i det foregående regnskabsår og fremlægge sammenfatninger af fremtidige planer (Management Agreement 2018-2021, paragraph 3.26, se fodnote 158).

2.5.2. *Kontrol med retsvæsenet*

(110) Domstolene og retsvæsenet fører dobbelt kontrol med behandlingen af personoplysninger. Hvis en indehaver af et judicielt embede eller en domstol ikke handler i en judiciel egenskab, sørger Information Commissioner for kontrollen. Hvis den dataansvarlige fungerer som retsmyndighed, kan ICO ikke udøve sine tilsynsfunktioner ([184]), og tilsynet udføres af særlige organer. Dette afspejler tilgangen i artikel 32 i direktiv (EU) 2016/680.

(111) 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 ([185]). Desuden har Lord Chief Justice (retspræsidenten) og Senior President of Tribunals udstedt en »Privacy Notice« (meddelelse om beskyttelse af personoplysninger) ([186]) som beskriver, hvordan domstolene i England og Wales behandler personoplysninger i forbindelse med domstolsfunktioner. De nordirske ([187]) og skotske domstole ([188]) har udstedt en lignende meddelelse.

(112) I Nordirland har Lord Chief Justice i Nordirland desuden udnævnt en dommer ved High Court til Data Supervisory Judge (datatilsynsdommer, DSJ) ([189]). De har også vejledt det nordirske retsvæsen om, hvad det 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 ([190]).

(113) I Skotland har Lord President udpeget en tilsynsførende dommer til at undersøge eventuelle klager vedrørende databeskyttelse. Dette er fastsat i reglerne om retlige klager (judicial complaints), der afspejler reglerne for England og Wales ([191]).

(114) Endelig udpeges der i Supreme Court en af Supreme Court Justices til at føre kontrol med databeskyttelsen.

([184]) Section 117 i DPA 2018.

([185]) Panelet har ansvaret for at yde vejledning og uddanne retsvæsenet. Det behandler også klager fra registrerede i forbindelse med domstoles, retters og enkeltpersoners behandling af personoplysninger. Panelet har til formål at tilvejebringe de midler, som medfører, at en klagesag kan afgøres. 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. Selv om panelet ikke selv pålægger økonomiske sanktioner, kan det, hvis det mener, at der foreligger en tilstrækkeligt alvorlig overtrædelse af DPA 2018, henvise sagen til Judicial Conduct Investigation Office (kontoret for retslig efterforskning af adfærd, JCIO), 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, hvorpå JCIO har undersøgt klagen, kan vedkommende desuden klage til Judicial Appointments and Conduct Ombudsman (ombudsmanden for udnævnelse og adfærd (se https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsmanden har beføjelse til at anmode JCIO om at genoptage en klagesag og kan foreslå, at klageren får erstatning, hvis ombudsmanden mener, at klageren har lidt skade som følge af fejl eller forsømmelser.

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

([187]) »Privacy Notice« fra Lord Chief Justice of Northern Ireland kan findes på følgende link: https://judiciaryni.uk/data-privacy.

([188]) »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

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

([190]) 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

([191]) Enhver klage, der er begrundet, behandles 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 domstolsmedlemmer, som kan findes på følgende link: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Klageadgang*

(115) 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.

(116) For det første har den registrerede ret til at indgive en klage til Information Commissioner, hvis den registrerede mener, at der i forbindelse med personoplysninger om vedkommende er sket en overtrædelse af Part 3 i DPA 2018 ([192]). Som beskrevet i betragtning (100) og (109) ovenfor har Information Commissioner beføjelse til at vurdere den dataansvarliges og databehandlerens overholdelse af DPA 2018, pålægge dem at træffe eller undlade at træffe bestemte foranstaltninger i tilfælde af manglende overholdelse og pålægge bøder.

(117) For det andet giver DPA 2018 klageadgang over for Information Commissioner. Hvis Information Commissioner ikke »gør fremskridt« ([193]) med en klage indgivet af den registrerede, har klageren adgang til retsmidler, idet denne kan anmode First Tier Tribunal ([194]) om at pålægge Information Commissioner at træffe passende foranstaltninger til at reagere på klagen eller underrette klageren om forløbet af klagen ([195]). Desuden kan enhver person, der modtager en af ovennævnte notices (information, assessment, enforcement eller penalty notice) fra Information Commissioner, appellere til en First Tier Tribunal. Hvis First Tier Tribunal finder, at Information Commissioners afgørelse ikke er i overensstemmelse med loven, eller at Information Commissioner burde have udøvet sin skønsbeføjelse anderledes, skal retten tage appellen til følge eller erstatte den pågældende notice med en anden notice eller afgørelse, som Information Commissioner kunne have udstedt eller truffet ([196]).

(118) For det tredje kan enkeltpersoner anlægge sag direkte mod dataansvarlige og databehandlere ved domstolene i henhold til 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. I henhold til Section 169 i DPA 2018 har enhver, der lider 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.

(119) For det fjerde kan enhver person, som mener, at vedkommendes 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. De dataansvarlige i henhold til Part 3 i DPA 2018, dvs. de kompetente myndigheder, er altid offentlige myndigheder som omhandlet i Human Rights Act 1998. En person, der hævder, at en offentlig myndighed har handlet (eller agter at handle) på en måde, der er uforenelig med en konventionsrettighed 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, når vedkommende er (eller ville være blevet) offer for den ulovlige handling ([197]).

([192]) Section 165 i DPA 2018.

([193]) Section 166 i DPA 2018 omhandler specifikt følgende situationer: a) Information Commissioner undlader at træffe passende foranstaltninger til 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 tre måneder, der indledes på det tidspunkt, hvor Information Commissioner modtager klagen, eller c) Information Commissioner, hvis dennes behandling af klagen ikke er afsluttet i løbet af denne periode, undlader at give klageren sådanne oplysninger i en efterfølgende periode på tre måneder.

([194]) 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.

([195]) Section 166 i DPA 2018.

([196]) Section 161 og 162 i DPA 2018.

([197]) Se sag *Brown v Commissioner* of the Met 2016, hvor retten tilkendte sagsøger erstatning i databeskyttelsessammenhæng i en sag anlagt mod politiet. Retten gav sagsøgeren medhold i hendes påstand om tilsidesættelse af forpligtelserne i DPA 1998, tilsidesættelse af HRA 1998 (og den beslægtede rettighed i EMRK's artikel 8) og erstatning for misbrug af private oplysninger (sagsøgte erkendte i sidste ende, at de havde overtrådt databeskyttelsesloven og EMRK, hvorfor dommen fokuserede på, hvilket retsmiddel der var passende). Som følge af disse tilsidesættelser tilkendte retten sagsøgeren økonomisk erstatning.

(120) Hvis retten fastslår, at en offentlig myndigheds handling er ulovlig, kan den inden for rammerne af sine beføjelser udstede den kendelse og give adgang til de retsmidler og den oprejsning, som den finder retfærdige og passende ([198]). Retten kan også erklære en primærretlig bestemmelse uforenelig med en rettighed, der er sikret ved EMRK.

(121) Endelig kan en person efter at have udtømt de nationale retsmidler indbringe en klage for Den Europæiske Menneskerettighedsdomstol for krænkelser af de rettigheder, der er sikret i henhold til EMRK.

2.6. **Videredeling**

(122) Det Forenede Kongeriges lovgivning tillader, at en retshåndhævende myndighed deler data med andre myndigheder til andre formål end dem, hvortil de oprindeligt blev indsamlet (såkaldt »videredeling«), på visse betingelser.

(123) 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 forholdsmæssig ([199]). I dette tilfælde finder alle de garantier, der er fastsat i Part 3 i DPA 2018 og analyseret ovenfor, anvendelse på den behandling, der foretages af den modtagende myndighed.

(124) I Det Forenede Kongeriges retsorden tillader forskellige love udtrykkeligt videredeling. Navnlig giver i) 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 ([200]), eller i tilfælde af gæld til en offentlig myndighed eller Kronen ([201]), ii) Crime and Courts Act 2013 (lov om kriminalitet og domstole) tillader udveksling af oplysninger med National Crime Agency (NCA) ([202]) med henblik på at bekæmpe, efterforske og retsforfølge grov og organiseret kriminalitet, iii) Serious Crime Act 2007 (lov om grov kriminalitet) giver offentlige myndigheder mulighed for at videregive oplysninger til organisationer, der bekæmper svig, med henblik på at forebygge svig ([203]).

(125) I disse love fastsættes det udtrykkeligt, at udvekslingen af oplysninger skal være i overensstemmelse med de regler, der er fastsat i DPA 2018. Desuden har College of Policing udstedt en vejledning i informationsudveksling, Authorised Professional Practice on Information Sharing ([204]), for at bistå politiet med at opfylde deres databeskyttelsesforpligtelser i henhold til UK GDPR, DPA og Human Rights Act 1998. Udvekslingens overensstemmelse med de gældende retlige rammer for databeskyttelse er naturligvis underlagt domstolskontrol ([205]).

(126) 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 et retshåndhævelsesformål, når behandlingen er tilladt ved lov ([206]). Denne type deling dækker to scenarier: 1) når en strafferetlig retshåndhævende myndighed deler oplysninger med en anden retshåndhævende myndighed end en efterretningsmyndighed (f.eks. en finans- eller skattemyndighed, en konkurrencemyndighed,

([198]) Section 8(1) i Human Rights Act 1998.
([199]) Section 36(3) i DPA 2018.
([200]) Section 56 i Digital Economy Act 2017, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2017/30/contents.
([201]) Section 48 i Digital Economy Act 2017.
([202]) Section 7 i Crime and Courts Act 2013, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2013/22/contents
([203]) Section 68 i Serious Crime Act 2007, som kan findes på følgende link: https://www.legislation.gov.uk/ukpga/2007/27/contents.
([204]) Authorised Professional Practice on Information Sharing findes på følgende link: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.
([205]) Se f.eks. *M 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 datadelingen, der fandt sted på grundlag af en aftale, som havde til formål at beskytte offentligheden og forebygge kriminalitet, og konkluderede, at de fleste aspekter af datadelingen var lovlige, undtagen i forbindelse med visse følsomme oplysninger, der blev delt mellem politiet og BCRP. Et andet eksempel er sagen Cooper v NCA [2019] EWCA Civ 16, hvor Court of Appeal stadfæstede dataudvekslingen mellem politiet og Serious Organised Crime Agency (agenturet for grov organiseret kriminalitet, SOCA), en retshåndhævende myndighed, der i øjeblikket er en del af National Crime Agency.
([206]) Section 36(4) i DPA 2018.

ungdomsforsorgen), 2) når en strafferetlig retshåndhævende myndighed 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. Som anført i afgørelsen vedtaget i henhold til forordning (EU) 2016/679 sikrer de garantier, der er fastsat i UK GDPR og Part 2 i DPA 2018, et beskyttelsesniveau, der i det væsentlige svarer til det beskyttelsesniveau, som ydes i Unionen ([207]).

(127) I det andet scenarie, for så vidt angår udveksling af data indsamlet af en strafferetlig retshåndhævende myndighed med en efterretningstjeneste af hensyn til statens sikkerhed, er retsgrundlaget for en sådan udveksling Counter Terrorism Act 2008 (lov om terrorbekæmpelse fra 2008, CTA 2008) ([208]). I henhold til CTA 2008 kan enhver person give oplysninger til en hvilken som helst efterretningstjeneste med henblik på varetagelse af en hvilken som helst af denne tjenestes funktioner, herunder »statens sikkerhed«.

(128) Med hensyn til betingelserne for udveksling af oplysninger af hensyn til statens sikkerhed begrænser Intelligence Services Act og Security Services Act efterretningstjenesternes mulighed for at indhente data til, hvad der er nødvendigt for at udføre deres lovbestemte opgaver. De kompetente myndigheder, der er omfattet af Part 3 i DPA 2018, og som ønsker at dele data med efterretningstjenesterne, skal overveje en række faktorer/begrænsninger ud over de lovbestemte funktioner, der er fastsat i Intelligence Services Act og Security Services Act ([209]). Section 20 i CTA 2008 præciserer, at enhver datadeling i henhold til Section 19 i CTA 2008 stadig skal være i overensstemmelse med databeskyttelseslovgivningen Det betyder, at alle begrænsninger og krav i DPA 2018 finder anvendelse. Endvidere er de retshåndhævende myndigheder og efterretningstjenesterne offentlige myndigheder som omhandlet i Human Rights Act 1998 og skal således sikre, at de handler i overensstemmelse med de rettigheder, der er garanteret i henhold til EMRK, herunder dennes artikel 8. Med andre ord betyder disse krav, at al datadeling mellem retshåndhævende myndigheder og efterretningstjenester skal være i overensstemmelse med databeskyttelseslovgivningen og EMRK.

(129) Efterretningstjenesternes behandling af personoplysninger, der er modtaget eller indhentet fra retshåndhævende myndigheder af hensyn til statens sikkerhed, er underlagt en række betingelser og garantier ([210]). Part 4 i DPA 2018 finder anvendelse på al behandling, der udføres af eller på vegne af efterretningstjenesterne. Den fastsætter de

([207]) Kommissionens gennemførelsesafgørelse i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Det Forenede Kongerige C(2021)4800.

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

([209]) Section 2, stk. 2, i Intelligence Services Act 1994 (se https://www.legislation.gov.uk/ukpga/1994/13/contents) 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 for at fremme et politisk parti i Det Forenede Kongeriges interesser«, mens Section 2(2) i Security Service Act 1989 (se https://www.legislation.gov.uk/ukpga/1989/5/contents) bestemmer, 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 videregives af disse, medmindre det er nødvendigt af hensyn til dette formål eller med henblik på at forebygge grov kriminalitet], og b) at tjenesten ikke foretager sig noget for at fremme et politisk partis interesser, og 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, det nationale kriminalitetsagenturs og andre retshåndhævende myndigheders aktiviteter«.

([210]) Garantier og begrænsninger i efterretningstjenesternes beføjelser reguleres også af Investigatory Powers Act 2016, som sammen med Regulation of Investigatory Powers Act 2000 for England, Wales og Nordirland og Regulation of Investigatory Powers (Scotland) Act 2000 for Skotland fastsætter retsgrundlaget for anvendelsen af sådanne beføjelser. Disse beføjelser er imidlertid ikke relevante i forbindelse med »videredeling«, da de omfatter efterretningstjenesternes direkte indsamling af personoplysninger. For en vurdering af de beføjelser, som efterretningstjenesterne har i medfør af Investigatory Powers Act, se Kommissionens gennemførelsesafgørelse i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Det Forenede Kongerige C(2021) 4800.

vigtigste databeskyttelsesprincipper (lovlighed, rimelighed og gennemsigtighed ([211]), formålsbegrænsning ([212]), dataminimering ([213]), nøjagtighed ([214]), opbevaringsbegrænsning ([215]) og -sikkerhed ([216]), fastsætter betingelser for behandlingen af særlige kategorier af oplysninger ([217]), fastsætter de registreredes rettigheder ([218]), kræver indbygget databeskyttelse ([219]) og regulerer international videreoverførsel af personoplysninger ([220]).

(130) Samtidig indeholder Section 110 i DPA 2018 en undtagelse fra bestemte bestemmelser i Part 4 i DPA 2018, når en sådan undtagelse er nødvendig af hensyn til statens sikkerhed. 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 Commissioner's undersøgelsesbeføjelser i overensstemmelse med internationale forpligtelser, visse af Information Commissioner's 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. Denne undtagelse kan gøres gældende på grundlag af en vurdering af den konkrete sag ([221]). Som forklaret af de britiske 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« ([222]). ICO fører tilsyn med, om undtagelser er blevet anvendt korrekt ([223]).

([211]) I henhold til Section 86(6) i DPA 2018 skal der med henblik på at fastslå databehandlingens rimelighed og gennemsigtighed tages hensyn til den metode, der anvendes til at indsamle oplysningerne. I den forstand opfyldes kravet om rimelighed og gennemsigtighed, hvis oplysningerne indsamles fra en person, der er lovligt bemyndiget eller forpligtet til at levere dem.

([212]) 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) kan kompatibel viderebehandling af personoplysninger 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 dette andet formål. Behandlingen bør anses for at være forenelig, hvis behandlingen 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).

([213]) Personoplysninger skal være tilstrækkelige, relevante og ikke for omfattende (Section 88 i DPA 2018).

([214]) Personoplysninger skal være korrekte og ajourførte (Section 89 i DPA 2018).

([215]) Personoplysninger må ikke opbevares længere end nødvendigt (Section 90 i DPA 2018).

([216]) Det sjette databeskyttelsesprincip er, at personoplysninger skal behandles på en måde, hvor der træffes passende sikkerhedsforanstaltninger for så vidt angår risici, der opstår som følge af behandlingen af personoplysninger. Risiciene 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 indføre sikkerhedsforanstaltninger, der er passende i forhold til de risici, der opstår som følge af behandling af personoplysninger, og (2) i tilfælde af automatisk behandling træffer hver dataansvarlig og hver databehandler forebyggende eller afhjælpende foranstaltninger baseret på en risikovurdering.

([217]) Section 86(2)(b) og Schedule 10 til DPA 2018.

([218]) Chapter 3 i Part 4 i DPA 2018, navnlig retten til adgang, berigtigelse og sletning, at gøre indsigelse mod behandlingen og ikke at være underlagt automatisk beslutningstagning, at gribe ind i automatiske afgørelser og at blive informeret om beslutningstagningen. Desuden skal den dataansvarlige give den registrerede oplysninger om behandlingen af vedkommendes personoplysninger.

([219]) Section 103 i DPA 2018.

([220]) 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 og Intelligence Services Act 1994.

([221]) Se sag *Baker v Secretary of State for the Home Department* [2001] UKit NSA2 (»Baker mod Secretary of State«).

([222]) UK Explanatory Framework for Adequacy Discussions, Section H: National Security Data Protection and Investigatory Powers Framework, side 15-16, som kan på følgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Se også dommen i sagen *Baker mod Secretary of State* (se fodnote 220), 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 den statens sikkerhed.

([223]) Se Memorandum of Understanding mellem ICO og UKIC, ifølge hvilket det gælder, at »når ICO modtager en klage fra en registreret, skal ICO sikre sig, at spørgsmålet er blevet behandlet korrekt, og, hvor det er relevant, at anvendelsen af en eventuel undtagelse er blevet anvendt korrekt« (Memorandum of Understanding between Information Commissions Office and the Det Forenede Kongerige Intelligence Community, paragraph 16, som kan findes på følgende link: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Hvad angår muligheden for at begrænse en hvilken som helst af ovennævnte rettigheder til beskyttelse af »statens sikkerhed«, fastsættes det endvidere i section 79 i DPA 2018, at en dataansvarlig kan anmode om et certifikat, der er underskrevet af en Cabinet Minister eller Attorney General, og som bekræfter, at en begrænsning af sådanne rettigheder til enhver tid er en nødvendig og forholdsmæssig foranstaltning til beskyttelse af statens sikkerhed ([224]). Den britiske regering har udstedt retningslinjer om nationale sikkerhedscertifikater i henhold til DPA 2018, som navnlig fremhæver, at enhver begrænsning af registreredes rettigheder med henblik på at beskytte statens sikkerhed skal være forholdsmæssig og nødvendig ([225]). Alle nationale sikkerhedscertifikater skal offentliggøres på ICO's websted ([226]).

(132) Certifikatet bør have en fast gyldighedsperiode på højst fem år, så det regelmæssigt tages op til revision af den udøvende magt ([227]). Det enkelte certifikat skal angive de personoplysninger eller kategorier af personoplysninger, der er omfattet af undtagelsen, og de bestemmelser i DPA 2018, som undtagelsen finder anvendelse på ([228]).

(133) Det er vigtigt at bemærke, at nationale sikkerhedscertifikater medfører en yderligere grund til at begrænse databeskyttelsesrettigheder af hensyn til den nationale sikkerhed. Med andre ord kan den dataansvarlige eller databehandleren kun basere sig på et certifikat, når de har konkluderet, at det er nødvendigt at påberåbe sig undtagelsen vedrørende statens sikkerhed, som skal anvendes fra sag til sag. Selv om et nationalt sikkerhedscertifikat finder anvendelse på den pågældende sag, kan ICO undersøge, om det i et konkret tilfælde var berettiget at påberåbe sig undtagelsen af hensyn til statens sikkerhed ([229]).

(134) Enhver person, der berøres direkte af udstedelsen af certifikatet, kan appellere udstedelsen til Upper Tribunal ([230]), ([231]) eller, hvis certifikatet identificerer data ved brug af en generel beskrivelse, anfægte certifikatets anvendelse på specifikke data ([232]).

(135) Upper Tribunal tager afgørelsen om at udstede et certifikat op til fornyet overvejelse og afgør, om der var rimelige grunde til at udstede certifikatet ([233]). 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 den fastslå, at certifikatet ikke finder anvendelse på specifikke personoplysninger, der er genstand for klagen ([234]).

([224]) DPA 2018 ophæver muligheden for at udstede certifikater i henhold til Section 28(2) i DPA 1998. Muligheden for at udstede »gamle certifikater« findes dog stadig, i det omfang der foreligger en historisk udfordring under loven fra 1998 (se DPA 2018, paragraph 17 i Part 5, Schedule 20). Denne mulighed forekommer imidlertid meget sjældent og gælder kun i begrænsede tilfælde såsom f.eks. hvor en registreret anfægter brugen af den nationale sikkerhedsundtagelse i forbindelse med en offentlig myndigheds behandling, der er sket i henhold til loven af 1998. Det skal bemærkes, at Section 28 i DPA 1998 i disse sager finder anvendelse i sin helhed og omfatter dermed den registreredes mulighed for at anfægte certifikatet. På nuværende tidspunkt findes der ikke nationale sikkerhedscertifikater, som er udstedet under DPA 1998.

([225]) United Kingdom Government Guidance on National Security Certificates under the Data Protection Act 2018 (de britiske myndigheders vejledning om nationale sikkerhedscertifikater i henhold til Data Protection Act 2018), som kan 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

([226]) Ifølge Section 130 i DPA 2018 kan ICO beslutte at undlade at offentliggøre hele eller dele af certifikatets tekst, hvis dette strider mod den nationale sikkerhed eller almenhedens interesse eller kan skade en persons sikkerhed. I disse sager offentliggør ICO dog, at certifikatet er blevet udstedt.

([227]) United Kingdom Government Guidance on National Security Certificates, paragraph 15, se fodnote 224.

([228]) United Kingdom Guidance on National Security Certificates, paragraph 5, fodnote 225.

([229]) 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 over for ICO skal dokumentere, at den, når den påberåber sig undtagelsen, har taget hensyn til sagens særlige omstændigheder. ICO offentliggør også en fortegnelse over de nationale sikkerhedscertifikater, som findes på følgende link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Upper Tribunal er den domstol, der har kompetence til at behandle appeller over afgørelser truffet af lavere forvaltningsdomstole. Den har særlig kompetence med hensyn til direkte appeller over afgørelser truffet af visse statslige myndigheder.

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

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

([233]) I sagen *Baker mod Secretary of State* (se fodnote 221) ophævede Information Tribunal et nationalt sikkerhedscertifikat, der var udstedt af Home Secretary, idet den fandt, at der ikke var nogen grund til at indføre en generel undtagelse for forpligtelsen til at besvare anmodninger om aktindsigt, og at 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.

([234]) United Kingdom Guidance on National Security Certificates, paragraph 25, fodnote 224.

(136) Der findes en anden gruppe af mulige begrænsninger, som i henhold til Schedule 11 til DPA 2018 finder anvendelse på visse bestemmelser i Part 4 i DPA 2018 ([235]) 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. Anvendelsen af disse bestemmelser er enten undtaget for visse kategorier af oplysninger (»klassebaseret«) eller undtaget i det omfang, at anvendelsen sandsynligvis vil skade beskyttede interesser (»skadebaseret«) ([236]). Skadebaserede undtagelser kan kun påberåbes, for så vidt anvendelsen af den 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. Klassebaserede undtagelser kan kun påberåbes i forbindelse med den specifikke, snævert definerede kategori af oplysninger, for hvilke 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.

(137) 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.

(138) Den behandling af personoplysninger, der foretages af efterretningstjenesterne i henhold til Part 4 i DPA 2018, overvåges af Information Commissioner ([237]).

(139) 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, navnlig 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 registrerede om udøvelsen af registreredes rettigheder og gennemførelse af undersøgelser.

(140) Information Commissioner har ligesom for Part 3 i DPA 2018 beføjelse til at underrette de dataansvarlige om en formodet overtrædelse og udstede advarsler om, at en behandling sandsynligvis vil overtræde reglerne, og udstede irettesættelser, når overtrædelsen bekræftes. Denne kan også udstede enforcement og penalty notices for overtrædelser af visse bestemmelser i loven ([238]). I modsætning til for andre dele af DPA 2018 kan Information Commissioner imidlertid ikke udstede en assessment notice til et nationalt sikkerhedsagentur ([239]).

(141) 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 statens sikkerhed. Dette omfatter Information Commissioners beføjelse til at udstede (enhver form for) notices i henhold til DPA (information, assessment,

([235]) Dette omfatter: 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.

([236]) Ifølge Explanatory Framework for Adequacy Discussions er de »klassebaserede« undtagelser: 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, 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, viii) arkivering i almenhedens interesse. UK Explanatory Framework for Adequacy Discussions, section H: National Security, side 13, se fodnote 222.

([237]) Section 116 i DPA 2018.

([238]) I henhold til Section 149(2) og Section 155 i DPA 2018 tilsammen kan der udstedes enforcement og penalty notices 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 sikrer 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 uden for konventionen og internationale organisationer som nævnt i Section 109 i DPA 2018. (Se betragtning (102) til (103)for yderligere oplysninger om enforcement og penalty notices).

([239]) 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).

enforcement og penalty notices), beføjelse til at foretage inspektioner i overensstemmelse med internationale forpligtelser, ransagnings- og inspektionsbeføjelser samt reglerne om lovovertrædelser ([240]). Som forklaret i betragtning (136) finder disse undtagelser kun anvendelse, hvis det er nødvendigt og forholdsmæssigt, og vurderes fra sag til sag. Anvendelsen af disse undtagelser kan underlægges domstolskontrol ([241]).

(142) ICO og Det Forenede Kongeriges efterretningstjenester har undertegnet et aftalememorandum ([242]), der fastlægger en ramme for samarbejde om en række spørgsmål, herunder anmeldelser af brud på datasikkerheden og behandling af klager fra registrerede. Deri fastsættes navnlig, at ICO, når denne modtager en klage, vurderer, om en eventuel undtagelse som følge af statens sikkerhed er blevet anvendt korrekt. Svar på forespørgsler fra ICO i forbindelse med behandlingen af individuelle klager skal gives inden for 20 hverdage af den pågældende United Kingdom Government Guidance on National Security Certificates i henhold til Data Protection Act ved hjælp af passende sikre kanaler, hvis der er tale om klassificerede oplysninger. ICO har fra april 2018 til dato modtaget 21 klager over efterretningstjenesterne fra enkeltpersoner. Hver klage blev vurderet, og resultatet er meddelt den registrerede ([243]).

(143) Desuden fører Intelligence and Security Committee (efterretnings- og sikkerhedsudvalget, ISC) parlamentarisk tilsyn med efterretningstjenesternes databehandling. Udvalget har sit retsgrundlag i Justice and Security Act 2013 (lov om retlige anliggender og sikkerhed, JSA 2013) ([244]). Ved loven oprettes ISC som et udvalg under Det Forenede Kongeriges parlament. ISC består af medlemmer, der tilhører parlamentets to kamre og udnævnes af premierministeren efter høring af oppositionslederen ([245]). ISC skal hvert år aflægge beretning til Parlamentet om udøvelsen af sine funktioner og andre rapporter, som det finder hensigtsmæssige ([246]).

(144) 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,

([240]) 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 Commissioners notices og beføjelser vedrørende adgang og inspektion) og Section 170-173 (lovovertrædelser vedrørende personoplysninger). Desuden for så vidt angår behandling foretaget af efterretningstjenesterne i Schedule 13 (Information Commissioners øvrige generelle opgaver), paragraph 1(a) og (g) og paragraph 2.

([241]) Se f.eks. *Baker v Secretary of State for the Home Department* (se fodnote 221).

([242]) Memorandum of Understanding between ICO og United Kingdom Intelligence Community, se fodnote 231.

([243]) 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).

([244]) Som forklaret af de britiske myndigheder udvidede JSA 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.

([245]) 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, som har udnævnt dem, eller hvis de ophører med at være parlamentsmedlem eller udnævnes til minister. Et medlem kan også træde tilbage.

([246]) Udvalgets rapporter og udtalelser er tilgængelige online via følgende link: http://isc.independent.gov.uk/committee-reports. I 2015 udsendte ISC rapporten »Privacy and Security: A modern and transparent legal framework« (se: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.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.

når de ikke vedrører igangværende operationer ([247]). I det Memorandum of Understanding, der er indgået mellem premierministeren og ISC ([248]), 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 ([249]). Premierministeren kan også anmode ISC om at undersøge igangværende operationer og gennemgå oplysninger, som agenturerne frivilligt fremlægger.

(145) I henhold til Schedule 1 til JSA 2013 kan ISC anmode lederne af hver af de tre efterretningstjenester om at videregive alle oplysninger. Agenturet skal stille disse oplysninger til rådighed, medmindre Secretary of State nedlægger veto mod dette ([250]). De britiske myndigheder forklarede, at der i praksis kun tilbageholdes meget få oplysninger fra ISC ([251]).

(146) Hvad angår klageadgang, kan en registreret i henhold til Section 165(2) i DPA 2018 indbringe en klage for ICO, hvis vedkommende mener, at der i forbindelse med personoplysninger om vedkommende er tale om en overtrædelse af Part 4 i DPA 2018, herunder misbrug af undtagelserne og begrænsningerne vedrørende statens sikkerhed.

(147) 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 ([252]), at gøre indsigelse mod behandling ([253]) samt til berigtigelse eller sletning.

(148) 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 ([254]). Skader omfatter både økonomiske tab og skader, der ikke indebærer økonomiske tab, såsom overlast ([255]).

(149) Endelig kan en person indgive en klage til Investigatory Powers Tribunal for enhver handling, der udføres af eller på vegne af Det Forenede Kongeriges efterretningstjenester ([256]). Investigatory Powers Tribunal (IPT) er oprettet ved Regulation of Investigatory Powers Act 2000 for England, Wales og Nordirland og Regulation of Investigatory Powers (Scotland) Act 2000 for Skotland (RIPA 2000) og er uafhængigt af den udøvende magt ([257]). I overensstemmelse med Section 65 i RIPA 2000 udnævnes medlemmerne af IPT af Kronen for en periode på fem år.

(150) Et medlem af domstolen kan afskediges af Kronen efter et forslag (»Address«) ([258]) fra begge parlamentets kamre ([259]).

(151) For at anlægge sag ved IPT (»standing requirement«, stående krav) skal en person i henhold til Section 65 i RIPA 2000 have en formodning om, i) at en efterretningstjeneste har udført aktiviteter vedrørende vedkommende, et hvilket som helst af dennes formuegoder, enhver kommunikation, der sendes af eller er bestemt for vedkommende, eller vedkommendes brug af en hvilken som helst posttjeneste, telekommunikationstjeneste eller telekommunikationssystem ([260]), og ii) at

([247]) Section 2 i JSA 2013.
([248]) Memorandum of Understanding mellem premierministeren og ISC kan findes på følgende link: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Memorandum of Understanding mellem premierministeren og ISC, paragraph 14, se fodnote247.
([250]) 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, stk. 2, i JSA 2013). Schedule 1, paragraph 4(2) i RIPA 2013.
([251]) UK Explanatory Framework — section H: National Security, s. 43.
([252]) Section 94(11) i DPA 2018.
([253]) Section 99(4) i DPA 2018.
([254]) Section 169 i DPA 2018, som tillader krav fra »en person, der lider skade som følge af overtrædelse af et krav i databeskyttelseslovgivningen«.
([255]) Section 169(5) i DPA 2018.
([256]) Jf. Section 65(2)(b) i RIPA.
([257]) I henhold til Schedule 3 til RIPA 2000 skal medlemmerne have nærmere angivet juridisk erfaring og kan genudnævnes.
([258]) Med hensyn til begrebet »Address« henvises til fodnote 183.
([259]) Schedule 3, paragraph 1(5) i RIPA 2000.
([260]) Section 65(4) i RIPA 2000.

aktiviteten har fundet sted under »anfægtelige omstændigheder« ([261]) eller »er udført af eller på vegne af efterretningstjenesterne« ([262]). Da navnlig denne »formodnings«-standard er blevet fortolket ret bredt ([263]), er indbringelse af en sag for retten underlagt relativt lave krav til søgsmålskompetence.

(152) 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 ([264]). 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 ([265]).

(153) Investigatory Powers Tribunal skal underrette klageren om, hvorvidt vedkommende har fået medhold eller ikke ([266]). 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 ([267]). I henhold til Section 67A i RIPA 2000 kan Investigatory Powers Tribunals afgørelse appelleres med forbehold af dens egen eller den relevante appeldomstols tilladelse.

(154) Enkeltpersoner kan navnlig indbringe et krav — og opnå erstatning — for IPT, hvis de mener, at en offentlig myndighed har handlet (eller agter at handle) på en måde, der er uforenelig med rettighederne i EMRK, herunder retten til privatlivets fred og databeskyttelse, og som derfor er ulovlig i henhold til Section 6(1) i Human Rights Act 1998. IPT har fået enekompetence i forbindelse med alle krav i henhold til Human Rights Act i forbindelse med efterretningstjenesterne. 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 appel til en passende appelret (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) v Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219« ([268]). Hvis IPT fastslår, at en handling fra en offentlig myndighed 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 ([269]).

([261]) 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, som varetager en retslig funktion, ikke anses for at have fundet sted under omstændigheder, der kan påklages (Section 65(7) og (8) i RIPA 2000).

([262]) 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 IPT, 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.

([263]) Se *Human Rights Watch mod Secretary of State* [2016] UKIPTrib15_165-CH. I denne sag fastslog IPT 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 på grund af sin personlige situation er udsat for sådanne foranstaltninger (se *Human Rights Watch mod Secretary of State*, præmis 41).

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

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

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

([267]) Dette kan omfatte et påbud om tilintetgørelse af ethvert register over oplysninger, som en offentlig myndighed er i besiddelse af i forbindelse med en hvilken som helst person.

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

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

(155) Når de nationale retsmidler er udtømt, kan en person indbringe sagen for Den Europæiske Menneskerettighedsdomstol med påstand om krænkelse af de rettigheder, der er garanteret i henhold til EMRK, herunder retten til privatlivets fred og databeskyttelse.

(156) Det følger af ovenstående, at Det Forenede Kongeriges strafferetlige myndigheders deling af oplysninger, der overføres i henhold til denne afgørelse til andre offentlige myndigheder, herunder efterretningstjenester, er underlagt begrænsninger og betingelser, der sikrer, at en sådan videredeling skal være nødvendig og forholdsmæssig og underlagt specifikke databeskyttelsesgarantier i henhold til DPA 2018. Desuden overvåges de berørte offentlige myndigheders behandling af oplysninger af uafhængige organer, og berørte personer har adgang til effektive retsmidler.

3. KONKLUSION

(157) Kommissionen mener, at Part 3 i DPA 2018 sikrer et beskyttelsesniveau for personoplysninger, der overføres med henblik på retshåndhævelse på det strafferetlige område fra kompetente myndigheder i Unionen til Det Forenede Kongeriges kompetente myndigheder, som i det væsentlige svarer til det, der er garanteret ved direktiv (EU) 2016/680.

(158) 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.

(159) 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 i almenhedens interesse, herunder i forbindelse med udveksling af personoplysninger mellem retshåndhævende myndigheder og andre offentlige myndigheder såsom nationale sikkerhedsorganer, vil være begrænset til, hvad der er strengt nødvendigt for at nå det pågældende legitime mål, og at der findes en effektiv retlig beskyttelse mod et sådant indgreb.

(160) Det bør derfor besluttes, at Det Forenede Kongerige sikrer et tilstrækkeligt beskyttelsesniveau som omhandlet i artikel 36, stk. 2, i direktiv (EU) 2016/680, fortolket i lyset af chartret om grundlæggende rettigheder.

(161) 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.

4. VIRKNINGERNE AF DENNE AFGØRELSE OG DATABESKYTTELSESMYNDIGHEDERNES HANDLINGER

(162) 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 under et annullationssøgsmål eller erklæres ugyldige som følge af en præjudiciel forelæggelse eller en ulovlighedsindsigelse.

(163) En afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet i medfør af artikel 36, stk. 3, i direktiv (EU) 2016/680 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.

(164) Det skal samtidig bemærkes, at i henhold til artikel 47, stk. 5, i direktiv (EU) 2016/680, og som Domstolen forklarede i Schrems-dommen, 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 ([270]).

([270]) *Schrems*, præmis 65.

5. **OVERVÅGNING, SUSPENSION, OPHÆVELSE ELLER ÆNDRING AF DENNE AFGØRELSE**

(165) I henhold til artikel 36, stk. 4, i direktiv (EU) 2016/680 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, der ikke længere er underlagt EU-retten, og som muligvis kan udvikle sig. I den henseende vil der blive lagt særlig vægt på anvendelsen i praksis af Det Forenede Kongeriges regler for overførsel af personoplysninger til tredjelande, herunder gennem indgåelse af internationale aftaler, og den indvirkning det kan få for beskyttelsesniveauet for de oplysninger, der overføres under denne afgørelse samt hvor effektivt individuelle rettigheder udøves på de områder, der er omfattet af afgørelsen. Blandt andre elementer vil Kommissionen kunne basere sin overvågning på oplysninger om udviklingen af sædvaneret samt ICO's og andre uafhængige organers tilsyn.

(166) For at lette denne overvågning bør Det Forenede Kongeriges myndigheder øjeblikkeligt og regelmæssigt underrette Kommissionen om enhver væsentlig ændring af Det Forenede Kongeriges retsorden, der 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, navnlig med hensyn til de elementer, der er anført i betragtning (165).

(167) 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 kompetente myndigheder Det Forenede Kongerige. Kommissionen bør også underrettes om eventuelle tegn på, at de foranstaltninger, der træffes af Det Forenede Kongeriges offentlige myndigheder med ansvar for forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger, herunder eventuelle tilsynsorganer, ikke sikrer det krævede beskyttelsesniveau.

(168) 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 øjeblikkeligt underrette de kompetente britiske myndigheder herom og anmode om, at der træffes passende foranstaltninger inden for en nærmere fastsat tidsramme, der ikke må overstige tre måneder. Hvor det er nødvendigt, kan denne tidsramme forlænges med en nærmere fastsat periode, idet der tages hensyn til de pågældende forholds karakter og/eller de foranstaltninger, der skal træffes.

(169) 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 58, stk. 2, i direktiv (EU) 2016/680 med henblik på helt eller delvis at suspendere eller ophæve denne afgørelse.

(170) 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.

(171) I behørigt begrundede særligt hastende tilfælde vil Kommissionen gøre brug af muligheden for efter proceduren i artikel 58, stk. 3, i direktiv (EU) 2016/680 at vedtage gennemførelsesretsakter, der finder anvendelse straks, og som suspenderer, ophæver eller ændrer afgørelsen.

6. **VARIGHED OG FORLÆNGELSE AF DENNE AFGØRELSE**

(172) Det bør tages 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 af den databeskyttelsesramme, der vurderes i denne afgørelse, samt andre relevante udviklinger.

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

(174) Hvis navnlig oplysninger som følge af overvågningen i henhold til 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 anvendelsesperiode med yderligere fire år. En sådan gennemførelsesretsakt om ændring af denne afgørelse skal vedtages efter proceduren i artikel 58, stk. 2, i direktiv (EU) 2016/680.

7. **AFSLUTTENDE BETRAGTNINGER**

(175) Det Europæiske Databeskyttelsesråd har offentliggjort sin udtalelse ([271]), som er blevet taget i betragtning ved udarbejdelsen af denne afgørelse.

(176) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 58 i direktiv (EU) 2016/680.

(177) I medfør af artikel 6a i protokol nr. 21 om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til TEU og til TEUF, er Irland ikke bundet af reglerne i direktiv (EU) 2016/680 og dermed denne gennemførelsesafgørelse, der vedrører medlemsstaternes behandling af personoplysninger, når de udfører aktiviteter, som henhører under tredje del, afsnit V, kapitel 4 eller 5, i TEUF, hvor Irland ikke er bundet af de regler om formerne for retligt samarbejde, der er fastsat i artikel 16 i TEUF. I henhold til Rådets gennemførelsesafgørelse (EU) 2020/1745 ([272]) skal direktiv (EU) 2016/680 desuden iværksættes og anvendes midlertidigt i Irland fra den 1. januar 2021. Irland er derfor bundet af denne gennemførelsesafgørelse på de betingelser, der gælder for anvendelsen af direktiv (EU) 2016/680 i Irland, jf. gennemførelsesafgørelse (EU) 2020/1745, for så vidt angår de Schengenregler, som Irland deltager i.

(178) I medfør af artikel 2 og 2a i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, er Danmark ikke bundet af reglerne i direktiv (EU) 2016/680 og dermed denne gennemførelsesafgørelse og er heller ikke omfattet af deres anvendelse i forbindelse med medlemsstaternes behandling af personoplysninger i forbindelse med aktiviteter, der henhører under tredje del, afsnit V, kapitel 4 eller kapitel 5 i TEUF. Da direktiv (EU) 2016/680 imidlertid er baseret på Schengenreglerne, meddelte Danmark i overensstemmelse med artikel 4 i nævnte protokol den 26. oktober 2016 sin beslutning om at gennemføre direktiv (EU) 2016/680. Danmark er derfor i henhold til folkeretten forpligtet til at gennemføre denne gennemførelsesafgørelse.

(179) For så vidt angår Island og Norge udgør denne gennemførelsesafgørelse en udvikling af bestemmelser i Schengenreglerne, jf. aftalen indgået mellem Rådet for Den Europæiske Union og Republikken Island og Kongeriget Norge om disse to staters associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne ([273]).

(180) For så vidt angår Schweiz udgør denne gennemførelsesafgørelse en udvikling af bestemmelser i Schengenreglerne, jf. aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne ([274]).

(181) For så vidt angår Liechtenstein udgør denne gennemførelsesafgørelse en udvikling af bestemmelser i Schengenreglerne, jf. protokollen mellem Den Europæiske Union, Det Europæiske Fællesskab, Det Schweiziske Forbund og Fyrstendømmet Liechtenstein om Fyrstendømmet Liechtensteins tiltrædelse af aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om dette lands associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne ([275]) —

([271]) Opinion 15/2021 regarding the European Commission draft implementing decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom, kan findes på følgende link https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Rådets gennemførelsesafgørelse (EU) 2020/1745 af 18. november 2020 om iværksættelse af bestemmelserne i Schengenreglerne vedrørende databeskyttelse og om midlertidig iværksættelse af visse bestemmelser i Schengenreglerne for Irland (EUT L 393 af 23.11.2020, s. 3).

([273]) EFT L 176 af 10.7.1999, s. 36.

([274]) EFT L 53 af 27.2.2008, s. 52.

([275]) EUT L 160 af 18.6.2011, s. 21.

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Med henblik på artikel 36 i direktiv (EU) 2016/680 sikrer Det Forenede Kongerige et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra Den Europæiske Union til Det Forenede Kongeriges offentlige myndigheder med ansvar for forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner.

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 47 i direktiv (EU) 2016/680 med hensyn til videregivelse af oplysninger til offentlige myndigheder i Det Forenede Kongerige inden for det anvendelsesområde, der er fastsat 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 og udøvelse af individuelle rettigheder, 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.

5. Kommissionen kan suspendere, ophæve eller ændre denne afgørelse, hvis det manglende samarbejde fra Det Forenede Kongeriges regerings side forhindrer Kommissionen i at afgøre, om konstateringen i artikel 1 er berørt.

Artikel 4

Denne afgørelse udløber den 27. juni 2025, medmindre den forlænges efter proceduren i artikel 58, stk. 2, i direktiv 2016/680/EU.

Artikel 5

Denne afgørelse er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 28. juni 2021.

På Kommissionens vegne
Didier REYNDERS
Medlem af Kommissionen