Udtalelse nr. 26/2025 vedrørende Europa-Kommissionens udkast til gennemførelsesafgørelse i henhold til forordning (EU) 2016/679 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Det Forenede Kongerige

Vedtaget den 16. oktober 2025

Resumé

Den 22. juli 2025 indledte Europa-Kommissionen vedtagelsesprocessen for sit udkast til gennemførelsesafgørelse om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Det Forenede Kongerige i henhold til artikel 45, stk. 2, i GDPR. Dette udkast til afgørelse forlænger gyldigheden af visse dele af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet af 28. juni 2021 indtil december 2031.

Samme dag anmodede Europa-Kommissionen Det Europæiske Databeskyttelsesråd om en udtalelse. Databeskyttelsesrådets vurdering af, om beskyttelsesniveauet i Det Forenede Kongerige er tilstrækkeligt, er foretaget på grundlag af gennemgangen af selve udkastet til afgørelse samt på grundlag af en analyse af den dokumentation, som Europa-Kommissionen har fremlagt.

Databeskyttelsesrådet fokuserede på vurderingen af både de generelle databeskyttelsesaspekter ved udkastet til afgørelse og offentlige myndigheders indsigt i personoplysninger, der overføres fra EØS til Det Forenede Kongerige med henblik på retshåndhævelse og national sikkerhed, herunder hvilke retsmidler der er til rådighed for borgere i EØS.

Databeskyttelsesrådet vurderede også, om garantierne i Det Forenede Kongeriges retlige ramme er på plads og er effektive.

Databeskyttelsesrådet har som hovedreference for dette arbejde anvendt sin GDPR Adequacy Referential (herefter "reference vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR"), der blev vedtaget den 28. november 2017 og senest revideret og vedtaget den 6. februar 2018, og Databeskyttelsesrådets henstillinger 2/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger.

Databeskyttelsesrådet glæder sig over den fortsatte tilpasning mellem Det Forenede Kongeriges og EU's databeskyttelsesramme, uanset den seneste udvikling i den relevante retlige ramme i Det Forenede Kongerige. På denne baggrund fremhæves i denne udtalelse en række punkter, der kræver yderligere analyse, samt nogle spørgsmål, som Kommissionen bør overvåge nøje i de kommende år som led i sin overvågningsforpligtelse i henhold til artikel 45, stk. 4, i GDPR.

Databeskyttelsesrådet bemærker, at Det Forenede Kongerige har indført ændringer vedrørende den "nedarvede" generelle EU-lovramme i kraft af Retained EU Law (Revocation and Reform) Act 2023 (herefter "REUL Act"), som bl.a. ophæver princippet om EU-rettens forrang (med garantier for visse bestemmelser i GDPR) og ophæver den direkte anvendelse af EU-rettens principper, herunder retten til privatlivets fred og databeskyttelse som afledt af chartret om grundlæggende rettigheder. Databeskyttelsesrådet opfordrer Kommissionen til at forklare og foretage en mere detaljeret vurdering af de ændringer, der er indført ved REUL Act, og vurdere deres indvirkning på den britiske retlige ramme generelt – og mere specifikt dens databeskyttelsesramme. Databeskyttelsesrådet anser også dette for at være et område, som Kommissionen bør overvåge nøje i fremtiden.

Databeskyttelsesrådet bemærker, at Secretary of State har fået nye beføjelser til at indføre ændringer af den nye databeskyttelsesramme via afledt lovgivning, som kræver mindre parlamentarisk kontrol i visse tilfælde, f.eks. internationale overførsler, automatiske afgørelser og forvaltningen af tilsynsmyndigheden Information Commission (herefter "IC"). Databeskyttelsesrådet opfordrer Kommissionen til i den endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet at fremhæve de områder, som den agter at overvåge nøje, fordi der er risiko for yderligere afvigelser fra EU's databeskyttelseslovgivning via den britiske afledte lovgivning.

Databeskyttelsesrådet bemærker ændringer i reglerne for overførsel af personoplysninger, navnlig den nye vejledende liste over elementer, der skal tages i betragtning ved tilstrækkelighedstesten. Denne indeholder ikke længere vigtige elementer, der indgik i den tidligere tilstrækkelighedstest for Det Forenede Kongerige[1]. Dette gælder både for tredjelandsoverførsler, der foretages i henhold til UK GDPR, og for overførsler af oplysninger, der behandles med henblik på retshåndhævelse. Databeskyttelsesrådet opfordrer Kommissionen til specifikt at uddybe sin vurdering af disse aspekter yderligere og overvåge udviklingen og den praktiske gennemførelse af denne nye tilstrækkelighedstest.

Databeskyttelsesrådet opfordrer Kommissionen til at foretage en mere detaljeret vurdering af omstruktureringen af Information Commissioner's Office (den uafhængige databeskyttelsesmyndighed, herefter "ICO"), som er blevet til en bestyrelse, samt reglerne for udnævnelse og afskedigelse af udøvende og ikke-udøvende bestyrelsesmedlemmer. Databeskyttelsesrådet opfordrer også Kommissionen til at fremlægge mere detaljerede oplysninger om ICO's nylige høring, der blev foretaget efter dette udkast til afgørelse, med henblik på at indføre et nyt triagesystem til behandling af klager. Databeskyttelsesrådet opfordrer Kommissionen til at overvåge alle disse ændringer, når de træder i kraft. Databeskyttelsesrådet noterer sig med tilfredshed ICO's gennemsigtighedspolitik og tilgængeligheden af statistiske og analytiske data om sine håndhævelsesaktiviteter, men opfordrer også Kommissionen til at foretage en mere detaljeret vurdering og overvåge anvendelsen af korrigerende beføjelser, effektiviteten af sanktioner og retsmidler for berørte parter i den britiske databeskyttelsesramme.

Databeskyttelsesrådet finder det afgørende at vurdere de udvidede undtagelser fra den nationale sikkerhed i henhold til retshåndhævelsesrammen og er fortsat særlig opmærksom på eventuelle undtagelser fra proportionalitetsprincippet og fra kravet om at behandle personoplysninger til et legitimt formål. På samme måde bør undtagelser fra tilsynsmyndighedens beføjelser gribes an med forsigtighed. Enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes ved chartret, skal respektere deres væsentligste indhold og må, under iagttagelse af proportionalitetsprincippet, kun indføres, hvis det er nødvendigt og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder. Databeskyttelsesrådet opfordrer Kommissionen til at supplere sin vurdering i den endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet og specifikt overvåge anvendelsen i praksis af undtagelserne med hensyn til national sikkerhed for de retshåndhævende myndigheder.

Databeskyttelsesrådet bemærker, at behandlingsaktiviteter, der udføres af kompetente retshåndhævelsesmyndigheder, under særlige omstændigheder kan være omfattet af de regler, der normalt gælder for nationale sikkerhedsmyndigheders behandling af personoplysninger. Her bør der lægges særlig vægt på at sikre, at databeskyttelsesrammen for behandling, der har relation til national sikkerhed, ikke udvides til at omfatte sammenhænge, der ikke har relation til national sikkerhed. Databeskyttelsesrådet opfordrer Kommissionen til at overvåge, om de kvalificerede kompetente myndigheder er i stand til at opretholde en klar sondring mellem forskellige behandlingsformål for at overholde de tilsvarende retlige rammer i overensstemmelse hermed.

Databeskyttelsesrådet glæder sig over de præciseringer, der er opnået mellem Det Forenede Kongerige og USA i forbindelse med Cloud Act-aftalen mellem Det Forenede Kongerige og USA, som

[1] i) tredjelandets regler vedrørende "offentlig sikkerhed, forsvar, national sikkerhed og strafferet samt offentlige myndigheders adgang til personoplysninger", ii) retspraksis, iii) eksistensen af effektive og håndhævelige rettigheder for de registrerede samt de administrative og retslige retsmidler, som de registrerede, hvis personoplysninger overføres, kan gøre brug af, og iv) en eller flere uafhængige tilsynsmyndigheder.

skaber yderligere juridisk klarhed. Samtidig vil Databeskyttelsesrådet gerne minde om behovet for at forbedre niveauet af garantier i paraplyaftalen mellem EU og USA, hvis garantier for privatlivets fred og databeskyttelse er indarbejdet i Cloud Act-aftalen mellem Det Forenede Kongerige og USA. Samlet set finder Databeskyttelsesrådet, at der er behov for en præcisering af Kommissionens vurdering af Cloud Act-aftalen mellem Det Forenede Kongerige og USA og en eventuel indvirkning på beskyttelsesniveauet. Databeskyttelsesrådet opfordrer Kommissionen til fortsat at inkludere Cloud Act-aftalen mellem Det Forenede Kongerige og USA i sine fremtidige vurderinger og revisioner.

Som det for nylig blev påpeget i erklæring 5/2024, mener Databeskyttelsesrådet, at kryptering er af afgørende betydning for at garantere sikkerheden og fortroligheden af personoplysninger og elektronisk kommunikation. Technical Capability Notices (herefter "pålæg om teknisk kapacitet") i henhold til IPA 2016, der pålægger virksomheder at kunne fjerne kryptering på regeringens anmodning, skaber systemiske sårbarheder og udgør en direkte trussel mod integriteten og fortroligheden af elektronisk kommunikation. En sådan udvikling fortjener opmærksomhed i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, navnlig i lyset af artikel 45, stk. 2, litra a), i GDPR, som kræver en vurdering ikke kun af den retlige ramme på papir, men også af dens gennemførelse, og bør overvåges.

Databeskyttelsesrådet bemærker, at Investigatory Powers Amendment Act 2024 (lov om ændring af efterforskningsbeføjelser fra 2024) indførte en særlig ordning for opbevaring og undersøgelse af store persondatasæt, for hvilke de personer, som personoplysningerne vedrører, "ikke kunne have nogen eller kun en lav, rimelig forventning om privatlivets fred". Databeskyttelsesrådet mener, at der er behov for yderligere præciseringer med hensyn til de relevante ændringer, navnlig med hensyn til begreberne "individuelle tilladelser" og "kategoritilladelser". Databeskyttelsesrådet opfordrer desuden Kommissionen til nøje at overvåge indførelsen af udtrykket "lav eller ingen rimelig forventning om privatlivets fred" i praksis.

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har –

under henvisning til artikel 70, stk. 1, litra s), i Europa-Parlamentets og Rådets forordning 2016/679/EU 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 (herefter "GDPR"),

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS), særlig bilag XI og protokol 37 til EØS-aftalen, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018[2], og

under henvisning til artikel 12 og artikel 22 i dets forretningsorden –

VEDTAGET FØLGENDE UDTALELSE:

1. INDLEDNING

1.1. ANVENDELSESOMRÅDET FOR KOMMISSIONENS UDKAST TIL AFGØRELSE

1. Den 22. juli 2025 anmodede Europa-Kommissionen ("Kommissionen") Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") om en udtalelse om udkastet til gennemførelsesafgørelse om ændring af Kommissionens gennemførelsesafgørelse (EU) 2021/1772 af 28. juni 2021 i henhold til GDPR om beskyttelse af personoplysninger i Det Forenede Kongerige ("udkastet til afgørelse"). I sit udkast til afgørelse konkluderede Kommissionen, at Det Forenede Kongerige fortsat sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra Den Europæiske Union til Det Forenede Kongerige inden for GDPR's anvendelsesområde.

2. Databeskyttelsesrådet bemærker, at dette udkast til afgørelse forlænger gyldigheden af Kommissionens gennemførelsesafgørelse (EU) 2021/1772 af 28. juni 2021 i henhold til GDPR om beskyttelse af personoplysninger i Det Forenede Kongerige ("den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige") med 6 år, som ellers ville udløbe den 27. juni 2025 (udløbsklausul). Den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige blev forlænget med seks måneder indtil den 27. december 2025 i medfør af afgørelse (EU) 2025/1225 den 24. juni 2025, for at gøre det muligt for Det Forenede Kongerige at afslutte sine databeskyttelsesreformer[3].

3. I sit udkast til afgørelse vurderede Kommissionen, "hvorvidt konklusionen om, at Det Forenede Kongerige sikrer et tilstrækkeligt beskyttelsesniveau, fortsat er faktuelt og retligt begrundet i lyset af den udvikling, der har fundet sted siden vedtagelsen af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige".

4. Kommissionen fokuserede sin vurdering på nye udviklinger i den britiske lovgivning om databeskyttelse, navnlig dem, der blev indført ved Data (Use and Access) Act 2025 (herefter "DUAA"). Kommissionen tog specifikt hensyn til elementerne i betragtning 281 i den tidligere afgørelse om

[2] Ved "medlemsstater" i denne udtalelse forstås "EØS-medlemsstater".

[3] Databeskyttelsesrådet afgav efter anmodning udtalelse nr. 6/2025 om forlængelse af Europa-Kommissionens gennemførelsesafgørelser i henhold til GDPR og retshåndhævelsesdirektivet om tilstrækkelig beskyttelse af personoplysninger i Det Forenede Kongerige.

tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige, som alle er indeholdt i udkastet til afgørelse.

5. Databeskyttelsesrådet er enigt i, at vurderingen primært bør fokusere på alle nye relevante udviklinger i den britiske lovgivning og de elementer, der er fremhævet i den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige for så vidt som alle de elementer, der er fastsat i artikel 45, stk. 2, i GDPR, vurderes. Databeskyttelsesrådet ser derfor gerne, at Kommissionen i sin endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet udtrykkeligt præciserer, at alle de elementer, der er anført i artikel 45, stk. 2, i GDPR, blev vurderet med henblik på at konkludere, at den britiske overordnede retlige ramme fortsat sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra Den Europæiske Union til Det Forenede Kongerige. Databeskyttelsesrådet vil også gerne have en præcisering fra Kommissionens side om, at den løbende vil vurdere disse elementer som led i sin overvågningsrolle.

1.2. ANVENDELSESOMRÅDET FOR DENNE UDTALELSE FRA DATABESKYTTELSESRÅDET

6. Databeskyttelsesrådet forventes at afgive en uafhængig udtalelse til Kommissionen med henblik på vurderingen af tilstrækkeligheden af beskyttelsesniveauet i et tredjeland[4] samt identificere eventuelle mangler i rammen for et tilstrækkeligt beskyttelsesniveau og fremsætte forslag til at afhjælpe disse[5]. På grund af den særlige situation i Det Forenede Kongerige supplerer den nye afgørelse om tilstrækkeligheden af beskyttelsesniveauet afgørelsen fra 2021, som fortsat er gyldig for de dele, der ikke specifikt er behandlet i dette udkast til afgørelse. Med denne udtalelse bygger Databeskyttelsesrådet på og videreudvikler ligeledes sin udtalelse nr. 14/2021[6]. Som følge heraf er Databeskyttelsesrådets analyse og bemærkninger i dets tidligere udtalelse vedrørende den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige generelt fortsat relevante.

7. Under hensyntagen til ovenstående har Databeskyttelsesrådet centreret sine bemærkninger omkring udvalgte punkter i udkastet til afgørelse, navnlig hvor der er behov for yderligere præcisering, yderligere oplysninger eller fremtidig overvågning fra Europa-Kommissionens side.

8. Databeskyttelsesrådet bemærker også, at i henhold til artikel 47 og 94 i forordning (EU) 2018/1725[7] kan Den Europæiske Unions institutioner, organer, kontorer og agenturer overføre personoplysninger til et tredjeland, et område, en sektor eller en international organisation, der er anerkendt af Europa-Kommissionen i henhold til artikel 45, stk. 3, i GDPR som havende et tilstrækkeligt beskyttelsesniveau, forudsat at overførslen udelukkende sker i forbindelse med opgaver inden for den dataansvarliges kompetence, uden at der kræves yderligere godkendelse. Databeskyttelsesrådet opfordrer

[4] Jf. artikel 70, stk. 1, litra s), i GDPR.

[5] Jf. Artikel 29-Gruppens Reference vedrørende et tilstrækkeligt beskyttelsesniveau, Kapitel 2: Proceduremæssige aspekter i forbindelse med vurdering af et tilstrækkeligt beskyttelsesniveau i henhold til GDPR, vedtaget den 28. november 2017, senest revideret og vedtaget den 6. februar 2018, WP254 rev. 01 (godkendt af Databeskyttelsesrådet, jf. https://edpb.europa.eu/our-worktools/general-guidance/endorsed-wp29-guidelines) (herefter "reference vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR").

[6] Udtalelse nr. 14/2021 om Europa-Kommissionens udkast til gennemførelsesafgørelse i henhold til forordning (EU) 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Det Forenede Kongerige, vedtaget den 13. april 2021, https://www.edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf.

[7] Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF ("EUDPR"), EUT L 295 af 21.11.2018, s. 39.

Kommissionen til at minde om denne retlige mulighed i betragtningerne til den endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

1.3. UDVIKLINGEN I DEN BRITISKE LOVGIVNING

9. Som forklaret i udkastet til afgørelse[8] agtede Det Forenede Kongerige efter udløbet af den fastlagte gennemførelsesperiode i udtrædelsesaftalen mellem Det Forenede Kongerige og EU[9] den 31. december 2020 at vedtage en ny databeskyttelsesramme, der ville afvige fra de EU-retlige rammer. I sidste ende foretog Det Forenede Kongerige dog kun begrænsede ændringer i sin eksisterende databeskyttelsesramme, navnlig i kraft af DUAA.

10. Ud over databeskyttelse er en af de vigtigste ændringer af den britiske retlige rammer, siden den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige blevet vedtaget, de "nedarvede" generelle EU-retlige rammer (såkaldt "bibeholdt EU-ret"), dvs. lovbestemmelser, der indgår i den britiske lovgivning via European Union (Withdrawal) Act 2018. Den bibeholdte EU-ret omfattede de generelle principper i EU-retten, herunder de grundlæggende rettigheder, der følger af EU's charter om grundlæggende rettigheder ("chartret[10]"), og proportionalitets- og nødvendighedsprincipperne, som har haft indflydelse på udviklingen og fortolkningen af databeskyttelseslovgivningen i Det Forenede Kongerige. I henhold til European Union (Withdrawal) Act 2018 bevarede den bibeholdte EU-ret sin forrang i forhold til den britiske afledte lovgivning, og den bibeholdte EU-ret skulle fortolkes i overensstemmelse med de generelle principper i EU-retten. Siden indførelsen af Retained EU Law (Revocation and Reform) Act 2023 ("REUL Act")[11], har Det Forenede Kongerige imidlertid fjernet den direkte anvendelse af EU-rettens principper fra sin nationale lovgivning, herunder de grundlæggende rettigheder, der følger af chartret. REUL Act fjernede også princippet om EU-rettens forrang, da bibeholdt EU-ret (nu kaldet "assimileret ret") nu skal læses i overensstemmelse med national ret i Det Forenede Kongerige og ikke i overensstemmelse med EU-rettens principper. Dette udgør en væsentlig ændring i den britiske retsorden.

11. Derudover kunne der, selv om det i øjeblikket er sat i bero, indføres en ny, mere lempelig juridisk test for dommere ved appelretten og højesteretten til at afvige fra gældende EU-retspraksis i henhold til REUL Act[12]. Denne ændring kan, hvis den gennemføres, være en væsentlig ændring i Det Forenede Kongerige.

12. På trods af disse ændringer glæder Databeskyttelsesrådet sig over, at der i REUL Act er indføjet garantier, der sikrer, at databeskyttelseslovgivningen ikke tilsidesættes under visse omstændigheder. Disse garantier omfatter kravet om, at enhver lovgivning, "der pålægger en forpligtelse eller tillægger en beføjelse til at behandle personoplysninger, ikke tilsidesætter et krav i den primære databeskyttelseslovgivning vedrørende behandling af personoplysninger", og at databeskyttelsesrammen fortsat tilsidesætter anden lovgivning i Det Forenede Kongerige[13]. Databeskyttelsesrådet bemærker dog, at disse garantier også omfatter to undtagelser, i) hvor det

[8] Jf. betragtning 2 i udkastet til afgørelse.
[9] Gennemførelsesperioden er en periode, der er aftalt i udtrædelsesaftalen mellem Det Forenede Kongerige og EU, hvor Det Forenede Kongerige ikke længere er medlem af EU, men fortsat er underlagt EU-reglerne og forbliver medlem af det indre marked og toldunionen. Jf. European Union (Withdrawal Agreement) Act 2020.
[10] Den Europæiske Unions charter om grundlæggende rettigheder (EUT C 326 af 26.10.2012, s. 391-407).
[11] Jf. betragtning 11 i udkastet til afgørelse.
[12] Jf. Section 6, Retained EU Law (Revocation and Reform) Act 2023 (Commencement No. 2 and Saving Provisions) (Revocation) Regulations 2024.
[13] Jf. Section 183A i DPA 2018 som indført ved Section 106, stk. 2, i DUAA.

britiske parlament kan vælge bevidst at tilsidesætte databeskyttelseskravene[14], og ii) hvor visse bestemmelser i Data Protection Act (herefter "DPA 2018") er fritaget og som sådan vil have forrang for UK GDPR[15]. Konsekvenserne af den anden undtagelse er stadig uvisse og debatteres i Det Forenede Kongerige.

13. Med hensyn til beskyttelsen af de grundlæggende rettigheder, der er nedfældet i chartret, forklares det i betragtning 12 i udkastet til afgørelse, at alle henvisninger til grundlæggende rettigheder og friheder i UK GDPR og DPA 2018 er blevet erstattet med henvisninger til rettigheder i henhold til den europæiske menneskerettighedskonvention, som er indarbejdet i den nationale lovgivning i henhold til menneskerettighedsloven fra 1998[16].

14. Databeskyttelsesrådet opfordrer Kommissionen til at foretage en mere detaljeret vurdering af disse ændringer af den britiske retsorden, jf. punkt 10, 11 og 12 ovenfor, med henblik på at beskrive de ændringer, der er indført ved REUL Act, og vurdere deres indvirkning på den britiske databeskyttelsesramme. Databeskyttelsesrådet mener også, at dette område skal overvåges nøje af Kommissionen i fremtiden, og opfordrer Kommissionen hertil.

15. Endelig bemærker Databeskyttelsesrådet en række ændringer i henhold til DUAA med hensyn til den retlige ramme, der gælder for elektronisk kommunikation, herunder cookies, og minder om, at behandlingen af personoplysninger kan udløse det materielle anvendelsesområde for UK GDPR[17]. Derfor opfordrer Databeskyttelsesrådet Kommissionen til at inddrage dem i sin vurdering med henblik på den endelige beslutning, i det omfang de kan have indflydelse på databeskyttelsen. Databeskyttelsesrådet opfordrer endvidere Kommissionen til nøje at overvåge den praktiske virkning af ændringerne vedrørende cookies, der er fritaget for samtykke.

1.4. GENERELLE BEMÆRKNINGER OG BEKYMRINGER

1.4.1. INTERNATIONALE FORPLIGTELSER INDGÅET AF DET FORENEDE KONGERIGE

16. Med hensyn til de internationale forpligtelser, som Det Forenede Kongerige har indgået[18], glæder Databeskyttelsesrådet sig over, at Det Forenede Kongerige fortsat tilslutter sig den europæiske menneskerettighedskonvention (EMRK) og er underlagt Menneskerettighedsdomstolens jurisdiktion. Derudover er Det Forenede Kongerige også tiltrådt konvention 108[19] og tillægsprotokollen hertil[20] og

[14] Jf. Section 183A, stk. 3, i DPA 2018 som indført ved Section 106, stk. 2, i DUAA.
[15] Disse bestemmelser fremgår af Section 186, stk. 3, i DPA 2018. Det betyder, at når der er en konflikt mellem artikel 23 i UK GDPR og et af de anførte afsnit, f.eks. Schedule 2 i DPA 2018, der indeholder undtagelser fra den registreredes rettigheder, vil fortolkningen af DPA 2018 have forrang.
[16] Jf. artikel 8 i den europæiske menneskerettighedskonvention.
[17] Databeskyttelsesrådets udtalelse nr. 5/2019 om samspillet mellem e-databeskyttelsesdirektivet og databeskyttelsesforordningen, navnlig med hensyn til databeskyttelsesmyndighedernes kompetence, opgaver og beføjelser, vedtaget den 12. marts 2019, tilgængelig på: https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.
[18] Jf. kapitel 1: Generelle oplysninger om begrebet et tilstrækkeligt beskyttelsesniveau i Reference vedrørende et tilstrækkeligt beskyttelsesniveau.
[19] Jf. konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108 af 28. januar 1981).
[20] Jf. tillægsprotokollen til konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, om tilsynsmyndigheder og grænseoverskridende datastrømme, der blev åbnet for undertegnelse den 8. november 2001.

har underskrevet konvention 108+[21] i 2018. Disse internationale forpligtelser er vigtige overvejelser[22] og bør tages i betragtning som led i vurderingen af forlængelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige i henhold til både GDPR og retshåndhævelsesdirektivet.

17. Generelt støtter Databeskyttelsesrådet indsatsen for, at tredjelande hurtigt ratificerer konvention 108+ som et meningsfuldt skridt mod tilpasning til internationalt anerkendte databeskyttelsesprincipper og som et signal om deres engagement i bredere standarder og grundlæggende rettigheder.

1.4.2. SECRETARY OF STATE'S BEFØJELSER TIL AT INDFØRE ÆNDRINGER I DUAA VIA AFLEDT LOVGIVNING

18. Selvom de fleste af ændringerne i den britiske databeskyttelsesramme har til formål at præcisere og lette overholdelsen af loven, kan nogle af dem, afhængigt af deres gennemførelse, have indflydelse på standarden for beskyttelse af personoplysninger i Det Forenede Kongerige.

19. I den forbindelse bemærker Databeskyttelsesrådet, at Secretary of State har fået nye beføjelser til at indføre ændringer i DUAA via afledt lovgivning, som kræver mindre parlamentarisk kontrol. I visse tilfælde, f.eks. internationale overførsler (se afsnit 2.3), automatiske afgørelser (afsnit 2.4) og forvaltning af Information Commissioner's Office (afsnit 3), er disse nye beføjelser brede, og der er ingen yderligere oplysninger i udkastet til afgørelse om, hvilke garantier der vil blive stillet, og hvordan disse beføjelser skal anvendes i praksis.

20. Databeskyttelsesrådet opfordrer Kommissionen til i den endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet at fremhæve de områder, som den agter at overvåge nøje, fordi der er risiko for yderligere afvigelser fra EU's databeskyttelseslovgivning via den britiske afledte lovgivning.

2. GENERELLE DATABESKYTTELSESMÆSSIGE ASPEKTER

2.1. ANERKENDTE LEGITIME INTERESSER

2.1.1. GENERELLE BEMÆRKNINGER

21. I betragtning 22, 23 og 24 fokuserer Kommissionen sin vurdering på indførelsen af et nyt retsgrundlag, nemlig behandling, der er nødvendig af hensyn til en anerkendt legitim interesse. Bilag 1 til den opdaterede UK GDPR indeholder en liste over disse anerkendte legitime interesser.

22. Ifølge ICO's vejledning om dette emne[23] skal dataansvarlige, der baserer sig på en anerkendt legitim interesse som retsgrundlag, stadig overholde alle andre krav i henhold til UK GDPR, herunder sikre, at behandlingen er nødvendig og forholdsmæssig til det på forhånd godkendte formål. Da dette ikke er nævnt i udkastet til afgørelse og udgør et væsentligt element i konklusionen om, at dette nye

[21] Jf. ændringsprotokollen til konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108+ af 18. maj 2018).
[22] Jf. betragtning 105 i GDPR.
[23] Jf. ICO's vejledning om legitime interesser, tilgængelig på https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/.

retsgrundlag ikke underminerer niveauet af beskyttelse af de registreredes rettigheder, opfordrer Databeskyttelsesrådet Kommissionen til at præcisere dette punkt.

23. Opstillingen af anerkendte legitime interesser i loven forekommer ikke i sig selv problematisk, og det samme gælder beslutningen om at indføre et sådant nyt retsgrundlag, hvilket skaber større klarhed for de dataansvarlige og bør hilses velkommen.

24. Databeskyttelsesrådet noterer sig dog, at visse anerkendte legitime interesser består i: i) nødvendigheden af at behandle personoplysninger af hensyn til den nationale sikkerhed, den offentlige sikkerhed eller forsvaret (betingelsen "national sikkerhed, offentlig sikkerhed og forsvar"), ii) nødvendigheden af at behandle personoplysninger for at afsløre, efterforske eller forebygge en forbrydelse (betingelsen "kriminalitet") og iii) "videregivelse med henblik på behandling som beskrevet i artikel 6, stk. 1, litra e)".

25. Med hensyn til betingelsen "national sikkerhed, offentlig sikkerhed og forsvar" og betingelsen "kriminalitet" bemærker Databeskyttelsesrådet, at udkastet til afgørelse ikke indeholder yderligere oplysninger om dataansvarliges og databehandleres praktiske anvendelse af disse retsgrundlag. Databeskyttelsesrådet ønsker mere information fra Kommissionen om de modtagne yderligere oplysninger og stillede garantier vedrørende den praktiske anvendelse af dette retsgrundlag fra de britiske kompetente myndigheder, og opfordrer Kommissionen til at overvåge anvendelsen af dette retsgrundlag.

26. Databeskyttelsesrådet bemærker også, at ICO arbejder på specifik vejledning om dette spørgsmål, som – på tidspunktet for denne udtalelse – omfatter en definition af disse begreber. I betragtning af vigtigheden af, at disse begreber præciseres, opfordrer Databeskyttelsesrådet Kommissionen til nøje at følge udviklingen af ICO's vejledning.

2.1.2. OFFENTLIGGØRELSE MED HENBLIK PÅ BEHANDLING SOM BESKREVET I ARTIKEL 6, STK. 1, LITRA E)

27. Databeskyttelsesrådet bemærker, at den nyligt anerkendte legitime interesse, der tillader "videregivelse med henblik på behandling som beskrevet i 6, stk. 1, litra e)", indfører mulighed for at dele personoplysninger med offentlige myndigheder på frivillig basis. Som ICO præciserer i sin seneste vejledning[24], giver denne anerkendte legitime interesse ikke i sig selv de anmodende myndigheder ret til adgang til personoplysninger, men en dataansvarlig kan påberåbe sig denne forhåndsgodkendte interesse, når myndigheder meddeler, at de har brug for oplysninger til en offentlig opgave eller funktion. Databeskyttelsesrådet bemærker også, at disse anmodninger om videregivelse til offentlige opgaver ikke kun kan efterkommes for personoplysninger, der er beregnet til formål, der er omfattet af UK GDPR, men også kan vedrøre behandlingsformål i henhold til Part 3 og Part 4 i DPA 2018. Denne ændring er derfor også relevant med hensyn til regeringens adgang i forbindelse med retshåndhævelse og national sikkerhed.[25]

28. I denne sammenhæng opstår spørgsmålet om, hvilke kriterier den dataansvarlige skal vurdere for at beslutte, om data frivilligt skal udleveres efter en anmodning om oplysninger. Navnlig opfatter Databeskyttelsesrådet det således, hvilket ICO også påpeger i sin vejledning[26], at nødvendighedstesten

[24] Jf. fodnote 23.
[25] Jf. ICO's vejledning om betingelser for anmodning om offentliggørelse til udførelse af en offentlig opgave, tilgængelig på https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/what-are-the-recognised-legitimate-interest-conditions/public-task-disclosure-request-condition/.
[26] Jf. fodnote 23.

for denne betingelse om anerkendt legitim interesse adskiller sig fra de øvrige betingelser i bilag 1. I forbindelse med anmodninger om offentliggørelse til udførelse af offentlige opgaver betyder nødvendighed, at den dataansvarlige skal undersøge, hvilken behandling der er nødvendig for at videregive de ønskede personoplysninger. Den dataansvarlige skal overveje, om de oplysninger, de ønsker at dele, er forholdsmæssige og nødvendige for at efterkomme anmodningen. Nødvendighedstesten omfatter derimod ikke, om personoplysningerne rent faktisk er nødvendige for at udføre den offentlige opgave eller funktion, da den dataansvarlige kan stole på den anmodende parts erklæring om, at vedkommende har brug for personoplysningerne til en bestemt offentlig opgave[27]. I mange tilfælde, især når anmodningerne fremsættes med henblik på retshåndhævelse eller national sikkerhed, vil den dataansvarlige ikke være i stand til at foretage en sådan vurdering.

29. På denne baggrund opfordrer Databeskyttelsesrådet Kommissionen til nøje at overvåge den praktiske anvendelse af denne bestemmelse.

30. Efter Databeskyttelsesrådets opfattelse bør de retshåndhævende myndigheder og de nationale sikkerhedsmyndigheder ikke anvende denne mekanisme til at omgå eksisterende retlige begrænsninger af deres bindende dataindhentningsbeføjelser eller til at indhente flere data, end det er strengt nødvendigt for at udføre deres opgaver. Desuden finder Databeskyttelsesrådet det vigtigt, at dataansvarlige tager højde for ICO's vejledning om, hvordan man validerer en anmodning om offentliggørelse til en offentlig opgave, og opfordrer Kommissionen til at medtage dette aspekt i den regelmæssige revision af afgørelsen.[28]

2.2. INDIVIDUELLE RETTIGHEDER

31. Databeskyttelsesrådet anerkender Kommissionens analyse af, at der har været begrænsede ændringer på området individuelle rettigheder. Dette omfatter ændringer til artikel 12 og en ny artikel 12A i UK GDPR, som yderligere præciserer fristerne for besvarelse af anmodninger fra registrerede.[29] Derudover indeholder artikel 13, stk. 5, i UK GDPR en undtagelse fra retten til information, hvis personoplysninger behandles til videnskabelige eller historiske forskningsformål i henhold til yderligere garantier i artikel 84B i UK GDPR. Databeskyttelsesrådet finder, at begge ændringer ikke underminerer det i det væsentlige tilsvarende beskyttelsesniveau, som UK GDPR sikrer.

2.2.1. RET TIL INDSIGT

32. Artikel 15, stk. 1A, i UK GDPR indfører en proportionalitetsvurdering som udviklet i henhold til den britiske nationale retspraksis. Navnlig skal dataansvarlige kun foretage "rimelige og forholdsmæssige søgninger" for at efterkomme anmodninger om indsigt.

33. Databeskyttelsesrådet bemærker, at en sådan proportionalitetsvurdering ikke findes i EU's databeskyttelsesramme – den indeholder ikke noget generelt forbehold med hensyn til proportionalitet i de foranstaltninger, som den dataansvarlige skal træffe for at efterkomme de

[27] Jf. fodnote 23.

[28] ICO præciserer i sine retningslinjer om betingelser for offentliggørelse til offentlige opgaver (se fodnote 25), at dataansvarlige f.eks. bør anmode om, at anmodningen fremsættes skriftligt, og kontrollere, at anmodningen er autentisk, eller at organisationens medarbejder er bemyndiget til at handle på organisationens vegne.

[29] Navnlig på grund af behovet for at bekræfte den registreredes identitet eller betalingen af et gebyr.

registreredes anmodning i henhold til artikel 12 i GDPR, men at den kun indeholder grunde til afslag i underafsnit 5.[30]

34. Efter Databeskyttelsesrådets opfattelse er det derfor vigtigt i tilstrækkelig grad at definere begrebet "rimelige og forholdsmæssige søgninger", som bør fortolkes snævert og på en tilstrækkeligt ensartet måde. Dataansvarlige bør have en konsekvent forståelse af, hvad der er "rimeligt og forholdsmæssigt", uanset om det er baseret på retspraksis eller vejledning fra en tilsynsmyndighed, da anvendelsen af dette begreb potentielt kan føre til forskellige standarder for overholdelse af retten til indsigt, navnlig afhængigt af niveauet af tekniske og organisatoriske foranstaltninger, som den dataansvarlige har indført for at håndtere anmodninger om indsigt. Databeskyttelsesrådet ser gerne, at Kommissionen giver mere detaljerede oplysninger om fortolkningen af "rimelige og forholdsmæssige søgninger" baseret på den nationale vejledning og tilgængelige retspraksis. På denne baggrund opfordrer Databeskyttelsesrådet Kommissionen til at overvåge, at retten til indsigt ikke begrænses unødigt.

2.2.2. GARANTIER FOR "INDVANDRINGSUNDTAGELSE"

35. Den tidligere såkaldte "indvandringsundtagelse"[31] gjorde det muligt for dataansvarlige, der var involveret i "indvandringskontrol", at begrænse visse registreredes rettigheder i henhold til DPA 2018, hvis dette sandsynligvis ville skade visse immigrationskontrolaktiviteter[32]. På grund af indsigelser mod lovligheden af den på tidspunktet for vedtagelsen af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige var behandlingen af personoplysninger i henhold til undtagelsen udelukket fra denne afgørelses anvendelsesområde.

36. Siden den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige er indvandringsundtagelsen blevet suppleret med garantier to gange[33]. Den indeholder nu følgende garantier: i) den må kun påberåbes fra sag til sag, ii) den registreredes rettigheder og frihedsrettigheder og potentielle sårbarheder tages i betragtning, iii) Secretary of State fører en fortegnelse over brugen af indvandringsundtagelsen og underretter generelt den registrerede om dens brug, og iv) en præcisering af, at brugen af indvandringsundtagelsen er begrænset til den behandling, der foretages af Secretary of State (herunder det britiske indenrigsministerium og dets styrelser). Derudover blev den nødvendige afvejning for at afgøre, om udøvelsen af den registreredes rettigheder kan skade en effektiv indvandringskontrol, beskrevet nærmere. ICO udsendte også detaljerede retningslinjer for anvendelsen af undtagelsen. I sine retningslinjer bekræftede ICO den snævre fortolkning af undtagelsen og at begrænsninger i form af indvandringsundtagelsen kun bør anvendes selektivt på specifikke rettigheder for registrerede. Den fastslog også, at dataansvarlige ved gennemførelsen af afvejningstesten skal sikre, at risikoen for indvandringskontrol er betydelig og opvejer risikoen for personens interesser.

---

[30] Artikel 12, stk. 5, i GDPR "*Oplysninger, der gives i henhold til artikel 13 og 14, og enhver meddelelse og enhver foranstaltning, der træffes i henhold til artikel 15-22 og artikel 34, er gratis. Hvis anmodninger fra en registreret er åbenbart grundløse eller overdrevne, især fordi de gentages, kan den dataansvarlige enten: a) opkræve et rimeligt gebyr under hensyntagen til de administrative omkostninger ved at give oplysningerne eller meddelelsen eller træffe den ønskede foranstaltning, eller b) afvise at efterkomme anmodningen. Bevisbyrden for, at anmodningen er åbenbart grundløs eller overdreven, påhviler den dataansvarlige.*"

[31] Se Schedule 2 til DPA 2018, Part1 i den tidligere udgave af DPA.

[32] Jf. punkt 61 og 62 i Databeskyttelsesrådets udtalelse nr. 14/2021: "skade en effektiv indvandringskontrol" eller "efterforskningen eller afsløringen af aktiviteter, som ville underminere opretholdelsen af en effektiv immigrationskontrol".

[33] Gennem lovgivning i 2022 og 2024.

37. Databeskyttelsesrådet noterer sig Kommissionens detaljerede analyse. På baggrund af de juridiske udfordringer, der ligger forud for disse ændringer, opfordrer Databeskyttelsesrådet Kommissionen til at overvåge den videre anvendelse heraf.

2.3. BEGRÆNSNINGER FOR VIDEREOVERFØRSEL

38. Databeskyttelsesrådet glæder sig over Kommissionens fortsatte opmærksomhed på den praktiske anvendelse af de britiske regler om overførsel af personoplysninger til tredjelande, og det opfordrer Kommissionen til at opretholde og uddybe dette engagement. Dette er særlig relevant med hensyn til Secretary of State's beføjelse til at udstede nye målrettede regler for godkendelse af overførsler i) til en specifik sektor eller et specifikt geografisk område i et tredjeland, ii) til en bestemt dataansvarlig eller databehandler, iii) til en bestemt modtager af personoplysningerne, iv) af visse specifikke typer personoplysninger, v) foretaget ved hjælp af visse specifikke midler eller vi) på grundlag af relevant lovgivning, ordninger, lister eller andre ordninger eller dokumenter, da de har virkning fra tid til anden, og til at give en person en skønsbeføjelse (artikel 45A, stk. 4, i UK GDPR).

39. Databeskyttelsesrådet forstår, at artikel 45A, stk. 4, i UK GDPR har til formål at give fleksibilitet til at godkende visse overførsler. Med hensyn til nr. ii) og iii) forstår Databeskyttelsesrådet f.eks., at de kan omfatte overførsler til private enheder i et tredjeland. Dette vil betyde, at sådanne private enheder forpligter sig til at overholde databeskyttelsestesten. Det er fortsat uklart, hvordan Secretary of State i praksis vil vurdere, om specifikke dataansvarlige i et tredjeland – som ikke betragtes som tilstrækkeligt sikkert – kan opfylde databeskyttelsestesten (f.eks. med hensyn til klageadgang). Ligeledes er det fortsat uklart, hvordan databeskyttelsestesten vil blive gennemført for artikel 45A, stk. 4, nr. iv) og v), i UK GDPR.

40. Databeskyttelsesrådet vil sætte pris på, hvis Kommissionen kan give yderligere oplysninger om de supplerende oplysninger og garantier, der er modtaget om den praktiske anvendelse af databeskyttelsestesten, og redegøre for sin vurdering af, hvordan beskyttelsesniveauet opretholdes i sådanne situationer.[34] Databeskyttelsesrådet opfordrer også Kommissionen til nøje at overvåge udviklingen med hensyn til anvendelsen af denne bestemmelse.

41. Desuden forstår Databeskyttelsesrådet ud fra yderligere oplysninger fra Kommissionen, at kriteriet om "ønskeligheden af at lette overførsler af personoplysninger til og fra Det Forenede Kongerige" ikke er et element i databeskyttelsestesten, men blot en yderligere faktor, som Secretary of State kan overveje, når testens kriterier er fuldt ud opfyldt. Databeskyttelsesrådet opfordrer Kommissionen til at præcisere dette i sin endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet, da det ikke fremgår helt klart af lovteksten, samt til at overvåge dens praktiske konsekvenser og gennemførelse af et sådant kriterium.

42. Med hensyn til den nye databeskyttelsestest, som er indført med DUAA[35], bemærker Databeskyttelsesrådet, at den nye vejledende liste over elementer, der skal tages i betragtning ved tilstrækkelighedstesten, ikke er udtømmende, og at den nye tilstrækkelighedstest fastsætter, at beskyttelsesstandarden for registrerede i modtagende tredjelande eller internationale organisationer "ikke er væsentligt lavere" end den, der er fastsat for registrerede i den relevante databeskyttelseslovgivning i Det Forenede Kongerige. Denne liste fjerner vigtige elementer, der indgik i den tidligere tilstrækkelighedstest i Det Forenede Kongerige, og som spiller en vigtig rolle i vurderingen af, om et tredjeland tilbyder et i det væsentlige tilsvarende niveau for beskyttelse af

[34] Jf. artikel 45A, stk. 4, i UK GDPR.
[35] Jf. betragtning 42 i udkastet til afgørelse.

personoplysninger. Den nye test henviser ikke længere til i) tredjelandets regler vedrørende "offentlig sikkerhed, forsvar, national sikkerhed og strafferet og offentlige myndigheders adgang til personoplysninger", ii) retspraksis (i stedet henviser den nye test nu til "landets forfatning, traditioner og kultur"), iii) eksistensen af effektive og håndhævelige rettigheder, som de registrerede nyder, og de administrative og retslige retsmidler, som de registrerede, hvis personoplysninger overføres, reelt kan gøre brug af (i stedet henviser den nye test til b) eksistensen af og beføjelserne tilknyttet en myndighed, der er ansvarlig for at håndhæve beskyttelsen af de registrerede med hensyn til behandlingen af personoplysninger i landet eller af organisationen, c) ordninger for retslig eller udenretslig klageadgang for registrerede i forbindelse med en sådan behandling) og iv) en eller flere uafhængige tilsynsmyndigheder (i stedet henviser den nye test til en "myndighed, der er ansvarlig for at håndhæve beskyttelsen af registrerede med hensyn til behandlingen af personoplysninger i landet eller af organisationen").

43. Selv om det anerkendes, at referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR kun indeholder begrænsede oplysninger om dette aspekt, minder Databeskyttelsesrådet om sin henvisning til, at "beskyttelsesniveauet for fysiske personer, hvis oplysninger overføres, ikke må undermineres af videreoverførslen"[36], hvilket ikke kan fortolkes således, at den ikke omfatter behovet for en uafhængig tilsynsmyndighed og registreredes rettigheder, som er effektive og kan håndhæves.

44. Databeskyttelsesrådet opfordrer Kommissionen til specifikt at uddybe sin vurdering af disse aspekter yderligere. En sådan præcisering vil skabe stor retssikkerhed og bidrage til at styrke tilliden til tilstrækkelighedsinstrumentet. Databeskyttelsesrådet opfordrer også Kommissionen til nøje at overvåge udviklingen og den praktiske gennemførelse af den nye tilstrækkelighedstest.

45. Med hensyn til det britiske (associerede) medlemskab af forordningen om grænseoverskridende betalinger (CBPR) bemærker Databeskyttelsesrådet, at det nuværende medlemskab ikke letter dataoverførsler fra Det Forenede Kongerige til andre medlemmer af CBPR-forummet. Databeskyttelsesrådet glæder sig over Kommissionens holdning i denne henseende, herunder forpligtelsen til fortsat nøje at overvåge den videre udvikling i denne henseende, navnlig hvis Det Forenede Kongerige har til hensigt at blive et fuldgyldigt medlem, og minder om, at CBPR ikke anses for at sikre et tilstrækkeligt beskyttelsesniveau for personoplysninger, der stammer fra EU.

2.4. AUTOMATISKE AFGØRELSER

46. Databeskyttelsesrådet noterer sig Section 80 i DUAA (indførelse af artikel 22A-22D i UK GDPR), som indfører væsentlige ændringer af rammen for automatiske afgørelser, navnlig når den er baseret på behandling af ikke-særlige kategorier af data. Indtil DUAA blev vedtaget, afspejlede artikel 22 i UK GDPR EU's rammer for databeskyttelse med et generelt forbud mod automatiske afgørelser med begrænsede undtagelser.

47. Artikel 22B, stk. 1, i UK GDPR forbyder behandling af særlige kategorier af personoplysninger til afgørelser, der udelukkende er baseret på automatisk behandling, og som har retsvirkninger eller tilsvarende betydelige virkninger for den registrerede, med visse undtagelser (artikel 22B, stk. 2 og 3, i UK GDPR, herunder når behandlingen er baseret på samtykke, kontrakt eller lovkrav).

[36] Jf. kapitel 3: Generelle databeskyttelsesprincipper, der skal sikre, at databeskyttelsesniveauet i et tredjeland, et område eller en eller flere specifikke sektorer i det pågældende tredjeland, eller en international organisation i det væsentlige svarer til det niveau, der fastsættes i EU-lovgivningen, i referencen vedrørende et tilstrækkeligt beskyttelsesniveau i henhold til GDPR.

48. Databeskyttelsesrådet bemærker, at dette forbud ikke gælder, når dataansvarlige træffer væsentlige afgørelser ved hjælp af automatiske processer baseret på ikke-særlige kategorier af oplysninger, medmindre retsgrundlaget for behandlingen er en anerkendt legitim interesse i henhold til artikel 6, stk. 1, litra ea), i UK GDPR.

49. Lovens fokus skifter fra at begrænse brugen af automatiske afgørelser til at sikre, at der er garantier på plads for vigtige afgørelser. Disse garantier omfatter at i) give den registrerede oplysninger om afgørelsesprocessen, ii) give den registrerede mulighed for at fremsætte bemærkninger til afgørelsen[37], iii) gøre indsigelse mod en sådan afgørelse samt iv) give den registrerede mulighed for at anmode om menneskelig indgriben fra den dataansvarliges side. Databeskyttelsesrådet bemærker, at selv om denne nye tilgang udgør en afvigelse fra den tidligere retlige ramme, kræver artikel 22C i UK GDPR, at dataansvarlige gennemfører passende garantier, der sikrer et tilstrækkeligt beskyttelsesniveau for registrerede.

50. I lyset af det hastigt skiftende lovgivningsmæssige miljø og fremskridt inden for automatiserede teknologier såsom AI, opfordrer Databeskyttelsesrådet Kommissionen til at udvide sin vurdering i den endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet af de forventede praktiske virkninger af denne nye tilgang, som endnu ikke er afprøvet i praksis, samt overvåge gennemførelsen heraf.

2.4.1. AUTOMATISKE AFGØRELSER OG MENNESKELIG MEDVIRKEN

51. Databeskyttelsesrådet glæder sig over præciseringen med hensyn til betydningen af automatiske afgørelser og menneskelig medvirken. Artikel 22A i UK GDPR præciserer, at en afgørelse, der udelukkende er baseret på automatisk behandling, betyder, at der ikke er nogen meningsfuld menneskelig medvirken, når den træffes. Dataansvarlige skal også vurdere, i hvilket omfang profilering bidrager til en afgørelse, for at afgøre, om menneskelig medvirken var meningsfuld.

52. I forlængelse heraf giver artikel 22D i UK GDPR Secretary of State beføjelse til gennem lovbestemmelser at præcisere, hvorvidt der er eller ikke er en meningsfuld menneskelig medvirken i vedtagelsen af den afgørelse, der er beskrevet i forordningen. Tilsvarende har Secretary of State også beføjelse til at beskrive, om den afgørelse, der er beskrevet i forordningen, anses for at have en tilsvarende væsentlig indvirkning på de registrerede.

53. Omfanget af disse skønsbeføjelser er uklare. Databeskyttelsesrådet opfordrer derfor Kommissionen til at analysere disse nyligt tildelte beføjelser til Secretary of State og overvåge udviklingen i denne henseende. På den anden side er Secretary of State's ekstra beføjelser med hensyn til de garantier, der kræves i artikel 22C i UK GDPR, en velkommen ændring, da de vil udbygge og/eller supplere de allerede krævede garantier samt fastlægge, hvad der er utilstrækkeligt med hensyn til garantier.

[37] Dvs. give yderligere oplysninger og begrundelser, hvilket endnu ikke er en formel juridisk indsigelse.

3. PROCEDURE OG HÅNDHÆVELSESMEKANISME

3.1. TILSYN OG HÅNDHÆVELSE

3.1.1. UAFHÆNGIGT TILSYN

54. Databeskyttelsesrådet bemærker, at Information Commissioner (ICO), der tidligere var struktureret som et enkeltmandsforetagende, med ikrafttrædelsen af DUA Act[38] vil få en ny struktur og blive en juridisk person (en bestyrelse), nemlig Information Commission (IC) i henhold til artikel 148 og Schedule 12A i DPA 2018.

55. Databeskyttelsesrådet bemærker, at omstruktureringen af en myndighed fra et enkeltmandsforetagende til en bestyrelse ikke i sig selv påvirker myndighedens uafhængighed og effektive håndhævelse. Der bør lægges vægt på andre elementer såsom reglerne om udnævnelse og afskedigelse, og i forlængelse heraf glæder Databeskyttelsesrådet sig over, at kun Hans Majestæt kan fjerne formanden for IC fra sit embede efter henstilling fra begge kamre i det britiske parlament i tilfælde af alvorlige forseelser.

56. Schedule 12A i DPA 2018 indeholder detaljerede regler om den nye IC's arbejde og funktion. Denne regulerer blandt andet IC's strukturelle og organisatoriske rammer, kravene til udnævnelse af dets udøvende og ikke-udøvende medlemmer samt andet personale (ansatte og et eksternt udvalg) og indeholder bestemmelser om mandatperiode, vederlag, regnskabsføring og afskedigelse. Nummer 5 og 6 i Schedule 12A[39] indeholder regler og garantier, der skal iagttages ved udnævnelse af ikke-udøvende medlemmer, og som kan være relevante for organets oprettelse og uafhængighed (f.eks. udvælgelse efter kvalifikationer og interessekonflikter).

57. Databeskyttelsesrådet bemærker, at udkastet til afgørelse ikke indeholder nærmere oplysninger om ændringen af den nye databeskyttelsesmyndigheds arbejde og funktion. Desuden er der ingen nærmere oplysninger om proceduren for udnævnelse og afskedigelse af udøvende og ikke-udøvende medlemmer. Da disse elementer er relevante for vurderingen af tilsynsmekanismen, opfordrer Databeskyttelsesrådet Kommissionen til yderligere at beskrive ændringerne og den relevante vurdering, navnlig med hensyn til IC's struktur og organisation, udnævnelsen og afskedigelsen af dens medlemmer, herunder de ikke-udøvende.

58. Med hensyn til IC's uafhængighed bemærker Databeskyttelsesrådet, at interessekonflikter i henhold til Section 6 i Schedule 12A til DPA 2018 kan forhindre Secretary of State i at udnævne en person til formand eller ikke-udøvende medlem af IC. I definitionen af udtrykket "interessekonflikt" henvises der i Section 6, stk. 5, til en økonomisk eller anden interesse, der kan påvirke den pågældende persons udøvelse af sit hverv som medlem af IC i negativ retning. Hvad angår IC-medlemmernes uafhængighed, kan en sådan "anden interesse", f.eks. særlig økonomisk tilknytning og/eller forretningsforbindelser, også tyde på interessekonflikter og bør tages i betragtning ved udnævnelsen af medlemmer til IC. Databeskyttelsesrådet opfordrer derfor Kommissionen til at overvåge, at begrænsningerne finder anvendelse i praksis.

59. I forbindelse med de opdaterede mål, som de interne kontrolstandarder skal tage hensyn til ved udførelsen af deres opgaver og udarbejdelsen af deres strategi, såsom fremme af innovation og

[38] Jf. Part 6 "The Information Commission", DUAA nr. 117, s. 133 ff.
[39] Jf. Schedule 12A til DPA 2018.

konkurrence (Section 120B i DPA 2018), minder Kommissionen om, at "EU's databeskyttelseslovgivning også tilsvarende afvejer beskyttelsen af personoplysninger med flere andre grundlæggende rettigheder og mål", og henviser til betragtning 2 og 4 samt artikel 23 i GDPR. Databeskyttelsesrådet anerkender, at databeskyttelse ikke er en absolut rettighed og skal afvejes i forhold til andre grundlæggende rettigheder og mål i overensstemmelse med proportionalitetsprincippet. Databeskyttelsesrådet bemærker imidlertid, at betragtning 2 og 4 i GDPR samt artikel 23 i GDPR adskiller sig fra en retlig bestemmelse, der udtrykkeligt kræver, at databeskyttelsesmyndighederne tager hensyn til en række mål i udøvelsen af deres funktioner. Af hensyn til klarheden opfordrer Databeskyttelsesrådet Kommissionen til at omformulere denne betragtning for at undgå at give indtryk af, at betragtning 2 og 4 samt artikel 23 i GDPR har samme betydning som Section 120B i DPA 2018, og overvåge, at gennemførelsen af disse opdaterede mål i praksis ikke fører til en uforholdsmæssig stor ubalance til skade for retten til beskyttelse af personoplysninger, der ville underminere beskyttelsesniveauet for personoplysninger.

3.1.2. HÅNDHÆVELSE, HERUNDER SANKTIONER

60. Databeskyttelsesrådet glæder sig over, at bestemmelsen i det tidligere lovforslag om reform af den britiske databeskyttelsesramme, Data Protection and Digital Information Bill[40] (herefter "DPDI-lovforslaget"), der fastsatte, at ICO skulle tage hensyn til Secretary of State's holdning i udøvelsen af sine beføjelser, ikke længere er medtaget i den nye databeskyttelsesramme.

61. Databeskyttelsesrådet finder det også positivt, at ICO siden vedtagelsen af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige har offentliggjort en lang række nyttige adfærdskodekser, retningslinjer, udtalelser og andre vejledninger til de relevante parter.

62. Som i udtalelse nr. 14/2021[41] fremhæver Databeskyttelsesrådet, at en effektiv tilsynsmekanisme, der giver mulighed for uafhængig undersøgelse af klager samt effektive administrative og retlige klageprocedurer, er centrale elementer i vurderingen af, om et databeskyttelsessystem giver et tilstrækkeligt beskyttelsesniveau. Desuden spiller eksistensen af effektive sanktioner en vigtig rolle for at sikre, at reglerne overholdes.

63. På denne baggrund henleder Databeskyttelsesrådet Kommissionens opmærksomhed på den offentlige høring, som ICO iværksatte den 22. august vedrørende sine forslag til behandling af klager[42], dvs. efter, at Kommissionen havde fremsat sit udkast til afgørelse. I indledningen[43] til forslagene til offentlig høring angiver ICO, at det forventer, at når DUAA t træder i kraft, vil flere klager blive løst af organisationerne uden inddragelse af ICO. Baggrunden for ICO's vurdering er, at DUAA fastsætter nye krav til organisationer om at indføre en klageprocedure specifikt for databeskyttelsesspørgsmål. Artikel 164A i DPA 2018[44] fastslår, at dataansvarlige skal træffe foranstaltninger for at hjælpe personer, der ønsker at klage over brugen af deres personoplysninger. De skal f.eks. stille en klageformular til rådighed, som kan udfyldes elektronisk og på anden vis, de skal bekræfte modtagelsen af klager inden for 30 dage og "uden unødig forsinkelse" træffe passende foranstaltninger til at besvare klagen og underrette klageren om resultatet af klagen. Hvis klager skal behandles af ICO, bør de forslag, der

[40] Jf. Section 32, ny artikel 120 E, F, G og H i Data Protection and Digital Information Bill.
[41] Jf. Databeskyttelsesrådets udtalelse nr. 14/2021, punkt 112-114.
[42] Jf. ICO's høring om udkast til ændringer i vores håndtering af klager vedrørende databeskyttelse: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/08/ico-consultation-on-draft-changes-to-how-we-handle-data-protection-complaints/; https://ico.org.uk/media2/nrljbhr2/proposed-dpt-framework-20250822.pdf
[43] Jf. fodnote 41.
[44] Jf. artikel 164A i DPA 2018.

fremsættes til offentlig høring, danne grundlag for ICO's klagebehandling. I den forbindelse foreslår ICO en form for triage-system, hvor klager behandles med forskellige prioriteter og resultater. Dette bør gøre det muligt for ICO som strategisk tilsynsmyndighed at fokusere sine ressourcer på de vigtigste risici og identificere systemiske problemer på et tidligere tidspunkt. ICO's forslag indeholder en ikke-udtømmende liste over kriterier, der kan øge eller mindske sandsynligheden for, at en klage bliver forfulgt yderligere[45].

64. De ændringer, der er beskrevet i punkt 57, kan føre til en ændring af den interne tilsynsmyndigheds tilgang til klagebehandling. Eftersom den offentlige høring først blev iværksat efter fremsættelsen af Kommissionens udkast til afgørelse, er disse ændringer endnu ikke afspejlet i udkastet til afgørelse.

65. Databeskyttelsesrådet opfordrer Kommissionen til at medtage dette element i sin vurdering og til navnlig at følge op på resultaterne af ICO's offentlige høring. Databeskyttelsesrådet opfordrer desuden Kommissionen til nøje at overvåge IC's fremtidige behandling af klager for at sikre, at der fortsat garanteres et tilsvarende beskyttelsesniveau.

66. Databeskyttelsesrådet bemærker endvidere, at de omfattende lovgivningsmæssige beføjelser, som Secretary of State er tillagt i kraft af DUA Act, herunder beføjelsen til at vedtage lovbestemmelser, kan have betydning for IC's og dets medlemmers arbejde. Databeskyttelsesrådet henviser f.eks. til, at det er nødvendigt, at IC hører Secretary of State i forbindelse med nogle af opgaverne. Navnlig kræver artikel 124A i DPA 2018[46], at IC fastlægger passende adfærdskodekser, der indeholder retningslinjer for korrekt behandling af personoplysninger, når det kræves i en retsakt, som Secretary of State har vedtaget. IC skal høre Secretary of State inden ændring eller udarbejdelse af sådanne kodekser.

67. I betragtning af betydningen af IC's uafhængighed opfordrer Databeskyttelsesrådet Kommissionen til nøje at overvåge Secretary of State's nye beføjelser, navnlig deres praktiske indvirkning på IC's arbejde.

68. Som Databeskyttelsesrådet allerede understregede i udtalelse nr. 14/2021, er ICO godt udstyret med de nødvendige beføjelser, der nøje svarer til de beføjelser, som EU-medlemsstaternes tilsynsmyndigheder har, jf. artikel 58 i GDPR. Samtidig er tilstedeværelsen af effektive sanktioner, som Databeskyttelsesrådet allerede har fremhævet, vigtig med hensyn til at sikre iagttagelsen af reglerne. Databeskyttelsesrådet opfordrer Kommissionen til at foretage en mere detaljeret vurdering og overvåge anvendelsen af korrigerende beføjelser, effektiviteten af sanktioner og retsmidler for de berørte parter i den britiske databeskyttelsesramme[47].

4. DET FORENEDE KONGERIGES OFFENTLIGE MYNDIGHEDERS INDSIGT I OG ANVENDELSE AF PERSONOPLYSNINGER, SOM ER OVERFØRT FRA DEN EUROPÆISKE UNION

69. Udkastet til afgørelse fokuserer på udviklinger, der er relevante for vurderingen af beskyttelsesniveauet i Det Forenede Kongerige siden vedtagelsen af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige, som fortsat er gyldig for de aspekter, der ikke er blevet ændret eller berørt. Denne generelle tilgang omfatter også Kommissionens analyse af offentlige myndigheders adgang til og brug af personoplysninger i Det Forenede Kongerige. Dette specifikke aspekt omtales ofte som "regeringens adgang" og er et af de elementer, der er anført

[45] Jf. fodnote 41.
[46] Adfærdskodeks for behandling af personoplysninger.
[47] Jf. Databeskyttelsesrådets udtalelse nr. 14/2021, punkt 113.

i artikel 45, stk. 2, litra a), i GDPR, som Kommissionen skal tage hensyn til ved afgørelsen af, om beskyttelsesniveauet i det væsentlige er tilsvarende.

70. På denne baggrund behandler de følgende afsnit en række specifikke punkter, der er rejst i det udkast til afgørelse, der i øjeblikket er til behandling, og som er relevante i forhold til personoplysninger, der overføres fra EØS i henhold til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige i henhold til GDPR, og som offentlige myndigheder i Det Forenede Kongerige har adgang til og behandler, herunder videreoverførsler. Databeskyttelsesrådets analyse og bemærkninger i udtalelse nr. 14/2021[48] forbliver generelt gyldige.

4.1. DE BRITISKE OFFENTLIGE MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER MED HENBLIK PÅ RETSHÅNDHÆVELSE PÅ DET STRAFFERETLIGE OMRÅDE

71. Databeskyttelsesrammerne for de britiske offentlige myndigheders adgang til og brug af personoplysninger med henblik på retshåndhævelse på det strafferetlige område har været genstand for lovgivningsmæssige ændringer siden Kommissionens tidligere vurdering, som fastlagt i den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige. Disse omfatter National Security Act 2023, Investigatory Powers Amendment Act 2024 og indførelsen af DUAA. Sidstnævnte behandles også i Kommissionens udkast til afgørelse om ændring af gennemførelsesafgørelse (EU) 2021/1773 samt i Databeskyttelsesrådets tilsvarende udtalelse, der er afgivet på grundlag af artikel 51, stk. 1, litra g), i retshåndhævelsesdirektivet.

4.1.1. RETSGRUNDLAG OG GÆLDENDE GARANTIER

4.1.1.1. EFTERFORSKNINGSBEFØJELSER TIL RETSHÅNDHÆVELSESFORMÅL

72. I betragtning 81-85 i udkastet til afgørelse redegør Kommissionen for ændringerne til Investigatory Powers Act 2016 (lov om efterforskningsbeføjelser fra 2016, herefter "IPA 2016"), indført ved Investigatory Powers Amendment Act 2024, for så vidt angår behandling til retshåndhævelsesformål.[49] Samlet set fremlægger Kommissionen detaljerede oplysninger. Med hensyn til én specifik ændring mener Databeskyttelsesrådet imidlertid, at udkastet til afgørelse med fordel kunne præciseres yderligere.

73. Med Investigatory Powers Amendment Act 2024 blev definitionen af "teleoperatør", dvs. de potentielle modtagere af en "retention notice" (et pålæg om opbevaring af oplysninger) i henhold til IPA 2016, revideret.[50] Den ændrede definition omfatter nu enhver person, der "kontrollerer eller udbyder et telekommunikationssystem, som i) ikke (helt eller delvist) er etableret i eller kontrolleres fra Det Forenede Kongerige, og ii) anvendes af en anden person til at tilbyde eller levere en teletjeneste til personer i Det Forenede Kongerige". Selv om Kommissionen henviser til de forklarende bemærkninger i Investigatory Powers Amendment Act 2024, hvoraf det fremgår, at Section 261, stk. 10, litra c), "indeholder yderligere præciseringer, der sikrer, at store virksomheder med komplekse

[48] Jf. Databeskyttelsesrådets udtalelse nr. 14/2021.

[49] Kommissionen påpeger, som beskrevet i betragtning 139-141 i gennemførelsesafgørelse (EU) 2021/1772, at visse retshåndhævende myndigheder også kan anvende målrettede efterforskningsbeføjelser i henhold til IPA 2016 med henblik på at forebygge eller afsløre grov kriminalitet. Ændringer af sådanne bestemmelser vedrører derfor ikke kun adgangen til oplysninger til nationale sikkerhedsformål, men også til retshåndhævelsesformål.

[50] Section 261, stk. 10, litra c) i IPA 2016, indføjet ved Section 19 i Investigatory Powers Amendment Act 2024.

virksomhedsstrukturer er fuldt omfattet af IPA 2016", og at "ændringen [...] ikke søger at bringe yderligere virksomheder inden for anvendelsesområdet", er virkningerne af denne ændring fortsat uklare, f.eks. om den vil udvide mængden af personoplysninger, der potentielt er omfattet af et pålæg om opbevaring Databeskyttelsesrådet opfordrer derfor Kommissionen til at behandle virkningerne af denne ændring nærmere og specifikt overvåge dette aspekt, navnlig i lyset af principperne om nødvendighed og proportionalitet.

4.1.1.2. UNDTAGELSER AF HENSYN TIL NATIONAL SIKKERHED FOR RETSHÅNDHÆVENDE MYNDIGHEDER

74. Section 88 i DUAA opdaterer de eksisterende undtagelser af hensyn til national sikkerhed inden for retshåndhævelsesrammen, så de afspejler de undtagelser, der findes i UK GDPR og efterretningstjenesternes regler.[51] Selvom de retshåndhævende myndigheder allerede kan begrænse visse forpligtelser af hensyn til beskyttelsen af den nationale sikkerhed – f.eks. de forpligtelser, der vedrører registreredes rettigheder – vil Section 78A i DPA 2018[52] også omfatte de fleste databeskyttelsesprincipper[53] og visse internationale dataoverførselskrav[54] som bestemmelser, der kan fraviges, hvis det er nødvendigt af hensyn til beskyttelsen af den nationale sikkerhed. Derudover kan nogle IC'ers beføjelser til at foretage tilsyn og iværksætte håndhævelsesforanstaltninger[55] muligvis fraviges under sådanne omstændigheder.

75. Disse ændringer nævnes ikke i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 45 i GDPR eller udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 36 i retshåndhævelsesdirektivet. Databeskyttelsesrådet finder det imidlertid vigtigt at vurdere disse udvidede undtagelser i forhold til principperne om nødvendighed og proportionalitet. I denne forbindelse minder Databeskyttelsesrådet om den anden af de fire såkaldte "europæiske væsentlige garantier": enhver begrænsning af udøvelsen af de rettigheder og friheder, der anerkendes ved chartret, skal respektere deres væsentligste indhold og kan med forbehold af proportionalitetsprincippet kun indføres, hvis den er nødvendig og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og frihedsrettigheder.[56] Databeskyttelsesrådet er bekymret over undtagelserne fra centrale databeskyttelsesprincipper, krav til internationale overførsler og IC's beføjelser.

76. I henhold til den reviderede regel kan fem af de seks databeskyttelsesprincipper fraviges, hvis det er nødvendigt for at beskytte den nationale sikkerhed.[57] Disse principper fastslår blandt andet, at det

[51] Se også Department for Science, Innovation & Technology, Data (Use and Access) Act factsheet: UK GDPR and DPA, offentliggjort den 27. juni 2025, s. 14, https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa.

[52] DUAA vil blive indfaset i flere trin. De væsentligste ændringer af databeskyttelseslovgivningen i Part 5 i Data (Use and Access) Act træder i kraft som led i trin 3, ca. 6 måneder efter stadfæstelse, https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement.

[53] Jf. Section 78A, stk. 1), stk. 2), litra a), og stk. 3), i Data Protection Act 2018 som indført ved Section 88 i DUAA.

[54] Jf. Section 78A, stk. 1), stk. 2), litra d), og stk. 4), i Data Protection Act 2018 som indført ved Section 88 i DUAA.

[55] Jf. Section 78A, stk. 1), stk. 2), litra e), f) og g), i Data Protection Act 2018 som indført ved Section 88 i DUAA.

[56] Jf. henstilling 2/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, vedtaget den 10. november 2020, s. 10.

[57] I henhold til Section 78A, stk. 2 og 3, i Data Protection Act 2018 finder kapitel 2 i del 3 i denne lov ikke anvendelse, hvis det er nødvendigt af hensyn til beskyttelsen af den nationale sikkerhed, med undtagelse af a) Section 35, stk. 1 (det første databeskyttelsesprincip), for så vidt som det kræver, at behandlingen af personoplysninger skal være lovlig, b) Section 35, stk. 2-5 (lovligheden af behandlingen og begrænsninger i behandlingen af følsomme oplysninger), c) Section 42 (sikkerhedsforanstaltninger: behandling af følsomme oplysninger), og d) Schedule 8 (betingelser for behandling af følsomme oplysninger).

retshåndhævelsesformål, hvortil personoplysninger indsamles, skal være specificeret, eksplicit og legitimt, og at personoplysninger skal være tilstrækkelige, relevante og ikke omfatter mere end, hvad der er nødvendigt til dette formål. De præciserer også, at personoplysninger skal være korrekte og kun opbevares så længe, det er nødvendigt. Som nævnt ovenfor omfatter de fremtidige undtagelser desuden nogle af kravene til internationale overførsler, såsom den såkaldte "anden betingelse for internationale overførsler", der er fastsat i Section 73, stk. 3, i Data Protection Act 2018. Denne betingelse kræver, at overførsler enten baseres på bestemmelser om tilstrækkeligheden af beskyttelsesniveauet, passende garantier eller – hvis ingen af disse finder anvendelse – på særlige omstændigheder. Undtagelserne påvirker også IC's beføjelser, f.eks. beføjelsen til at udstede "information notices" (pålæg om udlevering af oplysninger) og "enforcement notices" (pålæg om overholdelse).[58]

77. Databeskyttelsesrådet bemærker, at selv om fritagelserne klart afviger fra retshåndhævelsesdirektivet, svarer de i høj grad til undtagelser og begrænsninger af hensyn til den nationale sikkerhed, der er fastsat i artikel 11 i Europarådets "moderniserede konvention 108" ("konvention 108+"[59]), som Det Forenede Kongerige undertegnede den 10. oktober 2018, men som på datoen for denne udtalelse ikke er blevet ratificeret af Det Forenede Kongerige eller endnu ikke er trådt i kraft.[60] I den forbindelse minder Databeskyttelsesrådet om, at Den Rådgivende Komité under konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (T-PD) for nylig har udstedt retningslinjer for de generelle principper i artikel 11 i den moderniserede konvention108[61].

78. I sin vejledning understreger Europarådet udtrykkeligt, at ingen undtagelse finder anvendelse, bl.a. af hensyn til proportionaliteten og legitimiteten af principperne om formålet med behandlingen. Det indebærer, at proportionaliteten af databehandlingen skal sikres, ligesom kravene om at behandle personoplysninger til et legitimt formål opfyldes. I overensstemmelse med vejledningen til konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger er Databeskyttelsesrådet særlig opmærksomt på eventuelle undtagelser fra proportionalitetsprincippet og fra kravet om at behandle personoplysninger til et legitimt formål. Tilsvarende mener Databeskyttelsesrådet, at eventuelle undtagelser fra tilsynsmyndighedens beføjelser bør gribes forsigtigt an. Selvom specifikke krav til tilsynsaktiviteter – såsom sikkerhedsgodkendelser – kan være relevante i forbindelse med behandling af oplysninger, der vedrører national sikkerhed, er det vigtigt at sikre et effektivt tilsyn for at forhindre, at der opstår et tilsynsmæssigt vakuum. I samme ånd fastsættes det i artikel 11, stk. 3, i konvention 108+, at undtagelser fra[62] konventionens artikel 15 "ikke berører kravet om, at behandlingsaktiviteter til nationale sikkerheds- og forsvarsformål skal underkastes uafhængig og effektiv kontrol og tilsyn i henhold til den nationale lovgivning" hos parterne i konventionen. Desuden bør eventuelle undtagelser fortolkes så restriktivt som muligt. Det forhold, at personoplysninger behandles af hensyn til den nationale sikkerhed, bør ikke i sig selv være tilstrækkeligt til, at der kan påberåbes en

[58] "Information notices" kræver, at en dataansvarlig eller databehandler giver IC de oplysninger, der med rimelighed er nødvendige for udførelsen af dennes funktioner. "Enforcement notices" giver IC beføjelse til at pålægge en person at træffe (eller undlade at træffe) bestemte foranstaltninger, hvis han finder, at personen ikke overholder bestemte databeskyttelsesforpligtelser.

[59] Jf. protokol om ændring af konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (CETS nr. 223).

[60] https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223

[61] https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/1680b6c146

[62] Jf. artikel 15 i konvention 108+, hvori det præciseres, hvordan parterne i konventionen skal sikre, at konventionens bestemmelser overholdes, ved at oprette en eller flere tilsynsmyndigheder.

undtagelse. Det bør stå klart, at en undtagelse fra databeskyttelsesordningen skal anvendes fra sag til sag, og kun hvis det er nødvendigt og forholdsmæssigt.[63]

79. Eftersom udkastene til afgørelser om tilstrækkeligheden af beskyttelsesniveauet ikke behandler dette punkt, opfordrer Databeskyttelsesrådet Kommissionen til at supplere sin vurdering i udkastet til afgørelse samt til specifikt at overvåge anvendelsen af de nationale sikkerhedsundtagelser for retshåndhævende myndigheder i praksis.

4.1.2. FÆLLES DATAANSVAR MELLEM DE BRITISKE EFTERRETNINGSTJENESTER OG RETSHÅNDHÆVENDE MYNDIGHEDER

80. På grundlag af de ændringer, som DUAA medfører, kan behandlingsaktiviteter foretaget af retshåndhævende myndigheder under særlige omstændigheder falde ind under de regler, der normalt finder anvendelse på de nationale sikkerhedsmyndigheders behandling af personoplysninger.[64] Med andre ord udvides databeskyttelsesrammen for behandling af nationale sikkerhedsoplysninger, der er fastlagt i Part 4 i DPA 2018, til at omfatte databehandling foretaget af retshåndhævende myndigheder, med forbehold af betingelserne i Section 89 i DUAA.

81. Kommissionen understreger, at betingelserne i Section 89 i DUAA indeholder strenge garantier: En kompetent myndighed skal angives som "kvalificeret kompetent myndighed" i regler fastsat af Secretary of State, som desuden skal udpege en bestemt behandlingsaktivitet, der udføres af den kvalificerede kompetente myndighed som fælles dataansvarlig sammen med mindst én efterretningstjeneste med henblik på at beskytte den nationale sikkerhed.[65]

82. Databeskyttelsesrådet anerkender, at disse garantier indebærer betydelige begrænsninger, men opfordrer Kommissionen til at overvåge den praktiske gennemførelse af disse regler. Der bør lægges særlig vægt på at sikre, at Part 4 i DPA 2018 udelukkende anvendes på behandlingsaktiviteter vedrørende national sikkerhed uden at udvides til andre sammenhænge. Selv om staterne har vide skønsbeføjelser med hensyn til nationale sikkerhedsspørgsmål, som det også anerkendes af ECHR[66], er det Databeskyttelsesrådets opfattelse, at trusler mod den nationale sikkerhed skal kunne skelnes fra hinanden ud fra deres art, alvor og de specifikke omstændigheder fra generelle risici for den offentlige sikkerhed eller fra grov kriminalitet. Kun i sådanne tilfælde er de retshåndhævende myndigheders arbejde i henhold til databeskyttelsesrammen for efterretningstjenester foreneligt med principperne om nødvendighed og proportionalitet.[67] Desuden finder Databeskyttelsesrådet det nødvendigt at overvåge, om kvalificerede kompetente myndigheder i praksis kan opretholde en klar sondring mellem

[63] Jf. også artikel 11 i konvention 108+, hvori det præciseres, at undtagelser skal være fastsat ved lov, respektere essensen af de grundlæggende rettigheder og frihedsrettigheder og udgøre en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund. I henhold til retningslinjerne i konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger vedrørende de generelle principper i artikel 11 indebærer dette, at der skal foretages og begrundes en afvejning af de involverede interesser mellem behovet for at fastsætte undtagelser fra visse bestemmelser i konventionen og respekten for den enkeltes menneskerettigheder og grundlæggende frihedsrettigheder.
[64] Jf. betragtning 72 i udkastet til afgørelse.
[65] Jf. betragtning 73 i udkastet til afgørelse.
[66] Jf. ECHR, Big Brother Watch m.fl. mod Det Forenede Kongerige, 25. maj 2021, præmis 305.
[67] Det følger af EU-Domstolens retspraksis, når den anvender nødvendigheds- og proportionalitetstesten på medlemsstaternes lovgivning, der giver offentlige myndigheder mulighed for at opbevare og få adgang til personoplysninger, at legitime mål såsom national sikkerhed eller bekæmpelse af grov kriminalitet er forskellige og derfor kan begrunde forskellige former for indgreb. Jf. Domstolen, forenede sager C-511/18, C-512/18 og C-520/18, La Quadrature du Net m.fl., 6. oktober 2020.

forskellige behandlingsformål for at overholde de tilsvarende retlige rammer i overensstemmelse hermed.

4.1.3. RETTEN TIL ADGANG

83. DUAA specificerer, at registrerede kun har ret til adgang til de relevante oplysninger, i det omfang, den dataansvarlige er i stand til at levere disse på grundlag af en rimelig og proportional søgning. Denne ændring indføres både i retshåndhævelsesrammen og i den nationale sikkerhedsramme.[68]

84. Kommissionen forklarer dette som en præcisering i overensstemmelse med fastlagte standarder, der er udviklet i henhold til national retspraksis, og som også tager hensyn til den registreredes interesser. Alligevel havde Databeskyttelsesrådet gerne set flere oplysninger om, hvordan begrebet "rimelig og forholdsmæssig søgning" fortolkes, også fordi artikel 14 i retshåndhævelsesdirektivet ikke indeholder et sådant element. Databeskyttelsesrådet anerkender, at der faktisk kan være scenarier, hvor en dataansvarligs bestræbelser på at identificere og lokalisere oplysninger om den registrerede kan betragtes som urimelige og uforholdsmæssige uden at bringe den væsentlige ækvivalens i fare.[69] Databeskyttelsesrådet minder om analysen og konklusionen i punkt 34 i denne udtalelse, som er relevante for både retshåndhævelsesordningen og den nationale sikkerhedsordning.

4.1.4. VIDEREOVERFØRSEL

4.1.4.1. EN NY DATABESKYTTELSESTEST

85. Når en kompetent myndighed har til hensigt at dele personoplysninger, der behandles i henhold til Part 3 i DPA 2018, med retshåndhævende myndigheder i et tredjeland, gælder der særlige krav. Disse overførsler kan navnlig finde sted, når de er godkendt i henhold til bestemmelser, som er fastlagt af Secretary of State eller, i mangel af sådanne, på grundlag af passende garantier. Hvis en overførsel hverken kan baseres på bestemmelser eller passende garantier, kan den kun finde sted under visse, nærmere angivne omstændigheder, benævnt "særlige omstændigheder", dvs. de situationer og betingelser, der kan betegnes som "undtagelser" i henhold til retshåndhævelsesdirektivets artikel 38.

86. Selv om Kommissionen bemærker, at ordningen for internationale overførsler af personoplysninger fra Det Forenede Kongerige fortsat ligger meget tæt på reglerne i kapitel V i direktiv (EU) 2016/680, fremgår det også af udkastet til afgørelse, at den retlige standard for bestemmelser til godkendelse af overførsler, som blev omtalt som bestemmelser om et tilstrækkeligt beskyttelsesniveau i det tidligere Section 74A i DPA 2018, og fornødne garantier er blevet omformuleret. I stedet for at henvise til et tilstrækkeligt beskyttelsesniveau kræver den nye "databeskyttelsestest" i Section 74AB i Data Protection Act 2028, at beskyttelsesstandarden for registrerede i modtagende tredjelande eller internationale organisationer "ikke er væsentligt lavere" end den standard, der gælder for registrerede i den relevante databeskyttelseslovgivning i Det Forenede Kongerige.

87. I denne forbindelse bemærker Databeskyttelsesrådet, at de elementer, som Secretary of State skal tage i betragtning ved vurderingen i henhold til Section 74AB, stk. 2, i DPA 2018, synes at være blevet reduceret i forhold til den tidligere vurdering af reglerne om et tilstrækkeligt beskyttelsesniveau.[70]

[68] Jf. Section 78, stk. 3 og 4, i Data (Use and Access) Act om ændring af Section 45 og 94 i DPA 2018.
[69] Det kan f.eks. hævdes, at dette er tilfældet for søgning efter beslaglagte enheder, som endnu ikke er blevet analyseret eller dekrypteret.
[70] Bestemmelsen i Section 74A, stk. 4, i DPA 2018, som blev udeladt ved DUAA, omfattede en liste over kriterier, der var identisk med artikel 36, stk. 3, i retshåndhævelsesdirektivet.

Databeskyttelsesrådet påpeger, at visse faktorer, som det mener spiller en vigtig rolle i vurderingen af, om et tredjeland tilbyder et i det væsentlige tilsvarende beskyttelsesniveau for personoplysninger, er blevet fjernet, og henviser til analysen og konklusionerne i punkt 42-43 i denne udtalelse. Databeskyttelsesrådet i) opfordrer navnlig Kommissionen til specifikt at behandle ændringerne og yderligere uddybe sin vurdering af den nye databeskyttelsestest. Databeskyttelsesrådet forstår, at de nye regler om overførsel af personoplysninger til tredjelande har til formål at give yderligere fleksibilitet. Databeskyttelsesrådet opfordrer samtidig Kommissionen til at overvåge den praktiske anvendelse af disse regler på området for retshåndhævelse og strafferetligt samarbejde. Dette er særlig relevant i forbindelse med Secretary of State's nye beføjelse til at fastlægge bestemmelser, der identificerer og godkender en overførsel på grundlag af den nye databeskyttelsestest, på enhver måde, herunder med henvisning til geografiske sektorer inden for et land, dataansvarlige eller databehandlere, modtagere af data, datatyper, overførselsmetoder og retlige instrumenter. Det er f.eks. stadig ikke klart, hvordan en bestemt dataansvarlig eller databehandler i et tredjeland, der ikke anses for at være tilstrækkeligt sikkert, vil kunne opfylde databeskyttelseskravene, når det gælder effektiv klageadgang eller registreredes rettigheder, der ikke allerede er fastlagt i det pågældende tredjelands lovgivning.

88. Databeskyttelsesrådet minder desuden om konklusionerne i punkt 41 vedrørende brugen af kriteriet om "ønskværdigheden af at lette overførsler af personoplysninger til og fra Det Forenede Kongerige" (Section 74AA, stk. 3, i Data Protection Act 2018) og opfordrer Kommissionen til i sin afgørelse at præcisere, at dette kriterium ikke er et element i databeskyttelsestesten, men blot en yderligere faktor, som Secretary of State kan overveje, når testens kriterier er fuldt ud opfyldt, da dette ikke fremgår helt klart af lovteksten. I denne henseende opfordrer Databeskyttelsesrådet Kommissionen til at overvåge de praktiske konsekvenser af Section 74AA, stk. 3, i Data Protection Act 2018, da det endnu er uklart, hvilken rolle "ønskværdigheden af at lette overførsler af personoplysninger til og fra Det Forenede Kongerige" vil spille i denne sammenhæng.

4.1.4.2. CLOUD ACT-AFTALEN MELLEM DET FORENEDE KONGERIGE OG USA

89. En anden relevant udvikling inden for videreoverførsel er ikrafttrædelsen i oktober 2022 af aftalen mellem Det Forenede Kongerige Storbritannien og Nordirlands regering og Amerikas Forenede Staters regering om adgang til elektroniske data med henblik på bekæmpelse af grov kriminalitet ("UK-U.S. Cloud Act Agreement"). Som Kommissionen korrekt påpeger, kan personoplysninger, der overføres fra EU til tjenesteudbydere i Det Forenede Kongerige, være genstand for påbud om fremlæggelse af bevismateriale udstedt af kompetente amerikanske retshåndhævende myndigheder i henhold til denne aftale.[71]

90. Da aftalen på tidspunktet for vedtagelsen af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige allerede var indgået, men endnu ikke trådt i kraft, understregede Kommissionen, at alle oplysninger og fremtidige præciseringer vedrørende den måde, hvorpå USA vil opfylde sine forpligtelser i henhold til aftalen, bør meddeles Kommissionen af Det Forenede Kongerige for at sikre en korrekt overvågning af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige i overensstemmelse med artikel 45, stk. 4, i GDPR. Kommissionen bemærkede, at der bør lægges særlig vægt på anvendelsen og tilpasningen af de garantier, der er fastsat i paraplyaftalen mellem EU og USA[72], til den specifikke type

[71] Jf. betragtning 87 i udkastet til afgørelse.
[72] Jf. aftalen mellem Amerikas Forenede Stater og Den Europæiske Union om beskyttelse af personoplysninger

overførsler, der er omfattet af Cloud Act-aftalen mellem Det Forenede Kongerige og USA.[73] Som opfølgning på denne erklæring henviser Kommissionen i sit udkast til afgørelse til flere præciseringer, der er opnået mellem Det Forenede Kongerige og USA i forbindelse med anvendelsen af paraplyaftalen mellem EU og USA på Cloud Act-aftalen mellem Det Forenede Kongerige og USA. Databeskyttelsesrådet glæder sig over disse præciseringer, som skaber yderligere juridisk klarhed. Samtidig er det værd at bemærke, at paraplyaftalen mellem EU og USA endnu ikke er blevet revideret, hvilket i et vist omfang begrænser de konklusioner, der kan drages med hensyn til virkningen og effektiviteten af dens anvendelse på Cloud Act-aftalen mellem Det Forenede Kongerige og USA.[74] Under hensyntagen til paraplyaftalen mellem EU og USA vil Databeskyttelsesrådet desuden gerne minde om behovet for at forbedre garantiniveauet i denne aftale. Dette gælder især adgangen til domstolsprøvelse. Registrerede i EU, som ikke er EU-borgere, har ikke et grundlag for domstolsprøvelse i henhold til Judicial Redress Act (lov om domstolsprøvelse). Derudover indeholder Privacy Act (lov om privatlivets fred) undtagelser, som ikke er blevet ændret ved Judicial Redress Act, og som begrænser enkeltpersoners mulighed for domstolsprøvelse i visse retshåndhævelses- og nationale sikkerhedssituationer. Kommissionen bemærker, at Judicial Redress Act ikke er den eneste mekanisme til at få adgang til domstolsprøvelse, men udkastet til afgørelse fastslår blot, at "afhængigt af omstændighederne og konteksten i den konkrete sag giver andre gældende amerikanske love alternative muligheder for adgang til domstolsprøvelse"[75]. Det er derfor uklart, om alle EU-borgere, hvis data kan være omfattet af Cloud Act-aftalen mellem Det Forenede Kongerige og USA, vil få adgang til domstolsprøvelse i USA.

91. Databeskyttelsesrådet bemærker også, at en specifik gensidig garanti i Cloud Act-aftalen mellem Det Forenede Kongerige og USA, hvorved begge parter begrænser den indvirkning, som aftalen kan have på henholdsvis personer fra Det Forenede Kongerige og USA, i sagens natur ikke finder anvendelse på enkeltpersoner i EU.[76] Databeskyttelsesrådet bemærker, at solide databeskyttelsesgarantier derfor er afgørende for at sikre, at de registreredes rettigheder i EU beskyttes tilstrækkeligt, hvis de behandles i henhold til denne aftale. Databeskyttelsesrådet opfordrer derfor Kommissionen til fortsat at inddrage Cloud Act-aftalen mellem Det Forenede Kongerige og USA i sine fremtidige vurderinger og revisioner af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.

92. Generelt mener Databeskyttelsesrådet, at der er behov for en præcisering af Kommissionens vurdering af Cloud Act-aftalen mellem Det Forenede Kongerige og USA og eventuelle virkninger af aftalen på beskyttelsesniveauet som vurderet i den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige. Resultaterne af den første revision af Cloud Act-aftalen mellem Det Forenede Kongerige og USA, som i henhold til aftalens artikel 12, stk. 1, skal gennemføres

---

i forbindelse med forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, EUT L 336 af 10.12.2016, s. 3-13, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01).

[73] Jf. betragtning 155 i gennemførelsesafgørelse 2021/1772. I henhold til artikel 9, stk. 1, i Cloud Act-aftalen mellem EU og USA finder paraplyaftalen mellem EU *og* USA tilsvarende anvendelse på Cloud Act-aftalen mellem Det Forenede Kongerige og USA. Den kan kun anvendes *analogt*, da paraplyaftalen regulerer grænseoverskridende overførsler mellem retshåndhævende myndigheder og ikke direkte samarbejde mellem en tjenesteudbyder og en retshåndhævende myndighed.

[74] Jf. artikel 23 i paraplyaftalen mellem EU og USA, der fastsætter, at parterne regelmæssigt skal foretage en fælles revision af de politikker og procedurer, der gennemfører aftalen, idet den første revision skal finde sted senest tre år efter aftalens ikrafttræden. Paraplyaftalen mellem EU og USA trådte i kraft i februar 2017.

[75] Jf. betragtning 93 i udkastet til afgørelse.

[76] Jf. aftalens artikel 4, stk. 3, og artikel 7, stk. 1, som indeholder bestemmelser om målrettede begrænsninger, der fastsætter, at ordrer, der er omfattet af aftalen, ikke bevidst må være rettet mod en "modtagende part-person". Derfor må USA ikke bevidst målrette en person, der befinder sig på Det Forenede Kongeriges område, og Det Forenede Kongerige skal overholde en tilsvarende begrænsning.

inden for et år efter aftalens ikrafttræden, kan være særligt informative for en sådan yderligere analyse.

4.1.5. TILSYN OG KLAGEADGANG

93. Databeskyttelsesrådet bemærker, at systemet for tilsyn med retshåndhævende myndigheder på det strafferetlige område i henhold til DPA 2018 og IPA 2016 samt de klagemekanismer, der er tilgængelige i henhold til Part 3 i DPA 2018, IPA 2016 og Human Rights Act 1998 (lov om menneskerettigheder), stort set forbliver uændrede. Tilsynet i Det Forenede Kongerige sikres navnlig fortsat, ud over ICO, af en kombination af forskellige Commissioners, nemlig Investigatory Powers Commissioner (kommissæren for efterforskningsbeføjelser, IPC), som bistås af andre Judicial Commissioners (retskommissærer) og en Biometrics and Surveillance Camera Commissioner (kommissær for biometri og overvågningskameraer).

94. Som Kommissionen har forklaret i betragtning 97 i udkastet til afgørelse, er der i Investigatory Powers Amendment Act 2024 kun foretaget begrænsede ændringer, navnlig gennem indførelse af stedfortrædende IPC'er, som IPC'er kan delegere specifikke beføjelser til, hvis de ikke kan eller ikke er tilgængelige til at varetage deres funktioner. Sådanne stedfortrædende IPC'er skal være Judicial Commissioners og udpeges af IPC.

95. Databeskyttelsesrådet noterer sig med tilfredshed, at de tidligere idéer i Data Protection and Digital Information Bill, som gik forud for DUUA, om at afskaffe Biometrics and Surveillance Camera Commissioner og overføre rollen til Investigatory Powers Commissioner, er blevet henlagt[77]. I den forbindelse opfordrer Databeskyttelsesrådet Kommissionen til at lægge større vægt på og give en mere detaljeret vurdering af den rolle, som Biometrics and Surveillance Camera Commissioner spiller i tilsynssystemet i forbindelse med sin overvågning og fremtidige revisioner af udkastet til afgørelse.

96. Som Databeskyttelsesrådet allerede understregede i udtalelse nr. 14/2021, spiller eksistensen af effektive sanktioner en vigtig rolle med hensyn til at sikre overholdelse af reglerne, selv om ICO er godt udstyret med de nødvendige beføjelser, som svarer nøje til EU-medlemsstaternes tilsynsmyndigheders beføjelser som anført i artikel 58 i GDPR[78].

97. Databeskyttelsesrådet noterer sig med tilfredshed ICO's gennemsigtighedspolitik og tilgængeligheden af statistiske og analytiske data, herunder eksempler på ICO's håndhævelsesaktiviteter i forhold til retshåndhævende organer[79]. I den forbindelse bemærker Databeskyttelsesrådet, at den britiske tilsynsmyndighed foretrækker irettesættelser i tilfælde af politistyrkers overtrædelse af databeskyttelseslovgivningen. En væsentlig undtagelse er det pålæg om overholdelse (Enforcement Notice), der blev udstedt til Crown Prosecution Service (en uafhængig retsforfølgningstjeneste) i januar 2024[80]. Databeskyttelsesrådet finder det også positivt, at ICO har offentliggjort en lang række adfærdskodekser, retningslinjer, udtalelser og andre vejledende dokumenter til de relevante parter.

98. I lyset af ovenstående og især i betragtning af de forestående væsentlige ændringer i den britiske tilsynsmyndigheds struktur og organisation, som allerede er analyseret i punkt 68 i denne udtalelse,

[77] Jf. https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner.
[78] Jf. Databeskyttelsesrådets udtalelse nr. 14/2021, punkt 112.
[79] Jf. f.eks. de detaljerede datasæt for databeskyttelsesklager på https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-protection-complaints/.
[80] Jf. https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/.

opfordrer Databeskyttelsesrådet Europa-Kommissionen til fortsat at overvåge effektiviteten af sanktioner og relevante retsmidler i den britiske databeskyttelsesramme.

4.2. DE BRITISKE OFFENTLIGE MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER TIL NATIONALE SIKKERHEDSFORMÅL.

99. Udkastet til afgørelse indeholder kun begrænsede oplysninger om de britiske offentlige myndigheders adgang til og brug af personoplysninger til nationale sikkerhedsformål. Kommissionen forklarer, at DUAA kun medførte mindre ændringer af rammerne for de britiske efterretningstjenesters databehandling[81], hvoraf nogle også er blevet indført i retshåndhævelsesrammen i Data Protection Act 2018. Disse ændringer er kort nævnt i betragtning 75 i udkastet til afgørelse. Desuden er de ændringer, der er foretaget i IPA 2016 siden vedtagelsen af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige, allerede behandlet i afsnit 3.2 i udkastet til afgørelse, hvor de vedrører både databehandling med henblik på retshåndhævelse og national sikkerhed.[82] Derfor gælder de anmodninger om præcisering og overvågning, der er beskrevet i afsnit 4.1.1.1 og 4.1.3 ovenfor, ligeledes for adgang til og brug af personoplysninger med henblik på den nationale sikkerhed.

4.2.1. BRUG AF TECHNICAL CAPABILITY NOTICES

100. Tidligere i år blev det i medierne afsløret, at den britiske regering angiveligt havde udstedt et påbud om teknisk kapacitet (Technical Capability Notice) i henhold til Section 253 i IPA 2016 til en stor teknologivirksomhed, der krævede, at udbyderen skulle have adgang til sine brugeres krypterede data i dekrypteret form.[83] I praksis ville dette angiveligt betyde at omgå den end-to-end-kryptering, som udbyderen tilbyder i sin cloudlagringsløsning. Denne tilgang er derfor blevet kaldt et "bagdørskrav".

101. Selv om retsgrundlaget for påbud om teknisk kapacitet allerede eksisterede på tidspunktet for vedtagelsen af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige, synes denne omtalte sag at markere det første kendte tilfælde af en sådan brug. Den udgør som sådan en væsentlig udvikling, der bør behandles nærmere, navnlig i lyset af GDPR's artikel 45, stk. 2, litra a), som kræver en vurdering ikke blot af den retlige ramme på papir, men også af dens gennemførelse.[84] Databeskyttelsesrådet ville derfor have forventet, at udkastet til afgørelse behandlede dette spørgsmål udtrykkeligt, og opfordrer Kommissionen til at supplere afgørelsen med det.

102. Offentligheden har ikke kendskab til alle oplysningerne i denne sag på grund af den fortrolige karakter af påbud om teknisk kapacitet, men det fremgår af den offentliggjorte anmodning om en privat mundtlig høring på Investigatory Powers Tribunals websted og af det offentligt tilgængelige uddrag af den private dom vedrørende denne høring, at der ikke er tale om mediespekulation.[85] Spørgsmålet

[81] Jf. betragtning 75 i udkastet til afgørelse.
[82] Jf. betragtning 98 i udkastet til afgørelse. De pågældende efterforskningsbeføjelser kan ikke kun udøves af nationale efterretningstjenester, men også af visse retshåndhævende myndigheder.
[83] Jf. "U.K. orders Apple to let it spy on users' encrypted accounts" (Washington Post, 7. februar 2025), https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/.
[84] Desuden præciseres det i GDPR's artikel 45, stk. 3, at Kommissionen skal tage hensyn til alle relevante udviklinger i tredjelandet, når den regelmæssigt reviderer sine konklusioner om tilstrækkeligheden af beskyttelsesniveauet.
[85] Jf. https://www.judiciary.uk/judgments/apple-inc-v-secretary-of-state-for-the-home-department/.

bør nævnes, og den påståede brug af Section 253 i IPA 2016 til at udstede et "bagdørskrav" bør fremhæves med henblik på fremtidig overvågning.

103. Som det for nylig blev påpeget i erklæring 5/2024, mener Databeskyttelsesrådet, at kryptering er af afgørende betydning for at garantere sikkerheden og fortroligheden af personoplysninger og elektronisk kommunikation. Især er ægte end-to-end-kryptering, der dækker terminaludstyret og de indeholdte data, og hvor dekrypteringsnøglerne udelukkende opbevares af brugeren, et vigtigt redskab til at sikre fortroligheden af elektronisk kommunikation.[86] Udstedelsen af påbud om teknisk kapacitet, der tvinger virksomheder til at kunne fjerne kryptering på regeringens anmodning, skaber systemiske sårbarheder og udgør en direkte trussel mod integriteten og fortroligheden af elektronisk kommunikation. I denne forbindelse gør Databeskyttelsesrådet opmærksom på sagen PODCHASOV mod RUSSIA, hvor Menneskerettighedsdomstolen fandt, at en "forpligtelse til at dekryptere end-to-end-krypteret kommunikation risikerer at blive et krav om, at udbydere af disse tjenester svækker krypteringsmekanismen for alle brugere, og at det derfor ikke står i rimeligt forhold til de legitime mål, der forfølges".[87]

104. Det antages, at den britiske regering primært vil søge at få adgang til ukrypterede brugerdata, hvis der er en risiko for den nationale sikkerhed, men Databeskyttelsesrådet finder, at anmodningen om en vurdering af brugen af påbud om teknisk kapacitet, som drøftet ovenfor, er lige så relevant i forbindelse med regeringens adgang til retshåndhævelsesformål.

4.2.2. RETSGRUNDLAG OG GÆLDENDE GARANTIER

105. Med Investigatory Powers Amendment Act 2024 blev der indført en særlig ordning for opbevaring og undersøgelse af store persondatasæt, for hvilke de personer, som personoplysningerne vedrører, "ikke kunne have nogen eller kun en lav rimelig forventning om privatlivets fred", som det formuleres i loven.[88] Med henblik på opbevaring og undersøgelse af sådanne specifikke undergrupper af store persondatasæt giver IPA 2016 nu mulighed for "individuelle tilladelser" og "kategoritilladelser". [89]

106. Begrebet store persondatasæt er bredt og kan omfatte mange forskellige datasæt.[90] Den kan finde anvendelse på følsomme oplysninger, men kan også omfatte offentligt og kommercielt tilgængelige data. På denne baggrund fandt den britiske regering det nødvendigt at revidere den tidligere ordning, hvor der blev anvendt samme garantier for alle store persondatasæt, og i stedet indføre forskellige garantier for opbevaring og undersøgelse af store persondatasæt afhængigt af indholdets følsomhed eller offentlige tilgængelighed eller graden af indgreb i forbindelse med efterretningstjenesternes opbevaring og undersøgelse af disse.[91] Efter Databeskyttelsesrådets opfattelse førte disse overvejelser

[86] Jf. erklæring 5/2024 om henstillingerne fra Gruppen på Højt Plan om Adgang til Data med henblik på Effektiv Retshåndhævelse, vedtaget den 4. november 2024, s. 4.
[87] Jf. Menneskerettighedsdomstolens dom af 13. februar 2024, 33696/19, præmis 79.
[88] Jf. Section 226A, stk. 1, i IPA 2016.
[89] Jf. Section 226A og 226BA i IPA 2016, som indført ved Section 2 i Investigatory Powers Amendment Act 2024.
[90] I Section 199 i IPA 2016 præciseres det, at en "efterretningstjeneste opbevarer store persondatasæt, hvis a) efterretningstjenesten indhenter et sæt oplysninger, der omfatter personoplysninger vedrørende en række personer, b) sættet er af en sådan art, at størstedelen af de pågældende personer ikke er eller sandsynligvis ikke vil være af interesse for efterretningstjenesten i forbindelse med udøvelsen af dens funktioner, c) efterretningstjenesten efter en forundersøgelse af indholdet opbevarer sættet med henblik på udøvelsen af sine funktioner, og d) sættet opbevares eller skal opbevares elektronisk med henblik på analyse i forbindelse med udøvelsen af disse funktioner".
[91] Jf. Home Office, Policy paper Investigatory Powers (Amendment) Bill: Bulk Personal Datasets and Third Party Bulk Personal Datasets, https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-bulk-personal-datasets-and-third-party-bulk-personal-datasets.

i sidste ende til, at der blev oprettet en særskilt ordning for store persondatasæt, for hvilke der kun er en lav eller ingen rimelig forventning om privatlivets fred.

107. Kommissionen diskuterer kort det nye begreb "kategoritilladelse" og anfører i udkastet til afgørelse, at "det med hensyn til opbevaring og undersøgelse af store persondatasæt er vigtigt, at den ordning, der er vurderet i betragtning 239 og 240 i gennemførelsesafgørelse (EU) 2021/1772, fortsat er gældende, navnlig behovet for en kendelse, der først godkendes af Secretary of State, og derefter af den pågældende Judicial Commissioner, med forbehold af kravene om foranstaltningens nødvendighed og proportionalitet, jf. Part 7 i IPA 2016"[92]. Analysen synes dog at være ufuldstændig. Databeskyttelsesrådet bemærker, at ikke blot indførelsen af "kategoritilladelser", men også af "individuelle tilladelser" udgør en relevant ændring, der følger af Investigatory Powers Amendment Act 2024 for ovennævnte specifikke datasæt: en "individuel tilladelse", som kan udstedes af chefen for en efterretningstjeneste eller en person, der handler på dennes vegne, erstatter nødvendigheden af en dommerkendelse for at opbevare, eller opbevare og undersøge store persondatasæt, for hvilke der kun er en lav eller ingen rimelig forventning om privatlivets fred.[93] Begreberne "kendelse" og "individuel tilladelse" bør derfor ikke forveksles og kan ikke bruges synonymt.[94] Dette gælder især, fordi den retslige godkendelse, der kræves for individuelle tilladelser, er begrænset til spørgsmålet om, hvorvidt det specifikke datasæt opfylder kriterierne for at blive klassificeret som ét med kun en lav eller ingen rimelig forventning om privatlivets fred, jf. Section 226A i IPA 2016.[95] En "kategoritilladelse" adskiller sig fra en "individuel tilladelse" og fraviger – jf. Section 226B, stk. 6, litra a,) i IPA 2016 – kravet om en sådan retslig godkendelse af en individuel tilladelse, når denne tilladelse vedrører et datasæt, der falder ind under en kategoritilladelse. Det skyldes, at der allerede er truffet en afgørelse, som er godkendt af en Judicial Commissioner om, at datasæt, der er omfattet af beskrivelsen i kategoritilladelsen, er et datasæt, som Section 226A ville finde anvendelse på.

108. Disse ændringer vedrører opbevaring og undersøgelse af store persondatasæt og ikke den oprindelige overvågning eller indsamling af dem, men Databeskyttelsesrådet vil dog gerne understrege den betydning, som Menneskerettighedsdomstolen tillægger forudgående uafhængig godkendelse i forbindelse med behandling af store persondatasæt. Domstolen fastslog, at "for at minimere risikoen for misbrug af beføjelsen til masseovervågning [...] skal processen være underlagt "end-to-end-garantier", hvilket betyder, at der på nationalt plan skal foretages en vurdering i hver fase af processen af nødvendigheden og proportionaliteten af de foranstaltninger, der træffes; at masseovervågning skal være underlagt uafhængig godkendelse fra starten, når formålet med og omfanget af operationen fastlægges; og at operationen skal være underlagt tilsyn og uafhængig efterfølgende kontrol."[96] Med dette in mente og på grundlag af en holistisk tilgang, hvor alle omstændighederne i sagen tages i betragtning ved vurderingen af tilstrækkeligheden, mener Databeskyttelsesrådet, at opbevaring og undersøgelse af store persondatasæt som minimum bør være underlagt enten en forudgående godkendelse fra en uafhængig myndighed eller en systematisk uafhængig efterfølgende kontrol foretaget af en domstol eller et tilsvarende organ, dvs. et uafhængigt organ, der kan træffe bindende afgørelser.

[92] Jf. betragtning 99 i udkastet til afgørelse.
[93] Section 200, stk. 1 og 2, i IPA 2016.
[94] Dette synes imidlertid at være tilfældet i betragtning 99 og 100 i udkastet til afgørelse.
[95] I Section 226BB, stk. 1, i IPA 2016 fastsættes det, at en Judicial Commissioner, når han skal afgøre, om en beslutning om at give en individuel tilladelse eller en kategoritilladelse skal godkendes, skal gennemgå konklusionerne fra den person, der har udstedt tilladelsen, for at kontrollere, om Section 226A finder anvendelse på de store persondatasæt, der er beskrevet i tilladelsen, eller om Section 226A finder anvendelse på alle datasæt, der falder ind under den datasætkategori, der er beskrevet i tilladelsen.
[96] ECHR, Big Brother Watch m.fl. mod Det Forenede Kongerige, 25. maj 2021, præmis 350.

109. I betragtning af de resterende behov for præciseringer opfordrer Databeskyttelsesrådet indtrængende Kommissionen til yderligere at undersøge begreberne "individuelle tilladelser" og "kategoritilladelser" i henhold til Investigatory Powers Amendment Act 2024. Databeskyttelsesrådet opfordrer desuden Kommissionen til nøje at overvåge gennemførelsen af udtrykket "lav eller ingen rimelig forventning om privatlivets fred" i praksis. Selvom Section 226A i IPA 2016 fastsætter en række kriterier for denne konstatering, finder Databeskyttelsesrådet det vigtigt at overvåge anvendelsen af dem, da de potentielt kan fortolkes bredt.[97]

4.2.3. TILSYN OG KLAGEADGANG

110. Som angivet i udkastet til afgørelse og tidligere analyseret i udtalelse nr. 14/2021 spiller Investigatory Powers Commissioner (IPC) og hans kontor (IPCO) en central rolle i tilsynet med de britiske efterretningstjenesters brug af efterforskningsbeføjelser. Endvidere er Investigatory Powers Tribunal (IPT) den retsinstans, der har kompetence til at give oprejsning i denne henseende. Som allerede nævnt i afsnit 3.1.5. om tilsynet på retshåndhævelsesområdet har Investigatory Powers Amendment Act 2024 kun medført begrænsede ændringer, navnlig gennem indførelsen af stedfortrædende IPC'er. Databeskyttelsesrådets bemærkninger i sin udtalelse nr. 14/2021 er derfor fortsat fuldt ud gyldige[98].

111. Databeskyttelsesrådet glæder sig over IPCO's gennemsigtige årlige rapportering, herunder tilgængeligheden af detaljerede statistikker for perioden 2019-2023, herunder om de britiske efterretningstjenesters anvendelse af massebeføjelser og om målretningsafgørelser og målrettede tilladelser med henblik på at indhente data i henhold til dataadgangsaftalen mellem Det Forenede Kongerige og USA. Databeskyttelsesrådet noterer sig også specifikt IPCO's tilsyn med Government Communications Headquarters' (regeringens hovedkvarter for kommunikation, GCHQ) masseovervågning af data, som Kommissionen har fremhævet i betragtning 102 i udkastet til afgørelse. I den forbindelse opfordrer Databeskyttelsesrådet Kommissionen til fortsat nøje at overvåge effektiviteten af tilsynssystemet på dette område, navnlig med hensyn til proportionaliteten af anmodningerne om masseovervågning[99].

112. Databeskyttelsesrådet bemærker desuden, at Investigatory Powers Tribunal også har offentliggjort en beretning om sine aktiviteter og retspraksis for perioden 2021-2023[100]. Rapporten fremhæver blandt andet vigtige og relevante udviklinger, såsom dommen fra Den Europæiske Menneskerettighedsdomstol i sagen *Wieder og Guarnieri mod Det Forenede Kongerige*, hvor det blev fastslået, at personer hvor som helst i verden kan indgive en klage til IPT, hvis handlingen er begået af en britisk offentlig myndighed og har fundet sted i Det Forenede Kongerige. Databeskyttelsesrådet opfordrer derfor Kommissionen til også at medtage IPT's aktiviteter i sin vurdering og i de fremtidige revisioner af udkastet til afgørelse.

---

[97] Section 226A i IPA 2016 henviser f.eks. til dataenes art, i hvilket omfang dataene er blevet offentliggjort, eller i hvilket omfang dataene er almindeligt kendt.

[98] Jf. udtalelse nr. 14/2021, punkt 200-215.

[99] For yderligere oplysninger henvises til Investigatory Powers Commissioner's årsberetning for 2023 på følgende link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf side 31, punkt 6.41.

[100] https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf

5. REVISION, VARIGHED OG FORLÆNGELSE AF UDKASTET TIL AFGØRELSE

113. Databeskyttelsesrådet bemærker, at den endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet gælder i seks år, dvs. indtil den 27. december 2031. Det ville således fortsat være det eneste tredjeland, hvis afgørelsen om tilstrækkeligheden af beskyttelsesniveauet har en udløbsklausul, som kombineres med den obligatoriske regelmæssige revision, der er fastsat i artikel 45, stk. 3, i GDPR. Databeskyttelsesrådet forstår, at den nye britiske retlige ramme vil kræve særlig opmærksomhed, og opfordrer Kommissionen til nøje at overvåge gennemførelsen af DUAA, herunder de fokusområder, der fremhæves i denne udtalelse, samt alle andre relevante udviklinger i Det Forenede Kongerige i denne henseende.

114. Databeskyttelsesrådet glæder sig over, at betragtning 68 i udkastet til afgørelse henviser til Databeskyttelsesrådets (og civilsamfundsgruppers) rolle i den regelmæssige revision i overensstemmelse med Databeskyttelsesrådets henstilling 1/2021[101]. Med hensyn til den praktiske inddragelse af Databeskyttelsesrådet og dets repræsentanter i forberedelsen og gennemførelsen af de fremtidige revisioner gentager Databeskyttelsesrådet, at al relevant dokumentation bør deles skriftligt med Databeskyttelsesrådet i tilstrækkelig god tid inden revisionerne.

115. I forbindelse med betragtning 113 forstår Databeskyttelsesrådet ud fra Kommissionen yderligere forklaringer, at hensigten er at foretage en revision ved udgangen af de fire år, og at Kommissionen udarbejder en offentlig rapport på dette grundlag[102]. Denne revision vil hjælpe Kommissionen med at vide, om den senest seks måneder før udløbet af udkastet til afgørelse skal indlede proceduren for forlængelse af gyldighedsperioden for udkastet til afgørelse[103].

116. Databeskyttelsesrådet glæder sig over denne hensigt og bemærker, at revisionen tjener et andet formål end udløbsklausulen og spiller en vigtig rolle i overvågningen af de retlige rammer. Databeskyttelsesrådet forventer derfor, at revisionen finder sted om fire år, og opfordrer Kommissionen til at gå videre med det til den tid.

117. Det er Databeskyttelsesrådets opfattelse, at denne fremtidige revision vil tage hensyn til de elementer, der er beskrevet i Kommissionens gennemførelsesafgørelse 2021/1772, og at betragtningerne vedrørende suspension og ophævelse af afgørelsen stadig er gyldige[104]. Af hensyn til retssikkerheden mener Databeskyttelsesrådet, at denne præcisering kunne fremgå af den endelige afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

På Det Europæiske Databeskyttelsesråds vegne

Formanden

(Anu Talus)

[101] Jf. betragtning 19 i Databeskyttelsesrådets henstilling nr. 1/2021.
[102] Jf. betragtning 110 i udkastet til afgørelse.
[103] Jf. betragtning 113 i udkastet til afgørelse.
[104] Jf. betragtning 168-171 i Kommissionens gennemførelsesafgørelse 2021/1173.