Udtalelse nr. 14/2021 vedrørende 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.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

INDHOLDSFORTEGNELSE

Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") har —

under henvisning til artikel 70, stk. 1, litra s), i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter "databeskyttelsesforordningen" eller "GDPR"),

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde (herefter "EØS-aftalen"), særlig bilag XI og protokol 37 som ændret ved afgørelse nr. 154/2018 truffet af Det Blandede EØS-Udvalg den 6. juli 2018[1], og

under henvisning til artikel 12 og 22 i Databeskyttelsesrådets forretningsorden —

VEDTAGET FØLGENDE UDTALELSE:

1. RESUMÉ

1. Europa-Kommissionen godkendte den 19. februar 2021 sit udkast til gennemførelsesafgørelse (herefter "afgørelsesudkastet") om tilstrækkelig beskyttelse af personoplysninger i Det Forenede Kongerige i henhold til databeskyttelsesforordningen[2]. Herefter iværksatte Europa-Kommissionen proceduren for den formelle vedtagelse heraf.

2. Samme dag udbad Europa-Kommissionen sig en udtalelse fra Databeskyttelsesrådet[3]. Databeskyttelsesrådets vurdering af tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige er foretaget på grundlag af en undersøgelse af selve afgørelsesudkastet og på en analyse af den dokumentation, som Europa-Kommissionen har haft til rådighed.

3. Databeskyttelsesrådet koncentrerede sig om vurderingen af både de generelle GDPR-aspekter af afgørelsesudkastet og om de offentlige myndigheders adgang til personoplysninger, der overføres fra EØS med henblik på retshåndhævelse og statens sikkerhed, herunder de retsmidler, der er til rådighed for borgere i EØS. Databeskyttelsesrådet foretog også en bedømmelse af, om de garantier, som gives i henhold til de retlige rammer i Det Forenede Kongerige, er indført og effektive.

4. Databeskyttelsesrådet har benyttet sit arbejdsdokument om en reference vedrørende tilstrækkelighed[4], som det vedtog i februar 2018, og sine anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger[5], som primær referenceramme til dette arbejde.

[1] Henvisninger til "medlemsstater" i denne udtalelse skal forstås som henvisninger til "EØS-medlemsstater".
[2] Se Europa-Kommissionens pressemeddelelse, Databeskyttelse: Europa-Kommissionen indleder en proces vedrørende udveksling af personoplysninger med Det Forenede Kongerige, 19. februar 2021, https://ec.europa.eu/commission/presscorner/detail/da/ip_21_661.
[3] Ibidem.
[4] Se Artikel 29-Gruppen, Reference vedrørende et tilstrækkeligt beskyttelsesniveau, vedtaget den 28. november 2017, som senest revideret og vedtaget den 6. februar 2018, WP254 rev.01 (godkendt af Databeskyttelsesrådet, se https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines), (herefter "*tilstrækkelighedsreferencen*").
[5] Se Databeskyttelsesrådets anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, vedtaget den 10. november 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_da.

1.1. Konvergensområder

5. Databeskyttelsesrådets primære mål er at afgive en udtalelse til Europa-Kommissionen om tilstrækkeligheden af beskyttelsesniveauet for personer i Det Forenede Kongerige. Det er vigtigt at anerkende, at Databeskyttelsesrådet ikke forventer, at de britiske retlige rammer er en nøjagtig gengivelse af den europæiske databeskyttelseslovgivning.

6. Databeskyttelsesrådet minder imidlertid om, at ifølge artikel 45 i GDPR og retspraksis fra Den Europæiske Unions Domstol (herefter "Domstolen") skal tredjelandets lovgivning bringes i overensstemmelse med kernen i de grundlæggende principper, der er fastlagt i databeskyttelsesforordningen, for at kunne anses for at yde et tilstrækkeligt beskyttelsesniveau. Den britiske databeskyttelsesramme er hovedsagelig baseret på EU's databeskyttelsesramme (navnlig databeskyttelsesforordningen og Europa-Parlamentets og Rådets direktiv (EU) 2016/680 (herefter "retshåndhævelsesdirektivet")), hvilket skyldes, at Det Forenede Kongerige var medlem af EU indtil den 31. januar 2020. Den britiske databeskyttelseslov, Data Protection Act 2018, som trådte i kraft den 23. maj 2018 og samtidig ophævede Data Protection Act 1998, specificerer desuden anvendelsen af databeskyttelsesforordningen efter britisk lov og gennemfører retshåndhævelsesdirektivet samt delegerer beføjelser og forpligtelser til den nationale tilsynsmyndighed for databeskyttelse den britiske informationskommissærs kontor ("UK Information Commissioner's Office" — herefter ICO"). Derfor anerkender Databeskyttelsesrådet, at Det Forenede Kongerige i store træk har ladet sin databeskyttelsesramme afspejle databeskyttelsesforordningen.

7. **Når Databeskyttelsesrådet analyserer lovgivning og praksis i et tredjeland, som var medlem af EU indtil for nylig, er det klart, at det finder mange aspekter, der i det væsentlige svarer til EU's databeskyttelsesramme.**

8. Inden for databeskyttelse bemærker Databeskyttelsesrådet, at der er stærk overensstemmelse mellem databeskyttelsesforordningens ramme og den britiske retlige ramme i visse centrale bestemmelser, f.eks. med hensyn til begreber (f.eks. "personoplysninger", "behandling af personoplysninger" og "dataansvarlig"), grundlag for lovlig og rimelig behandling til legitime formål, formålsbegrænsning, datakvalitet og dataproportionalitet, dataopbevaring, sikkerhed og fortrolighed, gennemsigtighed, særlige kategorier af oplysninger, direkte markedsføring og automatiske afgørelser og profilering.

1.2. Udfordringer

9. Det Forenede Kongerige var indtil for nylig medlem af EU. Databeskyttelsesrådet har derfor ved analysen af britisk lov og praksis fundet mange aspekter, der i det væsentlige svarer til EU-niveauet. Samtidig har Databeskyttelsesrådet, både på grund af sin rolle i vedtagelsen af en konstatering af et tilstrækkeligt beskyttelsesniveau og på grund af tidsfaktoren, besluttet at rette opmærksomheden mod de aspekter, som ser ud til at trænge til et nøjere eftersyn.

10. Ikke desto mindre er der stadig udfordringer, og Databeskyttelsesrådet mener, at nedenstående punkter skal vurderes yderligere for at sikre, at beskyttelsesniveauet i Det Forenede Kongerige kan anses for i det væsentlige at svare til EU-niveauet, og at de bør overvåges nøje af Europa-Kommissionen.

1.2.1. Generelt

11. Den første udfordring, der har generel karakter, vedrører overvågningen af, hvordan det britiske retlige databeskyttelsessystem udvikler sig. Den britiske regering har nemlig oplyst, at det er dens

hensigt at udforme separate og uafhængige databeskyttelsespolitikker og eventuelt afvige fra EU's databeskyttelseslovgivning. Sådanne politiske erklæringer er endnu ikke kommet til udtryk i de britiske retlige rammer. Imidlertid kan denne potentielle **afvigelse vise sig at være en trussel mod opretholdelsen af beskyttelsesniveauet for personoplysninger, der overføres fra EU**. **Europa-Kommissionen opfordres derfor til at følge denne form for udvikling nøje fra ikrafttrædelsen af tilstrækkelighedsafgørelsen og træffe de nødvendige foranstaltninger, herunder ved at ændre og/eller suspendere afgørelsen om nødvendigt.**

1.2.2. Generelle databeskyttelsesaspekter

12. For det første er den såkaldte "**immigration exemption**" (immigrationsundtagelse), som er fastlagt i **Data Protection Act 2018, Schedule 2, del 1**, afsnit 4, "**bredt" formuleret**. Den gælder bl.a., hvis en dataansvarlig ikke indhenter personoplysninger med henblik på immigrationskontrol, men stiller dem til rådighed for en anden dataansvarlig, som behandler disse personoplysninger med henblik på immigrationskontrol.

13. Databeskyttelsesrådet opfordrer Europa-Kommissionen til at indhente en status over retssagen *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* og at få verificeret, eftersom denne afgørelse ikke er endelig (retskraftig), om den bliver stadfæstet eller ændret ved appelafgørelsen, idet den tager eventuelt nyt om denne sag i betragtning og gør rede for det i sin afgørelse. **Databeskyttelsesrådet opfordrer også Europa-Kommissionen til i tilstrækkelighedsafgørelsen at oplyse yderligere om immigrationsundtagelsen[6], især vedrørende nødvendigheden og proportionaliteten af en så bred undtagelse i britisk lov, navnlig for så vidt angår det brede personelle anvendelsesområde.** Samtidig opfordrer Databeskyttelsesrådet Europa-Kommissionen til at undersøge yderligere, om der findes eller påtænkes supplerende garantier i den britiske retlige ramme, f.eks. i form af retligt bindende instrumenter, som kan supplere immigrationsundtagelsen ved at øge dens forudsigelighed og styrke garantierne for de registrerede og samtidig sikre en bedre og hurtig vurdering og overvågning af kravene om nødvendighed og proportionalitet.

14. For det andet anerkender Databeskyttelsesrådet ganske vist, at Det Forenede Kongerige har gengivet størstedelen af kapitel V i databeskyttelsesforordningen i sin egen databeskyttelsesramme, men Databeskyttelsesrådet har fundet visse aspekter af den britiske retlige ramme **med hensyn til videreoverførsel**, som kan underminere beskyttelsesniveauet ved overførsel af personoplysninger fra EØS.

15. Artikel 44 i GDPR[7] bestemmer nemlig, at overførsel og videreoverførsel af personoplysninger kun må finde sted, hvis det beskyttelsesniveau, som fysiske personer garanteres i medfør af GDPR, ikke

[6] Også som resultat af den løbende gennemgang af anvendelsen af immigrationsundtagelsen, som der henvises til på s. 5 i den britiske regerings "Explanatory Framework for Adequacy Discussions, Section E3: Schedule 2 Restrictions, 13 March 2020", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] "*Enhver overførsel af personoplysninger, som underkastes behandling eller planlægges behandlet efter overførsel til et tredjeland eller en international organisation, må kun finde sted, hvis betingelserne i dette kapitel med forbehold af de øvrige bestemmelser i denne forordning opfyldes af den dataansvarlige og databehandleren, herunder ved videreoverførsel af personoplysninger fra det pågældende tredjeland eller den pågældende internationale organisation til et andet tredjeland eller en anden international organisation. Alle bestemmelserne i dette kapitel anvendes for at sikre, at det beskyttelsesniveau, som fysiske personer garanteres i medfør af denne forordning, ikke undermineres.*"

undermineres. **Dette betyder ikke blot, at den britiske lovgivning "i det væsentlige skal svare til" EU-lovgivningen med hensyn til behandling af personoplysninger, der overføres til Det Forenede Kongerige i henhold til den kommende tilstrækkelighedsafgørelse, men også at de gældende regler i Det Forenede Kongerige med hensyn til videreoverførsel af disse personoplysninger til tredjelande skal sikre, at der fortsat ydes et beskyttelsesniveau, der i det væsentlige svarer til EU-niveauet.**

16. Selv om Databeskyttelsesrådet noterer sig, at Det Forenede Kongerige i henhold til sin retlige ramme kan anerkende bestemte områders tilstrækkelige databeskyttelsesniveau i lyset af den britiske retlige ramme, ønsker Databeskyttelsesrådet at fremhæve, at disse områder måske endnu ikke er omfattet af en tilstrækkelighedsafgørelse udstedt af Europa-Kommissionen og ikke sikrer et beskyttelsesniveau, der "i det væsentlige svarer til" det niveau, der garanteres i EØS. Det kan medføre potentielle risici i beskyttelsen af personoplysninger, der overføres fra især EØS, hvis den britiske databeskyttelsesramme fremover afviger fra EU's regelværk. Desuden har Det Forenede Kongerige allerede anerkendt tilstrækkeligheden i de tredjelande, som er omfattet af en tilstrækkelighedskonstatering udstedt af Europa-Kommissionen i henhold til direktiv 95/46/EF[8], mens Europa-Kommissionen snart reviderer disse konstateringer, hvis konklusioner dermed endnu ikke kendes.

17. **I henseende til ovennævnte situationer bør Europa-Kommissionen varetage sin tilsynsrolle, og hvis det beskyttelsesniveau ved overførsel af personoplysninger fra EØS, der i det væsentlige svarer til EU-niveauet, ikke opretholdes, bør Europa-Kommissionen overveje at ændre tilstrækkelighedsafgørelsen for at indføre specifikke garantier for personoplysninger, der overføres fra EØS, og/eller suspendere tilstrækkelighedsafgørelsen.**

18. **Vedrørende internationale aftaler mellem Det Forenede Kongerige og tredjelande** opfordres Europa-Kommissionen til for det første at undersøge samspillet mellem den britiske databeskyttelsesramme og landets internationale forpligtelser ud over aftalen om adgang til elektroniske oplysninger med henblik på bekæmpelse af grov kriminalitet indgået mellem Det Forenede Kongerige og USA[9] (herefter "CLOUD Act-aftalen mellem Det Forenede Kongerige og USA"), navnlig for at sikre kontinuiteten i beskyttelsesniveauet, når personoplysninger overføres fra EU til Det Forenede Kongerige på grundlag af tilstrækkelighedsafgørelsen om Det Forenede Kongerige og derefter videreoverføres til andre tredjelande, og for det andet at fortsætte sit tilsyn og om nødvendigt at skride ind, hvis indgåelsen af internationale aftaler mellem Det Forenede Kongerige og tredjelande risikerer at underminere det niveau for beskyttelse af personoplysninger, der er sikret i EU.

19. Desuden opfordres Europa-Kommissionen til at overvåge, om CLOUD Act-aftalen mellem Det Forenede Kongerige og USA sikrer passende supplerende garantier under hensyntagen til følsomhedsniveauet for de berørte datakategorier og de unikke krav til serviceudbydernes, frem for myndighedernes, direkte overførsel af elektronisk bevismateriale, idet den også vurderer de

[8] Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).

[9] Se aftalen mellem Det Forenede Kongerige Storbritannien og Nordirland og Amerikas Forenede Stater om adgang til elektroniske data med henblik på bekæmpelse af grov kriminalitet, Washington DC, USA, 3. oktober 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

omstændigheder, hvorunder der kan gives garantier i kraft af en hensigtsmæssig gennemførelse af tilpasningen af paraplyaftalen mellem EU og USA[10].

20. Endvidere bemærker Databeskyttelsesrådet, at videreoverførsel også kan ske fra Det Forenede Kongerige til et andet tredjeland baseret på **dataoverførselsværktøjer efter den gældende britiske databeskyttelseslovgivning**[11]. Efter Schrems II-dommen[12] opfordrer Databeskyttelsesrådet Europa-Kommissionen til i tilstrækkelighedsafgørelsen at give forsikringer om, at de nødvendige garantier bliver indført effektivt, også under hensyntagen til lovgivningen i det modtagende tredjeland.

21. Med hensyn til fraværet i den britiske lovgivning af den **beskyttelse, der gives i henhold til artikel 48 i GDPR**, opfordrer Databeskyttelsesrådet Europa-Kommissionen til at give yderligere forsikringer og specifikke henvisninger til den britiske lovgivning, som sikrer, at det beskyttelsesniveau, der garanteres af den britiske retlige ramme, i det væsentlige svarer til det beskyttelsesniveau, der garanteres i EØS.

22. Med hensyn til **procedure- og håndhævelsesmekanismer** bemærker Databeskyttelsesrådet, at de centrale elementer, der skal kendetegne en databeskyttelsesramme, som er i overensstemmelse med EU's ramme, er, at der findes en effektiv og velfungerende uafhængig tilsynsmyndighed og et system med adgang til passende søgsmålsmekanismer, der giver borgere i EØS mulighed for at udøve deres rettigheder og indgive klage uden at støde på besværlige forhindringer for administrativ og retslig prøvelse.

23. Databeskyttelsesrådet anerkender, at Det Forenede Kongerige har gengivet størstedelen af de relevante bestemmelser i GDPR i den britiske databeskyttelsesforordning og i Data Protection Act 2018, men opfordrer ikke desto mindre Europa-Kommissionen til løbende at overvåge udviklingen i den britiske retlige ramme og praksis, som kan få ødelæggende virkninger for disse områder.

1.2.3. Offentlige myndigheders adgang til oplysninger, der overføres til Det Forenede Kongerige

24. Databeskyttelsesrådet noterer sig de betydelige ændringer i den britiske retlige ramme, der er gældende for sikkerheds- og efterretningstjenester, især med hensyn til aflytning og indsamling af kommunikationsdata. Databeskyttelsesrådet forstår, at disse ændringer bl.a. er en reaktion på den sag, som er blevet anlagt ved Domstolen og Den Europæiske Menneskerettighedsdomstol (herefter "Menneskerettighedsdomstolen"), og de nylige domme i den forbindelse.

25. Databeskyttelsesrådet bifalder navnlig, at Det Forenede Kongerige har oprettet Investigatory Powers Tribunal (retten vedrørende undersøgelsesbeføjelser). Denne ret har ikke kun kompetence til at behandle sager om retshåndhævende myndigheders anvendelse af undersøgelsesbeføjelser, men også efterretningstjenesternes. Det er derfor Databeskyttelsesrådets opfattelse, at retten vedrørende undersøgelsesbeføjelser fungerer som en egentlig domstol som omhandlet i artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder (herefter "chartret").

26. Desuden glæder Databeskyttelsesrådet sig over indførelsen i Investigatory Powers Act 2016 (loven om undersøgelsesbeføjelser af 2016, herefter "IPA 2016") af "Judicial Commissioners"

[10] Se Aftale mellem Amerikas Forenede Stater og Den Europæiske Union om beskyttelse af personoplysninger i forbindelse med forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, december 2016 (herefter "paraplyaftalen mellem EU og USA"), https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=LEGISSUM:3104_8&from=EN.
[11] Se artikel 46 og 47 i den britiske databeskyttelsesforordning.
[12] Se Schrems II.

(retskommissærer), hvilket er en klar forbedring. Rådet forstår, at en af retskommissærernes vigtige opgaver er at forhåndsgodkende forskellige overvågningsforanstaltninger i de enkelte sager, herunder målrettet aflytning og masseindsamling af kommunikationsdata (den såkaldte "double lock"-procedure).

27. For at kunne vurdere effektiviteten af dette supplerende tilsynsniveau mener Databeskyttelsesrådet imidlertid, at det er nødvendigt med en yderligere klarlægning af de scenarier, hvor en lovlig aflytning er mulig uden godkendelse fra Investigatory Powers Commissioner (kommissæren for undersøgelsesbeføjelser) eller retskommissærerne, og opfordrer Europa-Kommissionen til yderligere at vurdere og påvise, at selv hvis double lock-proceduren ikke finder anvendelse, giver den britiske retlige ramme de fornødne garantier, herunder gennem et effektivt efterfølgende tilsyn og klagemuligheder for borgerne, og sikrer dermed et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er sikret inden for EU.

28. Endvidere opfordrer Databeskyttelsesrådet Europa-Kommissionen til yderligere at bedømme betingelserne for at kunne påberåbe sig tvingende grunde og til at tilvejebringe præciseringer vedrørende de muligheder, som de berørte registrerede har for at udøve deres rettigheder, og de eventuelle klagemuligheder, de får tilbudt i forbindelse med "equipment interference"-operationer (udstyrsinterferens), især i tilfælde af en afvigelse fra double lock-proceduren.

29. Desuden mener Databeskyttelsesrådet, at der er brug for yderligere klarlægning og vurdering af masseindsamling, navnlig udvælgelse og anvendelse af selektorer, for at klarlægge, i hvilket omfang adgangen til personoplysninger overholder den tærskel, som Domstolen har fastlagt, og hvilke garantier der er indført til at beskytte de borgeres grundlæggende rettigheder, hvis data aflyttes i denne forbindelse, herunder med hensyn til dataopbevaringsperioden. En uafhængig vurdering foretaget af kompetente britiske tilsynsmyndigheder ville være særdeles nyttig. Databeskyttelsesrådet understreger også, at det forekommer desto mere kritisk, at "overseas-related communications" (oversøisk kommunikation), som falder inden for masseaflytning, synes at indebære, at Det Forenede Kongerige direkte kan aflytte og masseindsamle dataene i EU, herunder data, der er under overførsel mellem EU og Det Forenede Kongerige, hvilket ville falde ind under afgørelsesudkastets anvendelsesområde. På grund af dette aspekts betydning opfordrer Databeskyttelsesrådet Europa-Kommissionen til at overvåge udviklingen på området nøje.

30. Stadig i forbindelse med masseaflytning understreger Databeskyttelsesrådet Menneskerettighedsdomstolens og Domstolens konsekvente vurdering og minder om de betænkeligheder, der er kommet til udtryk med hensyn til sekundære data, som bør sikres med specifikke garantier på grund af deres følsomhed. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til nøje at vurdere, om garantierne i britisk lov for denne kategori af personoplysninger sikrer et beskyttelsesniveau, der i det væsentlige svarer til det, der garanteres i EØS.

31. I denne forbindelse er Databeskyttelsesrådet bekendt med, at efterretnings- og sikkerhedsudvalgets (Intelligence and Security Committee) offentlige rapport fra 2016 om anvendelsen af massebeføjelser[13] vedrører praksis i henhold til den tidligere retlige ramme, som blev erstattet af loven om undersøgelsesbeføjelser af 2016 (IPA). Rådet er ikke desto

[13] Se Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, august 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

mindre af den opfattelse, at det er nødvendigt, at de kompetente britiske tilsynsmyndigheder foretager yderligere uafhængige vurderinger og tilsyn med anvendelsen af automatiserede databehandlingsredskaber, og opfordrer Europa-Kommissionen til yderligere at vurdere dette spørgsmål og de garantier, som i denne forbindelse vil blive givet eller kan gives til de registrerede i EØS.

32. Databeskyttelsesrådet er enig med kommissæren for undersøgelsesbeføjelser i, at der er brug for yderligere gennemsyn og tilsyn for at sikre, at de garantier, der i praksis gives af de kompetente myndigheder på området for statens sikkerhed og efterretning til at afhjælpe uoverensstemmelser med anvendelsen af den relevante lovgivning, opretholdes og fortsat forbedres. Databeskyttelsesrådet bifalder også, at kommissæren for undersøgelsesbeføjelser følgelig i 2019 foretog en gennemgang af sin tilgang til inspektion af masseaflytning, "*herunder en nøje gennemgang af de teknisk komplekse måder, hvorpå masseaflytning faktisk foregår*", og forpligtede sig til at inkludere "*en detaljeret undersøgelse af de selektorer og søgekriterier, som Menneskerettighedsdomstolen har hentydet til*", i de kommende inspektioner af masseaflytning fra 2020. På grund af dette aspekts betydning er Databeskyttelsesrådet bekymret for, at kommissæren for undersøgelsesbeføjelser endnu ikke har foretaget en detaljeret undersøgelse af selektorer og søgekriterier, og opfordrer Europa-Kommissionen til nøje at overvåge udviklingen på dette punkt, især fordi det endnu ikke er klarlagt, hvilken konkret form et sådant tilsyn skal have.

33. Med hensyn til videregivelse af oplysninger til oversøiske områder understreger Databeskyttelsesrådet, at anvendelsen af undtagelsen efter britisk ret af hensyn til statens sikkerhed kan føre til, at der mangler garantier, der kan sikre, at principperne om formålsbegrænsning, nødvendighed og proportionalitet også overholdes, eller at det modtagende tredjeland også i tilstrækkelig grad fastlægger eller respekterer rettigheder for borgerne og rettigheder med hensyn til tilsyn og adgang til retsmidler. Databeskyttelsesrådet anbefaler Europa-Kommissionen at foretage yderligere undersøgelser af de overordnede garantier, som gives i henhold til britisk ret med hensyn til oversøisk videregivelse, navnlig i lyset af anvendelsen af undtagelser begrundet i statens sikkerhed.

34. Endelig er Databeskyttelsesrådet bekymret over andre former for udveksling og videregivelse af oplysninger på basis af andre instrumenter, navnlig de forskellige internationale aftaler, som er indgået mellem Det Forenede Kongerige og tredjelande, især når disse instrumenter fortsat er utilgængelige for offentligheden, f.eks. kommunikationsefterretningsaftalen mellem Det Forenede Kongerige og USA ("UK-US Communication Intelligence Agreement"). Virkningen af en sådan aftale kan blive, at de garantier, der gives i forbindelse med adgang og anvendelse af personoplysninger til nationale sikkerhedsformål, omgås. Databeskyttelsesrådet er af den opfattelse, at indgåelsen af bilaterale eller multilaterale aftaler med tredjelande med henblik på efterretningssamarbejde som retsgrundlag for direkte aflytning og indsamling af personoplysninger eller overførsel af personoplysninger til de pågældende lande også kan få betydelig indflydelse på betingelserne for yderligere brug af de indsamlede oplysninger, eftersom sådanne aftaler sandsynligvis vil berøre den britiske databeskyttelsesramme i den form, hvori den er vurderet.

1.3. Konklusion

35. Databeskyttelsesrådet mener, at tilstrækkelighedsvurderingen af Det Forenede Kongerige er unik, fordi landet har været en EU-medlemsstat. Desuden vil det også blive den første tilstrækkelighedsafgørelse, der indeholder en ophørsbestemmelse.

36. Derfor anerkender Databeskyttelsesrådet mange konvergensområder mellem den britiske databeskyttelsesramme og EU's databeskyttelsesramme. Samtidig og efter en nøje analyse af Europa-Kommissionens afgørelsesudkast og den britiske databeskyttelseslovgivning har Databeskyttelsesrådet imidlertid identificeret en række udfordringer, som gennemgås grundigt i denne udtalelse. I denne forbindelse ønsker Databeskyttelsesrådet at lægge vægt på Europa-Kommissionens altafgørende rolle i overvågningen af al relevant udvikling i Det Forenede Kongerige.

37. I lyset af ovenstående anbefaler Databeskyttelsesrådet Europa-Kommissionen at løse de udfordringer, der påpeges i denne udtalelse. Databeskyttelsesrådet opfordrer også Europa-Kommissionen til nøje at overvåge al relevant udvikling i Det Forenede Kongerige, som kan påvirke, om niveauet for beskyttelse af personoplysninger i det væsentlige svarer til EU-niveauet, og hurtigt træffe eventuelt nødvendige forholdsregler.

2. INDLEDNING

2.1. Den britiske databeskyttelsesramme

38. Den britiske databeskyttelsesramme er hovedsagelig baseret på EU's databeskyttelsesramme (navnlig GDPR og retshåndhævelsesdirektivet), hvilket skyldes, at Det Forenede Kongerige var medlem af EU indtil den 31. januar 2020. Den britiske databeskyttelseslov, Data Protection Act 2018, som trådte i kraft den 23. maj 2018 og samtidig ophævede Data Protection Act 1998, specificerer desuden anvendelsen af databeskyttelsesforordningen efter britisk lov og omsætter retshåndhævelsesdirektivet i britisk ret samt delegerer beføjelser og forpligtelser til den nationale tilsynsmyndighed for databeskyttelse, den britiske ICO.

39. Som nævnt i betragtning 12 til Europa-Kommissionens afgørelsesudkast vedtog den britiske regering loven om udtræden af EU, European Union (Withdrawal) Act 2018, hvorved direkte EU-lovgivning, der finder direkte anvendelse, indarbejdes i britisk lov. I henhold til denne lov har britiske ministre beføjelse til at vedtage sekundær lovgivning ved hjælp af lovbestemte instrumenter for at foretage de nødvendige ændringer i "retained EU law" (bibeholdt EU-ret) efter Det Forenede Kongeriges udtræden af EU, så den passer til britiske forhold.

40. Følgelig består den relevante retlige ramme, der finder anvendelse i Det Forenede Kongerige efter udgangen af overgangsperioden[14], af:

- United Kingdom General Data Protection Regulation (Det Forenede Kongeriges forordning om databeskyttelse, herefter "den britiske databeskyttelsesforordning"), som omsat i britisk ret i henhold til European Union (Withdrawal) Act 2018, som ændret ved Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019 (herefter "DPPEC 2019")
- Data Protection Act 2018 ("DPA 2018"), som ændret ved DPPEC 2019, og DPPEC 2020 og
- Investigatory Powers Act 2016 ("IPA 2016")

[14] Overgangsperioden er fastsat til at slutte den 31. december 2020, hvorefter EU-retten ikke længere finder anvendelse i Det Forenede Kongerige. Passerelleperioden ("bridge period") er fastsat til at slutte senest den 30. juni 2021 og henviser til den supplerende periode, hvori fremsendelse af personoplysninger fra EØS til Det Forenede Kongerige ikke betegnes som en overførsel.

(under ét benævnt "den britiske databeskyttelsesramme").

2.2. Rækkevidden af Databeskyttelsesrådets vurdering

41. Europa-Kommissionens afgørelsesudkast er resultatet af en vurdering af den britiske databeskyttelsesramme fulgt af drøftelser med den britiske regering. I overensstemmelse med artikel 70, stk. 1, litra s), i databeskyttelsesforordningen forventes Databeskyttelsesrådet at afgive en uafhængig udtalelse om Europa-Kommissionens konklusioner, at finde eventuelle mangler i tilstrækkelighedsrammen og at bidrage med forslag til at afhjælpe disse.

42. Som nævnt i tilstrækkelighedsreferencen: "*Under alle omstændigheder bør de af Kommissionen forelagte oplysninger være udtømmende og sætte Databeskyttelsesrådet i stand til at foretage en vurdering af databeskyttelsesniveauet i det pågældende tredjeland*"[15].

43. I denne forbindelse skal det bemærkes, at Databeskyttelsesrådet kun modtog dele af den dokumentation, der var relevant for undersøgelsen af den britiske retlige ramme, rettidigt. Databeskyttelsesrådet modtog størstedelen af den britiske lovgivning, der henvises til i afgørelsesudkastet, via linksene hertil i dette udkast. Europa-Kommissionen var ikke i stand til at give Databeskyttelsesrådet skriftlige redegørelser og forpligtelser fra britisk hold i forbindelse med kommunikationen mellem de britiske myndigheder og Europa-Kommissionen under dette arbejde[16].

44. På baggrund af ovenstående betragtninger og på grund af den begrænsede tidsramme (to måneder), som Databeskyttelsesrådet har fået til at vedtage denne udtalelse, har rådet valgt at fokusere på nogle specifikke punkter, der fremlægges i afgørelsesudkastet, og præsentere sin analyse af og udtalelse om disse.

45. Når Databeskyttelsesrådet analyserer lovgivning og praksis i et tredjeland, som var medlem af EU indtil for nylig, er det klart, at det finder mange aspekter, der i det væsentlige svarer til EU's databeskyttelsesramme. I lyset af sin rolle i vedtagelsen af en konstatering af et tilstrækkeligt beskyttelsesniveau og den mængde lovstof og praksis, der skal analyseres, har Databeskyttelsesrådet besluttet at fokusere på de aspekter, hvor det fandt mest grund til en nøjere undersøgelse. Endvidere dækker en meget stor del af analysen, i tråd med Domstolens retspraksis, den retlige ordning for at give adgang af hensyn til statens sikkerhed til personoplysninger, der overføres til Det Forenede Kongerige, og det britiske sikkerhedsapparats praksis. Imidlertid skal man huske, at statens sikkerhed

---

[15] Se WP254 rev.01, s. 3.

[16] Hvad angår: artikel 48 i GDPR (fodnote 78 i afgørelsesudkastet); styrkede garanti- og sikkerhedsforanstaltninger, som dataansvarlige skal træffe ved databehandling i forbindelse med statens sikkerhed (fodnote 64 i afgørelsesudkastet); kravet til den dataansvarlige om at overveje fra sag til sag, om det er nødvendigt at benytte sig af undtagelsen, selvom der er udstedt et certifikat om statens sikkerhed (betragtning 126 og fodnote 172 i afgørelsesudkastet); det forhold, at beskyttelsen i paraplyaftalen mellem EU og USA vil finde anvendelse på alle personoplysninger, der fremlægges eller opbevares i henhold til CLOUD Act-aftalen mellem Det Forenede Kongerige og USA, uanset arten eller typen af det organ, der fremsætter en anmodning herom; detaljerne i den konkrete gennemførelse af de databeskyttelsesgarantier, der stadig er genstand for drøftelser mellem Det Forenede Kongerige og USA; bekræftelsen på, at de britiske myndigheder kun vil lade denne aftale træde i kraft, når de er sikre på, at gennemførelsen heraf er i overensstemmelse med de retlige forpligtelser, der er fastsat deri, herunder klarhed med hensyn til overholdelsen af databeskyttelsesstandarder for enhver oplysning, der fremsættes anmodning om i henhold til denne aftale (betragtning 153 i afgørelsesudkastet); situationer, hvor data overføres fra EU til Det Forenede Kongerige inden for rækkevidden af dette afgørelsesudkast, og det forhold, at der altid vil være en forbindelse til de britiske øer, en "British Islands connection", og at eventuel udstyrsinterferens vedrørende sådanne data derfor kræver en obligatorisk interferenskendelse som fastsat i § 13, stk. 1, i IPA 2016 (betragtning 206 i afgørelsesudkastet); og de eksempler, der gives på operationelle formål (betragtning 216 og fodnote 369 i afgørelsesudkastet).

naturligvis er et rets- og sikkerhedsområde, hvor medlemsstaternes lovgivning ikke er harmoniseret på EU-plan og derfor kan variere.

46. Databeskyttelsesrådet tog EU's gældende databeskyttelsesramme i betragtning, herunder chartrets artikel 7, 8 og 47, som henholdsvis beskytter retten til privatliv og familieliv, retten til beskyttelse af personoplysninger og adgangen til effektive retsmidler og en retfærdig rettergang, og artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder ("EMRK"), som beskytter retten til privatliv og familieliv. Foruden ovenstående tog Databeskyttelsesrådet kravene i GDPR i betragtning sammen med den relevante retspraksis.

47. Formålet med dette arbejde er at afgive en udtalelse til Europa-Kommissionen om vurderingen af tilstrækkeligheden af beskyttelsesniveauet i Det Forenede Kongerige. Begrebet "tilstrækkeligt beskyttelsesniveau", som allerede var at finde i direktiv 95/46/EF, er blevet videreudviklet af Domstolen. Det er vigtigt at minde om den standard, som Domstolen opstiller i Schrems I-sagen, nemlig, at mens "beskyttelsesniveauet" i tredjelandet "i det væsentlige svarer" til det niveau, der er sikret inden for EU, kan "*de midler, som tredjelandet anvender i denne henseende for at sikre et sådant beskyttelsesniveau, [...] være forskellige fra de midler, som gennemføres inden for [EU]*"[17]. Formålet er derfor ikke at afspejle den europæiske lovgivning punkt for punkt, men at fastsætte centrale hovedkrav i den lovgivning, der er genstand for en undersøgelse. Beskyttelsesniveauets tilstrækkelighed kan opnås ved en kombination af rettigheder for de registrerede og forpligtelser for dem, der behandler data, eller som fører kontrol med en sådan databehandling, og ved tilsyn fra uafhængige organer. Databeskyttelsesreglerne er imidlertid kun effektive, hvis de kan håndhæves og bliver fulgt i praksis. Der skal derfor ikke kun tages hensyn til indholdet i de regler, der gælder for personoplysninger, som overføres til et tredjeland eller en international organisation, men også til det system, der skal sikre reglernes effektivitet. Effektive håndhævelsesmekanismer er af afgørende betydning for databeskyttelsesreglernes effektivitet[18].

2.3. Generelle kommentarer og betænkeligheder

2.3.1. Internationale forpligtelser, som Det Forenede Kongerige har påtaget sig

48. Ifølge artikel 45, stk. 2, litra c), i databeskyttelsesforordningen og tilstrækkelighedsreferencen[19] skal Europa-Kommissionen, når den vurderer tilstrækkeligheden af beskyttelsesniveauet i et tredjeland, bl.a. tage hensyn til internationale forpligtelser, som tredjelandet har påtaget sig, eller andre forpligtelser, der følger af tredjelandets deltagelse i multilaterale eller regionale systemer, navnlig i forbindelse med beskyttelse af personoplysninger, samt gennemførelsen af sådanne forpligtelser. Der bør endvidere tages hensyn til tredjelandets tiltrædelse af Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (herefter "konvention 108"))[20] og tillægsprotokollen hertil[21].

49. **I denne henseende bifalder Databeskyttelsesrådet, at Det Forenede Kongerige har tilsluttet sig EMRK og er under Menneskerettighedsdomstolens jurisdiktion. Desuden har Det Forenede**

[17] Se Domstolens dom af 6. oktober 2015, C-362/14, Maximillian Schrems mod Data Protection Commissioner, ECLI:EU:C:2015:650, præmis 73 og 74 (Schrems I).
[18] Se WP254 rev.01, s. 3.
[19] Se WP254 rev.01, s. 3.
[20] Se Konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling, Konvention 108, af 28. januar 1981.
[21] Se tillægsprotokol om tilsynsmyndigheder og grænseoverskridende dataudveksling til Konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling, som kan undertegnes fra den 8. november 2001.

Kongerige også tilsluttet sig konvention 108 og tillægsprotokollen hertil, har i 2018 undertegnet konvention 108+[22] og arbejder i øjeblikket på at ratificere den.

2.3.2. Den britiske databeskyttelsesrammes mulige fremtidige afvigelse

50. Som nævnt i betragtning 281 i afgørelsesudkastet skal Europa-Kommissionen tage i betragtning, at Det Forenede Kongerige efter udgangen af overgangsperioden, der er fastsat i udtrædelsesaftalen[23], administrerer, anvender og håndhæver sin egen databeskyttelsesordning, og så snart den midlertidige bestemmelse i artikel FINPROV.10A i handels- og samarbejdsaftalen mellem EU og Det Forenede Kongerige[24] ikke længere finder anvendelse, kan dette afføde mærkbare ændringer af den databeskyttelsesramme, der er blevet vurderet i afgørelsesudkastet, og andre relevante forandringer.

51. Europa-Kommissionen har derfor besluttet at indarbejde en ophørsbestemmelse i sit udkast til afgørelse[25] med en udløbsdato fire år efter afgørelsens ikrafttræden.

52. Det er vigtigt at bemærke, at de britiske ministres mulighed for at vedtage sekundær lovgivning efter udløbet af passerelleperioden kan medføre, at den britiske databeskyttelsesramme i fremtiden afviger betydeligt fra EU's ramme.

53. Den britiske regering har nemlig oplyst, at det er dens hensigt at udforme separate og uafhængige databeskyttelsespolitikker, som kan medføre afvigelser fra EU's databeskyttelseslovgivning[26]. Denne hensigt omfatter indlemmelse af personoplysningsaspekter i

[22] Se protokol om ændring af Konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (herefter "konvention 108+") af 18. maj 2018.

[23] Se Aftale om Det Forenede Kongerige Storbritannien og Nordirlands udtræden af Den Europæiske Union og Det Europæiske Atomenergifællesskab (EUT L 29 af 31.1.2020, s. 7).

[24] Se Handels- og samarbejdsaftale mellem Den Europæiske Union og Det Europæiske Atomenergifællesskab på den ene side og Det Forenede Kongerige Storbritannien og Nordirland på den anden side (EUT L 444 af 31.12.2020, s. 14).

[25] Se artikel 4 i afgørelsesudkastet. Se også betragtning 282 i afgørelsesudkastet.

[26] Den britiske nationale datastrategi (senest ajourført den 9. december 2020 https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) omfatter bl.a. følgende opgave: "*At kæmpe for den internationale dataudveksling. Informationsstrømmen på tværs af grænserne er drivkraften bag globale forretninger, forsyningskæder og handel og skaber vækst i hele verden. Den spiller også en bredere samfundsmæssig rolle. Overførsel af personoplysninger sikrer, at folk får deres løn udbetalt, og hjælper dem med at holde kontakten med deres kære. Og som coronaviruspandemien har vist, kan udveksling af sundhedsdata bidrage til altafgørende videnskabelig forskning i sygdomme og samtidig forene landene i deres beredskab mod globale sundhedskriser.* ***Efter at have forladt Den Europæiske Union vil Det Forenede Kongerige kæmpe for fordelene ved dataudveksling.*** *Vi vil fremme bedste praksis hos os selv og samarbejde med vores internationale partnere om* ***at sikre, at dataene ikke begrænses i urimelig grad af nationale grænser og fragmenterede retlige ordninger****, således at vi kan udnytte dataenes fulde potentiale*" fremhævelse tilføjet).

handelsaftaler[27], hvilket er en praksis, der medfører risiko for, at det niveau for beskyttelse af personoplysninger, som Det Forenede Kongerige fastsætter, falder[28].

54. Endelig skal det bemærkes, at ikke alene er Det Forenede Kongerige siden udløbet af overgangsperioden ikke længere bundet af Domstolens retspraksis, men er muligvis heller ikke længere bundet af Domstolens allerede afsagte domme, der anses for bibeholdt retspraksis i den britiske retlige ramme, idet Det Forenede Kongerige navnlig har mulighed for at ændre bibeholdt EU-ret efter udløbet af passerelleperioden, og Supreme Court er ikke bundet af bibeholdt retspraksis fra EU overhovedet[29].

55. **I betragtning af risiciene ved den britiske databeskyttelsesrammes eventuelle afvigelse fra EU's regelværk efter udløbet af passerelleperioden bifalder Databeskyttelsesrådet Europa-Kommissionens beslutning om at indføre en fireårig ophørsbestemmelse i sit udkast til afgørelse. Databeskyttelsesrådet vil imidlertid gerne fremhæve betydningen af Europa-Kommissionens tilsynsrolle[30]. Europa-Kommissionen bør nemlig løbende overvåge al relevant udvikling i Det Forenede Kongerige, som kan påvirke, om niveauet for beskyttelse af personoplysninger, som overføres i henhold til tilstrækkelighedsafgørelsen om Det Forenede Kongerige, i det væsentlige svarer til EU-niveauet, og efter afgørelsens ikrafttræden føre fast tilsyn med dette. Desuden bør Europa-Kommissionen træffe passende foranstaltninger ved at suspendere, ændre eller ophæve tilstrækkelighedsafgørelsen på grundlag af de foreliggende omstændigheder, hvis Europa-Kommissionen efter vedtagelsen af tilstrækkelighedsafgørelsen ser tegn på, at der ikke længere sikres et tilstrækkeligt beskyttelsesniveau i Det Forenede Kongerige.**

56. Databeskyttelsesrådet vil på sin side gøre sit bedste for at informere Europa-Kommissionen om relevante foranstaltninger, som måtte blive truffet af medlemsstaternes datatilsynsmyndigheder i den private eller den offentlige sektor, og navnlig for så vidt angår klager, som registrerede i EØS, indgiver vedrørende overførsel af personoplysninger fra EØS til Det Forenede Kongerige.

3. GENERELLE DATABESKYTTELSESASPEKTER

3.1. Indholdsprincipper

[27] Ibidem: "*At lette den grænseoverskridende dataudveksling:* ***Vi vil arbejde globalt for at fjerne unødvendige hindringer for internationale dataudvekslinger. Vi vil aftale ambitiøse databestemmelser i vores handelsforhandlinger*** *og anvende vores nye plads som selvstændig part i Verdenshandelsorganisationen til at påvirke handelsreglerne om data i en bedre retning.* ***Vi vil fjerne hindringer for internationale dataoverførsler****, der understøtter vækst og innovation, herunder ved at udvikle en ny kapacitet i Det Forenede Kongerige, der skaber nye og innovative mekanismer til internationale dataoverførsler. Vi vil også samarbejde med G20-partnerne om at skabe interoperabilitet mellem nationale dataordninger for at minimere gnidninger ved overførsel af data mellem forskellige lande*" fremhævelse tilføjet).

[28] Se Europa-Parlamentets beslutning af 12. december 2017 "Udvikling af en digital handelsstrategi" (2017/2065(INI)), litra V), hvori det understreges, "at beskyttelsen af personoplysninger ikke er til forhandling i [EU-]handelsaftaler", på: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_DA.html. Se også Europa-Parlamentets beslutning af 25. marts 2021 om Kommissionens evalueringsrapport om gennemførelsen af den generelle forordning om databeskyttelse to år efter dens anvendelse, punkt 28, hvori der står, at Europa-Parlamentet: "støtter Kommissionens praksis med at behandle spørgsmål om data- og persondatastrømme adskilt fra handelsaftaler", https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_DA.html.

[29] Se § 6, stk. 3-6, i EU (Withdrawal) Act 2018.

[30] Se artikel 45, stk. 4, i GDPR.

57. Kapitel 3 i tilstrækkelighedsreferencen omhandler "Indholdsprincipper". Et tredjelands system skal indeholde indholdsprincipper, for at databeskyttelsesniveauet i tredjelandet kan anses for i det væsentlige at svare til det niveau, der er sikret inden for EU. Databeskyttelsesrådet anerkender, at Det Forenede Kongerige ikke har en kodificeret forfatning, idet der ikke findes et enkelt dokument med de grundlæggende bestemmelser, der findes i en grundlov. Imidlertid er retten til respekt for privatlivet og familielivet (og retten til databeskyttelse som led i denne ret) og retten til en retfærdig rettergang[31] indarbejdet i menneskerettighedsloven af 1998 (Human Rights Act 1998), og den konstitutionelle værdi af denne bestemmelse er blevet anerkendt af de britiske domstole. Human Rights Act 1998 indeholder nemlig de rettigheder, der er fastlagt i EMRK[32]. Desuden har Human Rights Act 1998 den meget vigtige bestemmelse, at offentlige myndigheder til enhver tid skal handle i overensstemmelse med EMRK[33].

58. Bortset fra forskelle i struktur og formalia mellem britisk lovgivning og EU-lovgivning bemærker Databeskyttelsesrådet som forventet, at den britiske tilgang til databeskyttelse svarer til EU's, fordi Det Forenede Kongerige var en EU-medlemsstat indtil den 31. januar 2020. Derfor er mange indholdsprincipper de samme som i GDPR og sikrer dermed et beskyttelsesniveau, der i det væsentlige svarer til EU-niveauet. Databeskyttelsesrådet har besluttet ikke at analysere de indholdsprincipper yderligere, som er i overensstemmelse med EU-retten, og er tilfreds med Europa-Kommissionens analyse i afgørelsesudkastet. Blandt disse indholdsprincipper kan nævnes: begreber (f.eks. "personoplysninger" "behandling af personoplysninger" og "dataansvarlig"), grundlag for lovlig og rimelig behandling til legitime formål, formålsbegrænsning, datakvalitet og dataproportionalitet, dataopbevaring, sikkerhed og fortrolighed, gennemsigtighed, særlige kategorier af oplysninger, direkte markedsføring og automatiske afgørelser og profilering. Databeskyttelsesrådet bemærker endvidere, at den britiske databeskyttelsesforordning og DPA 2018 omfatter indholdsprincipper, som rækker ud over, hvad der kræves ifølge tilstrækkelighedsreferencen, og afspejler de principper, der er fastlagt i GDPR, hvilket hæver det beskyttelsesniveau, der er sikret i Det Forenede Kongerige. Disse indholdsprincipper er f.eks. dem, der vedrører anmeldelser af brud på persondatasikkerheden, den databeskyttelsesansvarlige, konsekvensanalyser vedrørende databeskyttelse og databeskyttelse gennem design og gennem standardindstillinger.

59. Men som nævnt i indledningen ønsker Databeskyttelsesrådet især i denne udtalelse at berøre visse punkter, som giver anledning til betænkeligheder, og rådet anmoder Europa-Kommissionen om præciseringer.

3.1.1. Retten til indsigt, berigtigelse, sletning og indsigelse

60. Den såkaldte immigrationsundtagelse ("immigration exemption"), som er fastlagt i **DPA 2018, Schedule 2, del 1**, afsnit 4, tillader dataansvarlige, der er involveret i immigrationskontrol, at undlade at anvende visse registreredes rettigheder som fastsat i DPA 2018, hvis dette sandsynligvis ville "*skade en effektiv immigrationskontrol*" eller "*efterforskningen eller afsløringen af aktiviteter, som ville underminere opretholdelsen af en effektiv immigrationskontrol*".

61. Som Europa-Kommissionen har anerkendt i sit afgørelsesudkast[34],og som Europa-Parlamentets LIBE-udvalg har henvist til i sin udtalelse om indgåelsen på Unionens vegne af

[31] Se artikel 6 og 8 i EMRK (Schedule 1 til Human Rights Act 1998).
[32] Se desuden betragtning 8-10 i afgørelsesudkastet.
[33] Se § 6 i Human Rights Act 1998.
[34] Se betragtning 62-65 i afgørelsesudkastet.

handels- og samarbejdsaftalen mellem EU og Det Forenede Kongerige[35], er denne undtagelse **"bredt" formuleret**. Den finder anvendelse på følgende rettigheder: retten til at blive underrettet, retten til indsigt, retten til sletning, retten til begrænsning af behandling og retten til indsigelse.

62. Det er desuden vigtigt at notere sig, at denne undtagelse også gælder, hvis en dataansvarlig ("dataansvarlig 1") ikke indhenter personoplysninger med henblik på immigrationskontrol, men stiller dem til rådighed for en anden dataansvarlig ("dataansvarlig 2"), som behandler disse personoplysninger med henblik på immigrationskontrol (f.eks. det britiske indenrigsministerium)[36].

63. I sagen *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (03 October 2019)* anfægtede ansøgerne lovligheden af immigrationsundtagelsen med påstand om, at den var i strid med artikel 23 i GDPR og uforenelig med de rettigheder, der er sikret ved chartrets artikel 7 og 8 om beskyttelse af privatlivets fred og af personoplysninger. High Court of England and Wales (herefter "High Court") undersøgte, om immigrationsundtagelsen, der er fastsat i DPA 2018, Schedule 2, del 1, afsnit 4, var lovlig, og fastslog dens lovlighed.

---

[35] Se i denne henseende vedrørende **den brede formulering** af immigrationsundtagelsen Udtalelse fra Europa-Parlamentets Udvalg om Borgernes Rettigheder og Retlige og Indre Anliggender om indgåelse på Unionens vegne af handels- og samarbejdsaftalen mellem Den Europæiske Union og Det Europæiske Atomenergifællesskab på den ene side og Det Forenede Kongerige Storbritannien og Nordirland på den anden side og af aftalen mellem Den Europæiske Union og Det Forenede Kongerige Storbritannien og Nordirland om sikkerhedsprocedurer for udveksling og beskyttelse af klassificerede informationer (2020/0382(NLE)), 5. februar 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_DA.pdf, punkt 10: *"minder i denne forbindelse om Parlamentets beslutninger fra februar og juni 2020, som påpeger **den generelle og brede undtagelse** for behandling af personoplysninger med henblik på immigrationsformål i Det Forenede Kongeriges lovgivning om databeskyttelse (UK Data Protection Act)"*, og punkt 11: *"er af den opfattelse, at det er nødvendigt at ændre **den generelle og brede undtagelse** for behandling af personoplysninger med henblik på immigrationsformål i Det Forenede Kongeriges lovgivning om databeskyttelse (UK Data Protection Act) […], før der kan træffes en gyldig afgørelse om tilstrækkelighed"* (fremhævelse tilføjet).

[36] Se eksemplet i ICO's "Guide to the General Data Protection Regulation (GDPR)", af 1. januar 2021, s. 307 (fremhævelse tilføjet): *"En privat enhed (dataansvarlig 1) underretter indenrigsministeriet (dataansvarlig 2) om en medarbejder, som menes at have indgivet falske dokumenter som dokumentation for sin identitet og sine kvalifikationer med henblik på at blive ansat. Arbejdsgiveren giver indenrigsministeriet den relevante information. Medarbejderens ret til at blive underrettet om, at vedkommendes personoplysninger er blevet videregivet til indenrigsministeriet, er begrænset, for så vidt som overholdelsen af denne ret sandsynligvis ville skade efterforskningen.*
***Arbejdsgiveren har derfor ingen pligt til at underrette medarbejderen om, at vedkommendes personoplysninger er blevet videregivet til indenrigsministeriet**, og **indenrigsministeriet** har heller ikke pligt til at sende den pågældende en meddelelse om databeskyttelse for at oplyse, at ministeriet nu behandler vedkommendes personoplysninger. Undtagelsen finder ensartet anvendelse på begge dataansvarlige.*
*Medarbejderen anmoder imidlertid om en kopi af sine personoplysninger fra indenrigsministeriet, som er i færd med at behandle dem. **Indenrigsministeriet kan anvende undtagelsen** til at tilbageholde visse af medarbejderens personoplysninger, hvis videregivelse heraf sandsynligvis ville skade efterforskningen. Hvis medarbejderen indgiver en lignende anmodning **til sin arbejdsgiver, kan denne også og i samme omfang anvende undtagelsen**."*
Dette præciseres på s. 300: *"Som regel vil indenrigsministeriet eller en underordnet enhed eller kontrahent være den dataansvarlige, der anvender denne undtagelse. Det er imidlertid vigtigt at bemærke, at anvendelsen af denne undtagelse ikke er begrænset til indenrigsministeriet. Det kan også være relevant for andre dataansvarlige såsom arbejdsgivere, universiteter og politiet, som er i kontakt med indenrigsministeriet i forbindelse med immigrationsanliggender."*

64. High Court lagde bl.a. følgende til grund:

- *"[…] immigrationsundtagelsen er blot et spørgsmål om "væsentlige samfundsinteresser" og forfølger et legitimt mål. […]"*, præmis 30
- *"immigrationsundtagelsen opfylder de krav, der stilles til en foranstaltning, der er "i overensstemmelse med loven". […]"*, præmis 38
- *"Immigrationsundtagelsen må kun anvendes, hvis og i det omfang overholdelsen af "de anførte GDPR-bestemmelser"* ***sandsynligvis ville skade*** *opretholdelsen af en effektiv immigrationskontrol eller efterforskningen eller afsløringen af aktiviteter, som ville underminere opretholdelsen af en effektiv immigrationskontrol. Ordlyden "sandsynligvis ville skade" (would be likely to prejudice) i forbindelse med Data Protection Act 1998 (som blev erstattet DPA 2018) blev fortolket således, at den betyder "en meget betydelig og tungtvejende sandsynlighed for skadelig virkning for samfundets interesser. Risikoen skal være af en sådan grad, at der "meget vel" kunne ske skade på disse interesser, selv om risikoen langt fra er mere sandsynlig end usandsynlig […]."*, præmis 39 (fremhævelse tilføjet).

65. Det bør fremhæves, at denne dom ikke er endelig, og at den er blevet anket, så vidt Databeskyttelsesrådet er informeret.

66. Databeskyttelsesrådet har specificeret i sine retningslinjer om begrænsninger i henhold til artikel 23 i GDPR ("artikel 23-retningslinjerne")[37], at *"[…] i en GDPR-sammenhæng skal begrænsningerne være* ***omfattet af en lovgivningsmæssig foranstaltning****, kun vedrøre* ***et begrænset antal rettigheder for den registrerede og/eller forpligtelser for den dataansvarlige****, som er angivet i artikel 23 i GDPR,* ***respektere det væsentligste indhold*** *af de omhandlede grundlæggende rettigheder og frihedsrettigheder, udgøre en* ***nødvendig og forholdsmæssig foranstaltning*** *i et demokratisk samfund og garantere et af de hensyn, der er fastsat i artikel 23, stk. 1, i GDPR […]"*[38].

67. Databeskyttelsesrådet minder også om, at det i betragtning 41 i GDPR hedder, at "*[n]år denne forordning henviser* ***til et retsgrundlag eller en lovgivningsmæssig foranstaltning****, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament, med forbehold for krav i henhold til den forfatningsmæssige orden i den pågældende medlemsstat. Et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning bør imidlertid være* ***klar(t) og præcis(t), og anvendelse heraf bør være forudsigelig for personer, der er omfattet af dets/dens anvendelsesområde****, jf. retspraksis fra Den Europæiske Unions Domstol og Den Europæiske Menneskerettighedsdomstol*" (fremhævelse tilføjet).

68. Selv om Menneskerettighedsdomstolen fastslog, at "*[e]ndvidere med hensyn til ordene "i overensstemmelse med loven" og "foreskrevet ved lov" i [EMRK's] artikel 8-11 bemærker Domstolen, at den altid har forstået udtrykket "lovgivning" i dets "materielle" og ikke dets "formelle" betydning; det omfatter såvel "skreven ret", som omfatter bestemmelser med lavere rang og lovgivning som lovgivningsmæssige foranstaltninger, der vedtages af faglige sammenslutninger ved delegation fra parlamentet inden for rammerne af deres selvstændige lovgivningsbeføjelse, og uskreven ret.*

[37] Se EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, version 1.0, vedtaget den 15. december 2020, som i øjeblikket er under færdigredigering efter en offentlig høring, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.
[38] Se artikel 23-retningslinjerne, punkt 9, s. 5.

*"Lovgivning" skal forstås således, at det omfatter både skreven ret og **retspraksis**"*[39], minder Databeskyttelsesrådet i artikel 23-retningslinjerne om, at *"ifølge Domstolens retspraksis skal enhver **lovgivningsmæssig foranstaltning**, der vedtages på grundlag af artikel 23, stk. 1, i GDPR, navnlig **opfylde de specifikke krav i artikel 23, stk. 2, i databeskyttelsesforordningen**. Det fastsættes ved artikel 23, stk. 2, i databeskyttelsesforordningen, at de lovgivningsmæssige foranstaltninger, der sætter begrænsninger for registreredes rettigheder og dataansvarliges forpligtelser, som minimum, hvor det er relevant, **skal indeholde specifikke bestemmelser om en række kriterier**. Generelt skal alle nedenstående kriterier **være omfattet af den lovgivningsmæssige foranstaltning**, der pålægger begrænsninger i henhold til artikel 23 i databeskyttelsesforordningen*".[40]

69. Det kan i denne henseende konstateres, at **immigrationsundtagelsen ikke** i sig selv **specificerer følgende elementer, som der henvises til i henhold til artikel 23, stk. 2, i GDPR**:

- "garantierne for at undgå misbrug eller ulovlig adgang eller overførsel" (d)
- "den dataansvarlige eller kategorierne af dataansvarlige" (e)[41]
- "risiciene for de registreredes rettigheder og frihedsrettigheder" (g)
- "de registreredes ret til at blive underrettet om begrænsningen, medmindre dette kan skade formålet med begrænsningen" (h).

70. ICO's GDPR-vejledning, "Guide to the General Data Protection Regulation (GDPR)"[42], herunder et kapitel om immigrationsundtagelsen, giver en klarlægning af immigrationsundtagelsen, men **kan ikke** som sådan udgøre supplerende bindende regler.

---

[39] Se Menneskerettighedsdomstolens dom af 14. september 2010, Sanoma Uitgevers B.V. mod Nederlandene, EC:ECHR:2010:0914JUD003822403, præmis 83 (fremhævelse tilføjet).

[40] Se artikel 23-retningslinjerne, punkt 45 og 46, s. 11. Chartrets artikel 52, stk. 3, bestemmer, at *"[i] det omfang dette charter indeholder rettigheder svarende til dem, der er sikret ved den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, har de samme betydning og omfang som i konventionen. Denne bestemmelse er ikke til hinder for, at EU-retten kan yde en mere omfattende beskyttelse".* Med hensyn til begrebet "**fastlagt i lovgivningen**" i henhold til chartrets artikel 52, stk. 1, bør de kriterier, som Menneskerettighedsdomstolen har udviklet, anvendes som foreslået i flere af Domstolens generaladvokaters forslag til afgørelse, se f.eks. forslag til afgørelse i forenede sager C-203/15 og C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, punkt 137-154, og i sag C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, punkt 88-114. Således kan der bl.a. henvises til Menneskerettighedsdomstolens dom i sagen Weber og Saravia mod Tyskland, præmis 84: *"Domstolen gentager, at ordlyden "**i overensstemmelse med loven**" som omhandlet i artikel 8, stk. 2, i [EMRK] for det første kræver, at den anfægtede foranstaltning skal have et vist grundlag i **national ret**; den henviser også til den pågældende **lovgivnings kvalitet**, som kræver, at den bør være tilgængelig for den berørte person, som desuden skal kunne forudse konsekvenserne heraf for vedkommende selv, og være forenelig med retsstatsprincipperne*" (fremhævelse tilføjet).
Se også betragtning 41 i GDPR: *"Et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning bør imidlertid være **klar(t)** og **præcis(t)**, og anvendelse heraf bør være **forudsigelig for personer, der er omfattet** af dets/dens anvendelsesområde, jf. retspraksis fra Den Europæiske Unions Domstol og Den Europæiske Menneskerettighedsdomstol"* (fremhævelse tilføjet).

[41] Se førnævnte sag for High Court, præmis 54: *"Efter min opfattelse er der intet ulovligt ved, at immigrationsundtagelsen er til rådighed **for alle dataansvarlige**, der behandler data i de nævnte øjemed. Som de sagsøgte påpeger, ville immigrationsundtagelsen uden paragraph 4(3)-(4) være frataget sin effektive virkning i tilfælde, hvor der indhentes personoplysninger fra tredjeparter (såsom en lokal myndighed eller skattevæsenet) med henblik på at opretholde en effektiv immigrationskontrol"* (fremhævelse tilføjet), hvilket bekræfter den **generaliserede** anvendelse af begrænsningerne.

[42] ICO's "Guide to the General Data Protection Regulation (GDPR)", af 1. januar 2021, s. 299-307.

Desuden er spørgsmålet om "lovgivningens kvalitet" særlig relevant i lyset af betydningen af de begrænsede rettigheder og udvidelsen af undtagelsen[43].

71. Ydermere beskriver "**skade-testen**" heller ikke de garantier, der skal forebygge misbrug eller ulovlig adgang eller overførsel, og som f.eks. indenrigsministeriet skal gennemføre.

72. I lyset af ovenstående bemærker Databeskyttelsesrådet, at der er behov for yderligere klarlægning af anvendelsen af immigrationsundtagelsen.

---

[43] Se førnævnte sag for High Court, præmis 57: *"Mr Knight oplyser over for mig, at kommissæren er ved at lægge sidste hånd på en vejledning om undtagelsen, men den får kun "retlig" status i den forstand, at den udstedes i medfør af kommissærens beføjelser i henhold til artikel 57, stk. 1, i GDPR. Den får ikke retlig status i henhold til DPA 2018."*
Der henvises navnlig i dommens præmis 56-60 til begrundelsen for indførelsen af en retligt bindende vejledning støttet af ICO:
"56. Endelig nævner jeg kommissærens udsagn om, at immigrationsundtagelsen ikke ville være en forholdsmæssig gennemførelse af artikel 23, stk. 1, i GDPR uden retlig vejledning til at give garantier med hensyn til betydningen og anvendelsen af denne undtagelse. Mr Knight anfører, at bestemmelsen er forholdsmæssig, hvis den suppleres med en sådan vejledning.
57. Mr Knight oplyser over for mig, at kommissæren er ved at lægge sidste hånd på en vejledning om undtagelsen, men den får kun "retlig" status i den forstand, at den udstedes i medfør af kommissærens beføjelser i henhold til artikel 57, stk. 1, i GDPR. Den får ikke retlig status i henhold til DPA 2018." Jeg forstår også, at indenrigsministeriet har fremlagt et udkast til en intern vejledning til personalet om immigrationsundtagelsen (se [22] ovenfor). I praksis får vejledning, der udstedes af kommissæren, indflydelse uanset sit retsgrundlag. Kommissæren har imidlertid ingen beføjelse til at udstede "bindende" vejledning af den art, som Supreme Court havde i tankerne i sagen Christian Institute (se [101] og [107]). Det synes at kræve primær lovgivning, hvis det skulle findes nødvendigt med en vejledning om immigrationsundtagelsen med samme status som de adfærdskodekser, der i øjeblikket er fastlagt i § 121-124 i DPA 2018.
58. I sin argumentation for en retlig vejledning hævder Mr Knight, at den sammenhæng, hvori anvendelsen af immigrationsundtagelsen vil forekomme, nødvendigvis indrammer betænkelighederne om, hvorvidt dens eksistens og anvendelse er nødvendig og forholdsmæssig. Han henleder opmærksomheden på især to spørgsmål i den retlige sammenhæng. For det første falder de personoplysninger, som immigrationsundtagelsen finder anvendelse på, i sagens natur sandsynligvis i en særlig kategori som omhandlet i artikel 9, stk. 1, i GDPR (dvs. data "om racemæssig eller etnisk baggrund"). Sådanne data er specificeret i GDPR, fordi de kræver en højere grad af beskyttelse (Opinion 1/15 [2019] 3 C.M.L.R 25, [141]). For det andet er det et grundlæggende træk ved databeskyttelseslovgivning, at især retten til indsigt er af stor betydning som indgangsvinkel for de registrerede til at kunne udøve deres øvrige rettigheder (se YS mod Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081, [2015] 1 C.M.L.R. 18, [44]).
59. Mr Knight peger på fire forhold af praktisk art. Hvis for det første de dataansvarlige ikke forklarer de registrerede, at de har benyttet en retlig undtagelse, eller giver dem et bredt sammendrag af begrundelserne herfor, vil den registrerede ikke kunne vide, at undtagelsen er blevet anvendt, og er derfor ikke i stand til at anfægte den effektivt. For det andet vil de registrerede blive særlig afhængige af, at de dataansvarlige anvender undtagelsen med omhu og kun i nødvendigt omfang. Selv om en registreret har ret til at klage til kommissæren over anvendelsen af undtagelsen eller anlægge søgsmål ved en domstol, vil den registrerede sandsynligvis ikke være bekendt med sine rettigheder og mangle midlerne til at gå til domstolene under omstændigheder, hvor der er behov for hurtig og præcis overholdelse af databeskyttelsesrettighederne. For det tredje vil den registrerede som immigrant sandsynligvis være i en sårbar situation. For det fjerde er dette ikke et abstrakt spørgsmål set i lyset af de sagsøgtes dokumentation for anvendelsen af immigrationsundtagelsen (se [4] ovenfor).
60. Mr Knight anfører, at der er en tæt parallel mellem den nuværende udfordring for immigrationsundtagelsen og [High Courts] begrundelse i Christian Institute [2016] UKSC 51. Ligesom i Christian Institute hævder han, at immigrationsundtagelsen er bred, bruger udefinerede termer, anvender en lav tærskel, er underlagt kontroller, der ikke fremgår tydeligt af bestemmelsen, og finder anvendelse på en meget bred vifte af sammenhænge og rettigheder. I modsætning til Christian Institute er der ingen offentligt tilgængelige vejledninger til immigrationsundtagelsen og endnu mindre en retlig status, som skal tages i betragtning."

73. Endvidere bemærker Databeskyttelsesrådet manglen på et retligt bindende instrument, som præciserer immigrationsundtagelsen med henblik på bedømmelsen af, om den i det væsentlige svarer til artikel 23 i databeskyttelsesforordningen og chartrets artikel 7 og 8. Samtidig mener Databeskyttelsesrådet, at Europa-Kommissionen er nødt til yderligere at godtgøre og dokumentere nødvendigheden og proportionaliteten af det brede personelle anvendelsesområde for immigrationsundtagelsen.

74. **Sammenfattende opfordrer Databeskyttelsesrådet Europa-Kommissionen til at indhente en status over førnævnte retssag, *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)*, og at få verificeret, eftersom denne afgørelse ikke er endelig (retskraftig), om den bliver stadfæstet eller ændret ved appelafgørelsen, idet den tager eventuelt nyt om denne sag i betragtning og gør rede for det i sin tilstrækkelighedsafgørelse. Databeskyttelsesrådet opfordrer også Europa-Kommissionen til at oplyse yderligere om nødvendigheden og proportionaliteten af immigrationsundtagelsen, navnlig for så vidt angår det brede personelle anvendelsesområde.**

75. **Samtidig opfordrer Databeskyttelsesrådet Europa-Kommissionen til at undersøge yderligere, om der findes eller påtænkes supplerende garantier i den britiske retlige ramme, f.eks. i form af retligt bindende instrumenter, som kan supplere immigrationsundtagelsen ved at øge dens forudsigelighed og styrke garantierne for de registrerede og samtidig sikre en bedre og hurtig vurdering og overvågning af kravene om nødvendighed og proportionalitet.**

3.1.2. Begrænsninger for videreoverførsel

76. Artikel 44 i GDPR bestemmer, at overførsel og videreoverførsel af personoplysninger kun må finde sted, hvis det beskyttelsesniveau, som fysiske personer garanteres i medfør af GDPR, ikke undermineres. Derfor skal personoplysninger, der overføres fra EØS til Det Forenede Kongerige på grundlag af tilstrækkelighedsafgørelsen, beskyttes på et niveau, der i det væsentlige svarer til det beskyttelsesniveau, som er sikret i henhold til EU's databeskyttelsesramme. **Dette betyder ikke blot, at den britiske lovgivning "i det væsentlige skal svare til" EU-lovgivningen med hensyn til behandling af personoplysninger, der overføres til Det Forenede Kongerige i henhold til afgørelsesudkastet, men også at de gældende regler i Det Forenede Kongerige med hensyn til videreoverførsel af disse personoplysninger til tredjelande skal sikre, at der fortsat ydes et beskyttelsesniveau, der i det væsentlige svarer til EU-niveauet.**

77. Det er derfor vigtigt, at eventuel videreoverførsel fra Det Forenede Kongerige til et andet tredjeland af personoplysninger fra EØS beskyttes korrekt med garantier eller udføres i overensstemmelse med reglerne om undtagelser[44] for at sikre kontinuiteten i den beskyttelse, som er sikret ved EU-retten. **Hvis denne beskyttelse ikke kan sikres, skal videreoverførsel af personoplysninger fra EØS ikke finde sted.**

78. Databeskyttelsesrådet anerkender, at Det Forenede Kongerige har gengivet størstedelen af kapitel V i GDPR i den britiske databeskyttelsesforordning (artikel 44-49) og i DPA 2018[45]. **Databeskyttelsesrådet har imidlertid identificeret visse aspekter af den britiske retlige ramme med**

[44] Se artikel 49 i den britiske databeskyttelsesforordning.
[45] Se §§ 17A, 17B, 17C og 18 i DPA 2018.

hensyn til videreoverførsel, som kan underminere beskyttelsesniveauet ved overførsel af personoplysninger fra EØS.

79. Den første udfordring, som Databeskyttelsesrådet har fundet, vedrører den anerkendelse som tilstrækkelig modtager, som Det Forenede Kongerige ifølge proceduren i DPA 2018 skal give tredjelande, internationale organisationer og områder[46]. Der vil nemlig kunne forekomme videreoverførsel fra Det Forenede Kongerige til tredjelande af personoplysninger fra EØS på grundlag af en eventuel fremtidig britisk "adequacy regulation" (tilstrækkelighedsregel)[47].

80. Som forklaret i betragtning 77 i afgørelsesudkastet har den britiske minister nærmere bestemt, efter samråd med ICO[48], beføjelse til at anerkende et tredjeland (eller et område eller en sektor i et tredjeland), en international organisation eller en beskrivelse af sådanne lande, områder, sektorer eller organisationer som enheder, der sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger. Den britiske minister skal ved vurderingen af beskyttelsesniveauets tilstrækkelighed tage de samme elementer i betragtning, som Europa-Kommissionen har pligt til at vurdere i henhold til artikel 45, stk. 2, litra a)-c), i GDPR sammenholdt med betragtning 104 i GDPR og bibeholdt EU-retspraksis. Dette betyder, at den relevante standard ved vurderingen af et tredjelands tilstrækkelige beskyttelsesniveau vil være, om det pågældende tredjeland sikrer et beskyttelsesniveau, der "i det væsentlige svarer" til det, der er sikret inden for Det Forenede Kongerige. Selv om Databeskyttelsesrådet noterer sig, at Det Forenede Kongerige i henhold til den britiske databeskyttelsesforordning kan anerkende bestemte områders databeskyttelsesniveau som tilstrækkeligt set i lyset af den britiske retlige ramme, ønsker Databeskyttelsesrådet at fremhæve, at sådanne områder måske endnu ikke er omfattet af en tilstrækkelighedsafgørelse udstedt af Europa-Kommissionen, som anerkender et beskyttelsesniveau, der "i det væsentlige svarer til" niveau, der garanteres i EU. Dette kan medføre potentielle risici i beskyttelsen af personoplysninger, der overføres fra EØS, især hvis den britiske databeskyttelsesramme fremover afviger fra EU's regelværk. Det skal bemærkes, at Domstolens centrale Schrems II-dom[49] i juli 2020 medførte ugyldiggørelse af afgørelsen om USA's værn om privatlivets fred, idet Domstolen fandt, at den amerikanske retlige ramme ikke kunne anses for at sikre et beskyttelsesniveau, der i det væsentlige svarede til EU-niveauet. Domstolens allerede afsagte domme, der anses for bibeholdt retspraksis i den britiske retlige ramme, er imidlertid muligvis ikke længere bindende for Det Forenede Kongerige, idet Det Forenede Kongerige navnlig har mulighed for at ændre bibeholdt EU-ret efter udløbet af passerelleperioden, og Supreme Court er ikke bundet af bibeholdt retspraksis fra EU overhovedet[50].

81. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til nøje at følge briternes arbejde med og kriterier for tilstrækkelighedsvurderingen for så vidt angår andre tredjelande, især med hensyn til tredjelande, der ikke anerkendes af EU som tilstrækkelige i henhold til databeskyttelsesforordningen. Når Europa-Kommissionen vurderer, at et givet tredjeland ikke sikrer et beskyttelsesniveau, der i det væsentlige svarer til det, der er sikret i EU, men som er fundet tilstrækkeligt af Det Forenede Kongerige, opfordrer Databeskyttelsesrådet Europa-Kommissionen**

[46] Se §17A i DPA 2018.
[47] Den britiske pendant til en tilstrækkelighedsafgørelse i henhold til GDPR.
[48] Se § 182(2) i DPA 2018. Se også aftalememorandum om ICO's rolle i forhold til nye britiske tilstrækkelighedsvurderinger, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.
[49] Se Schrems II.
[50] Se § 6, stk. 3-6, i EU (Withdrawal) Act 2018.

til at træffe enhver nødvendig foranstaltning, f.eks. en ændring af tilstrækkelighedsafgørelsen om Det Forenede Kongerige for at tilføje specifikke garantier for personoplysninger med oprindelse i EØS, og/eller at overveje at suspendere tilstrækkelighedsafgørelsen om Det Forenede Kongerige, hvis personoplysninger, der overføres fra EØS til Det Forenede Kongerige, videreoverføres til det pågældende tredjeland på grundlag af den britiske tilstrækkelighedsregel.

82. **Den anden udfordring** vedrører den kommende evaluering af de allerede eksisterende tilstrækkelighedsafgørelser, som Europa-Kommissionen har udstedt i henhold til direktiv 95/46/EF. Efter denne evaluering beslutter Europa-Kommissionen muligvis, at visse lande, som hidtil har været omfattet af en tilstrækkelighedsafgørelse, ikke længere yder et beskyttelsesniveau, der i det væsentlige svarer til EU-niveauet set i lyset af den nuværende EU-lovgivning og nyere retspraksis. Som fastsat i DPA 2018, Schedule 21, afsnit 4, har Det Forenede Kongerige imidlertid allerede anerkendt disse landes beskyttelsesniveau som tilstrækkeligt. Selvom den britiske minister skal gennemføre en evaluering af disse tilstrækkelighedskonstateringer inden for fire år, bemærker Europa-Kommissionen i sit afgørelsesudkast, at disse tilstrækkelighedskonstateringer ikke automatisk ophører, hvis den britiske minister ikke gennemfører den påkrævede evaluering inden fristen på fire år[51].

83. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til, når EU's gennemgang af de allerede eksisterende tilstrækkelighedsafgørelser er færdiggjort, at overvåge, om et land, som den ikke længere bedømmer til at sikre et tilstrækkeligt beskyttelsesniveau, stadig anerkendes som sådan af Det Forenede Kongerige. Hvis dette er tilfældet, opfordrer Databeskyttelsesrådet på grundlag af betragtning 277-280 i afgørelsesudkastet Europa-Kommissionen til at træffe enhver nødvendig foranstaltning til at afhjælpe situationen, f.eks. at ændre tilstrækkelighedsafgørelsen for at tilføje specifikke krav til personoplysninger med oprindelse i EØS og/eller suspendere tilstrækkelighedsafgørelsen, hvis personoplysninger, der overføres fra EØS til Det Forenede Kongerige, videreoverføres til det pågældende tredjeland. Databeskyttelsesrådet opfordrer Europa-Kommissionen til at fortsætte denne overvågning i hele gyldighedsperioden for tilstrækkelighedsafgørelsen om Det Forenede Kongerige.**

84. **Den tredje udfordring** vedrører videreoverførsel af personoplysninger fra EØS til utilstrækkelige lande baseret på de overførselsværktøjer, der er fastsat i artikel 46 og 47 i den britiske databeskyttelsesforordning. Selv om den britiske databeskyttelsesforordning fastsætter de samme overførselsværktøjer som GDPR, påpeger Databeskyttelsesrådet behovet for at sikre, at de garantier, de indeholder, sikrer en effektiv beskyttelse i tredjelandet, især i lyset af Schrems II-dommen.

85. Efter Schrems II-dommen, hvori Domstolen mindede om, at den beskyttelse, som EU yder personoplysninger, skal følge disse data overalt, har Databeskyttelsesrådet allerede vedtaget de første henstillinger om supplerende foranstaltninger[52] for at hjælpe dataeksportørerne, når det er påkrævet, med at sikre, at de registrerede tilbydes et beskyttelsesniveau, der i det væsentlige svarer til det, der garanteres inden for EU.

[51] Se betragtning 82 i afgørelsesudkastet.

[52] Se Databeskyttelsesrådets henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, vedtaget den 10. november 2020, som i øjeblikket er under færdigredigering efter en offentlig høring, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_da.pdf.

86. Ifølge Domstolen tilkommer det dataeksportørerne i hvert enkelt tilfælde og, hvor det er relevant, i samarbejde med dataimportøren i tredjelandet at undersøge, om lovgivningen eller praksis i tredjelandet påvirker effektiviteten af de fornødne garantier, der er fastsat i artikel 46 i GDPR om overførselsværktøjer[53]. Når det er tilfældet, skal dataeksportørerne træffe supplerende foranstaltninger, der kan afhjælpe disse huller i beskyttelsen og bringe den op på det niveau, som EU-retten kræver.

87. **Databeskyttelsesrådet opfordrer for at sikre kontinuiteten i beskyttelsen Europa-Kommissionen til i afgørelsesudkastet at forsikre om, at når overførselsværktøjer i henhold til artikel 46 og 47 i den britiske databeskyttelsesforordning anvendes af dataeksportører i Det Forenede Kongerige til videreoverførsel til et andet tredjeland af personoplysninger, der er overført fra EØS, skal disse dataeksportører i hvert enkelt tilfælde vurdere det pågældende tredjelands databeskyttelsesramme og, hvor det er nødvendigt, træffe passende foranstaltninger til at sikre den effektive overholdelse af de garantier, der ligger i det valgte overførselsværktøj, for at sikre, at beskyttelsesniveauet i det væsentlige svarer til det, der garanteres inden for EU. Databeskyttelsesrådet understreger, at uden disse forsikringer er der risiko for, at det beskyttelsesniveau, der i det væsentlige svarer til EU-niveauet, udvandes gennem videreoverførsel fra Det Forenede Kongerige.**

88. **Den fjerde udfordring** med videreoverførsler vedrører de internationale aftaler, der er blevet eller i fremtiden bliver indgået af Det Forenede Kongerige, og den direkte adgang til personoplysninger fra EØS, som myndigheder fra tredjelande, der har indgået sådanne aftaler, eventuelt får. Databeskyttelsesrådet er nemlig stærkt bekymret over den allerede indgåede CLOUD Act-aftale mellem Det Forenede Kongerige og USA, og Europa-Kommissionen anerkender denne udfordring, idet den understreger, at "*en mulig ikrafttrædelse af aftalen kan påvirke det beskyttelsesniveau, der er blevet vurderet i denne afgørelse*"[54]. Baseret på denne aftale, når den er trådt i kraft, vil personoplysninger, der overføres fra EØS til Det Forenede Kongerige i henhold til afgørelsesudkastet, nemlig blive omfattet af bestemmelserne i denne aftale, der fastsætter betingelser for amerikanske myndigheders direkte adgang, hvilket påvirker den britiske databeskyttelsesramme, herunder bestemmelserne om videreoverførsel. Som følge heraf kan beskyttelsesniveauet for personoplysninger, der er overført fra EØS, i væsentlig grad blive berørt og påvirket af bestemmelserne i den aftale, der er indgået med USA. Databeskyttelsesrådet bemærker i denne forbindelse, at Europa-Kommissionen i betragtning 153 i afgørelsesudkastet henviser til britiske myndigheders forklaringer uden at citere dem eller fremlægge konkrete skriftlige forsikringer eller løfter eller påpege specifikke retlige bestemmelser i britisk lov, som ville udmønte sådanne forklaringer.

89. Databeskyttelsesrådet har tidligere givet udtryk for disse betænkeligheder i et brev af 15. juni 2020 til Europa-Parlamentet[55]. Databeskyttelsesrådet fremhævede heri, at det på baggrund af *EU's regelværk inden for databeskyttelse og navnlig GDPR og retshåndhævelsesdirektivet* tager forbehold med hensyn til, hvorvidt aftalens garantier for adgang til personoplysninger i Det Forenede Kongerige vil gælde under bestemte omstændigheder, hvor amerikansk lov pålægger

[53] Se Schrems II, præmis 134.
[54] Se betragtning 153 i afgørelsesudkastet.
[55] Se Databeskyttelsesrådets svarbrev til Parlamentsmedlemmerne Sophie in't Veld og Moritz Körner om aftalen mellem Det Forenede Kongerige og USA i henhold til US Cloud Act, vedtaget den 15. juni 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

videregivelsesforpligtelser, og hvorvidt disse garantier er tilstrækkelige i forhold til EU-niveauet med henblik på ikke at underminere det beskyttelsesniveau, der er sikret i EU.

90. Endvidere kan bestemmelserne i CLOUD Act-aftalen mellem Det Forenede Kongerige og USA i væsentlig grad berøre de materielle og processuelle betingelser, der gælder for amerikanske myndigheders direkte adgang til personoplysninger, der befinder sig hos dataansvarlige eller databehandlere i Det Forenede Kongerige, og dermed påvirke det beskyttelsesniveau, der er garanteret efter britisk ret. For at sikre et beskyttelsesniveau, der i det væsentlige svarer til det, der er sikret efter EU-retten, er det f.eks. "*afgørende, at garantierne i henhold til en sådan aftale omfatter en obligatorisk retslig forhåndstilladelse som en afgørende garanti for adgang til metadata og indholdsdata. På basis af sin foreløbige vurdering kan Databeskyttelsesrådet, omend det bemærker, at aftalen henviser til anvendelsen af national ret, ikke finde en så klar bestemmelse i aftalen mellem Det Forenede Kongerige og USA*"[56].

91. Mens Europa-Kommissionen fremhæver, at data, der indhentes i henhold til denne aftale, vil være omfattet af beskyttelsesforanstaltninger, der svarer til de specifikke garantier, der er fastsat ved den såkaldte "paraplyaftale mellem EU og USA", er Databeskyttelsesrådet bekymret for, om indarbejdelsen af disse garantier i CLOUD Act-aftalen mellem Det Forenede Kongerige og USA alene i form af en henvisning, der finder tilsvarende anvendelse, vil leve op til kriterierne om klare, præcise og tilgængelige regler for så vidt angår adgangen til personoplysninger og i tilstrækkelig grad underbygge, at disse garantier er effektive og kan håndhæves efter britisk ret.

92. **Databeskyttelsesrådet henstiller derfor til Europa-Kommissionen, at den klarlægger, hvordan og på grundlag af hvilket retligt instrument det kan sikres, at sådanne beskyttelsesforanstaltninger, der svarer til de specifikke garantier i paraplyaftalen mellem EU og USAn, kan få virkning og være bindende efter britisk ret.**

93. Databeskyttelsesrådet bemærker også, at bestemmelserne i CLOUD Act-aftalen mellem Det Forenede Kongerige og USA, sammenholdt med § 3 i US CLOUD Act[57], vækker tvivl om den reelle anvendelse af de garantier, der gives i aftalen for de amerikanske retshåndhævende myndigheders adgang til personoplysninger i Det Forenede Kongerige, som behandles af udbydere af elektroniske kommunikationstjenester eller onlinetjenester (herefter "serviceudbydere"), som er omfattet af USA's jurisdiktion. Hvis en sådan serviceudbyder, der befinder sig i Det Forenede Kongerige, er omfattet af amerikansk lov (f.eks. fordi der er tale om et datterselskab af et amerikansk selskab), er det nemlig stadig ikke bekræftet, om de amerikanske myndigheder vil være forpligtet til at anvende CLOUD Act-aftalen mellem Det Forenede Kongerige og USA for at indhente sådanne data. Idet Europa-Kommissionen i afgørelsesudkastet påpeger, at der "*vil blive lagt særlig vægt på anvendelsen og tilpasningen af paraplyaftalens beskyttelse af den specifikke type overførsler, der er omfattet af aftalen mellem Det Forenede Kongerige og USA*", understreger Databeskyttelsesrådet på grundlag af sin foreløbige vurdering, at det er uklart, om de garantier, der er fastsat i CLOUD Act-aftalen mellem Det Forenede Kongerige og USA, og derfor den, der gives i paraplyaftalen mellem EU og USA, vil finde anvendelse på alle eventuelle anmodninger fra amerikanske myndigheder om adgang til data i Det Forenede Kongerige i henhold til US CLOUD Act.

94. Der kan komme andre internationale aftaler med eller forpligtelser over for tredjelande, som Det Forenede Kongerige muligvis vil indgå i fremtiden, og disse vil finde anvendelse på personoplysninger, der er overført fra EØS til Det Forenede Kongerige i henhold til

[56] Se Databeskyttelsesrådets førnævnte brev.
[57] Se US CLOUD Act, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

afgørelsesudkastet[58]. Afhængigt af bestemmelserne i disse aftaler og anvendelsen af specifikke beskyttelsesklausuler kan disse internationale aftaler, ved at berøre den britiske databeskyttelsesramme, også få en betydelig indflydelse på de materielle og processuelle betingelser for tredjelandes myndigheders adgang til personoplysninger i Det Forenede Kongerige. Dette er især tilfældet med udkastet til anden tillægsprotokol til Europarådets konvention om IT-kriminalitet ("Budapestkonventionen"), som denne konventions parter, herunder flere ikke-EU-lande, i øjeblikket forhandler om. Protokoludkastet indeholder nemlig klausuler, som kan aktiveres af parterne efter eget skøn, f.eks. vedrørende tilladelse til at give adgang til indholdsdata eller ikke. Mens alle EU-medlemsstater vil aktivere klausulerne i overensstemmelse med EU's databeskyttelsesregler, er der ikke givet nogen garanti med hensyn til Det Forenede Kongerige, som i væsentlig grad kan afvige fra det beskyttelsesniveau, der til den tid sikres inden for EU. Et andet eksempel på ovennævnte udfordringer er den første britiske handelsaftale efter Brexit, nemlig aftalen mellem Det Forenede Kongerige og Japan om et omfattende økonomisk partnerskab[59] ("CEPA"), som trådte i kraft den 1. januar 2021[60], og som indeholder bestemmelser om personoplysninger[61]. Databeskyttelsesrådet bemærker endvidere, at Det Forenede Kongerige også officielt den 1. februar 2021 bekendtgjorde sin anmodning om optagelse i det omfattende og progressive grænseoverskridende Stillehavspartnerskab ("CPTPP"), som omfatter Stillehavspartnerskabsaftalen ("TPP")[62].

95. Databeskyttelsesrådet bemærker, at ud over CLOUD Act-aftalen mellem Det Forenede Kongerige og USA er de ovennævnte internationale aftaler ikke behandlet i afgørelsesudkastet.

96. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til:**

- **at undersøge samspillet mellem den britiske databeskyttelsesramme og landets internationale forpligtelser ud over CLOUD Act-aftalen mellem Det Forenede Kongerige og USA, navnlig for at sikre kontinuiteten i beskyttelsesniveauet, når personoplysninger, der er overført fra EØS til Det Forenede Kongerige, videreoverføres til andre tredjelande på grundlag af tilstrækkelighedsafgørelsen omDet Forenede Kongerige, og at fortsætte sit tilsyn og om nødvendigt at skride ind, hvis indgåelsen af internationale aftaler mellem Det Forenede Kongerige og tredjelande risikerer at underminere det niveau for beskyttelse af personoplysninger, der er sikret i EU**

- **at give Databeskyttelsesrådet de britiske myndigheders skriftlige forpligtelser og identificere specifikke bestemmelser i britisk ret i forbindelse med forklaringen om den eventuelle**

[58] Se afsnit 2.3.3 ovenfor.

[59] Se UK-Japan: Agreement for a Comprehensive Economic Partnership [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Se den britiske regerings vejledning om britiske handelsaftaler med ikke-EU-lande, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] I henhold til artikel 8.80, stk. 5, i CEPA forpligter parterne sig til at tilskynde til udviklingen af mekanismer til fremme af forenelighed mellem deres forskellige retlige tilgange til beskyttelse af personoplysninger. I henhold til artikel 8.84 forpligter parterne sig til at undlade at forbyde eller begrænse den grænseoverskridende elektroniske overførsel af information, herunder personoplysninger, når det sker som led i forretningsaktiviteter, der foretages af en person, der er omfattet som omhandlet i CEPA.

[62] I henhold til artikel 14.11, stk. 2, i TPP tillader hver part grænseoverskridende elektronisk overførsel af information, herunder personoplysninger, når det sker som led i forretningsaktiviteter, der foretages af en person, der er omfattet.

anvendelse og gennemførelse af CLOUD Act-aftalen mellem Det Forenede Kongerige og USA, jf. betragtning 153 i afgørelsesudkastet

- **i denne forbindelse at overvåge, om CLOUD Act-aftalen mellem Det Forenede Kongerige og USA sikrer passende supplerende garantier under hensyntagen til følsomhedsniveauet for de berørte datakategorier og de unikke krav til serviceudbydernes, frem for myndighedernes, direkte overførsel af elektronisk bevismateriale, idet den også vurderer de garantier, der kan sikres i kraft af en hensigtsmæssig gennemførelse af tilpasningen af paraplyaftalen mellem EU og USAn**

- **at vurdere virkningen af og de potentielle risici ved bestemmelserne om personoplysninger i internationale aftaler, som for nylig er blevet indgået af Det Forenede Kongerige, f.eks. CEPA.**

97. **Den femte udfordring**, som Databeskyttelsesrådet har fundet, vedrører anvendelsen af undtagelser for overførsel af personoplysninger til et tredjeland. Selv om de tilgængelige undtagelser ifølge den britiske databeskyttelsesforordning er de samme som dem, der er fastsat i GDPR, er det vigtigt, at ICO anlægger og fortsat vil anlægge en fortolkning i henseende til anvendelsen af disse undtagelser, som stemmer overens med Databeskyttelsesrådets fortolkning. Hvis dette ikke er tilfældet, eller hvis Det Forenede Kongerige afviger fra denne fortolkning i fremtiden, vil der være risiko for, at beskyttelsesniveauet for data, der overføres fra EØS til tredjelande via Det Forenede Kongerige, undermineres.

98. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til som led i sin tilsynsopgave specifikt at kontrollere, om den britiske fortolkning af anvendelsen af undtagelser forbliver i tråd med EU's fortolkning. Hvis Det Forenede Kongerige imidlertid følger en anden fortolkning af anvendelsen af undtagelser til skade for beskyttelsesniveauet, er det afgørende, at Europa-Kommissionen træffer de nødvendige foranstaltninger ved at ændre tilstrækkelighedsafgørelsen for at sikre sig, at beskyttelsesniveauet for personoplysninger fra EØS, der overføres til Det Forenede Kongerige, således ikke undermineres, når disse data videreoverføres fra Det Forenede Kongerige til tredjelande på basis af en anden fortolkning af undtagelserne.**

99. **Den sjette** og sidste **udfordring** i dette afsnit omhandler fraværet i den britiske databeskyttelsesramme af de beskyttelsesforanstaltninger, der er fastsat i artikel 48 i GDPR.

100. Europa-Kommissionen klarlægger nemlig i sit afgørelsesudkast, at i mangel af tilstrækkelighedsregler eller de fornødne garantier kan en overførsel kun finde sted på grundlag af undtagelser, der er fastsat i artikel 49 i den britiske databeskyttelsesforordning, "*med undtagelse af artikel 48 i forordning (EU) 2016/679, som Det Forenede Kongerige ikke har valgt at indarbejde i den britiske databeskyttelsesforordning*".[63] Når der ikke findes en bestemmelse i den britiske databeskyttelsesramme, som i det væsentlige svarer til artikel 48 i GDPR, vedrørende overførsler eller videregivelser efter en retsafgørelse eller en administrativ afgørelse truffet i et andet tredjeland, kan det give anledning til retsusikkerhed med hensyn til, om beskyttelsesniveauet for personoplysninger, der er overført fra EØS til Det Forenede Kongerige i henhold til afgørelsesudkastet, bliver berørt i væsentlig grad.

101. Databeskyttelsesrådet har i sin tilstrækkelighedsreference påpeget med hensyn til videreoverførsler, at "*[v]idereoverførsel af personoplysninger fra den oprindelige modtager af den oprindelige overførsel af oplysninger bør kun være tilladt, når den efterfølgende modtager (dvs. modtageren af videreoverførslen) også er underlagt regler (herunder kontraktbestemmelser), som giver et*

[63] Se fodnote 78 i afgørelsesudkastet.

tilstrækkeligt beskyttelsesniveau, og følger de relevante instrukser ved behandling af oplysningerne på den dataansvarliges vegne"[64]. Desuden understreger Databeskyttelsesrådet, at "*[d]et påhviler den oprindelige modtager af de oplysninger, som overføres fra EU, at sikre, at der stilles passende garantier for oplysningernes videreoverførsel, når der ikke foreligger en afgørelse om beskyttelsesniveauets tilstrækkelighed*. *Sådanne videreoverførsler af personoplysninger må kun finde sted til begrænsede og specifikke formål, og så længe der er et retsgrundlag for behandlingen*"[65]. Som en del af kapitel V i GDPR skal artikel 48 tages fuldt ud i betragtning ved vurderingen af, om den britiske retlige ramme sikrer et beskyttelsesniveau i denne henseende, som i det væsentlige svarer til EU-niveauet[66].

102. Databeskyttelsesrådet understreger i denne forbindelse Domstolens retspraksis vedrørende risikoen for misbrug og ulovlig adgang til og anvendelse af data, navnlig at "*[h]vad angår det inden for Unionen sikrede beskyttelsesniveau for frihedsrettigheder og grundlæggende rettigheder fremgår det af Domstolens faste praksis, at en EU-lovgivning, som indebærer et indgreb i de ved chartrets artikel 7 og 8 sikrede grundlæggende rettigheder, skal fastsætte klare og præcise regler, som regulerer rækkevidden og anvendelsen af en foranstaltning og opstiller en række mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres oplysninger mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse oplysninger. Behovet for at råde over sådanne garantier er så meget desto større, når personoplysningerne undergives automatisk databehandling, og der eksisterer en betydelig risiko for ulovlig adgang til disse oplysninger*"[67].

103. Databeskyttelsesrådet bemærker i denne forbindelse, at den britiske databeskyttelsesramme, baseret på oplysningerne i afgørelsesudkastet, ikke klart bestemmer, at enhver dom afsagt af en domstol eller ret og enhver afgørelse truffet af en administrativ myndighed i et tredjeland, der kræver, at en dataansvarlig eller en databehandler overfører eller videregiver personoplysninger, kun kan anerkendes eller håndhæves på nogen måde, hvis den bygger på en gældende international aftale mellem det anmodende tredjeland og Det Forenede Kongerige. Artikel 48 i GDPR er en væsentlig bestemmelse i kapitel V i GDPR, da den kræver, at overførsel eller videregivelse af personoplysninger efter en retsafgørelse eller administrativ afgørelse truffet i et tredjeland kun kan anerkendes eller håndhæves, hvis den bygger på en gældende international aftale mellem det anmodende tredjeland og Unionen eller en medlemsstat, uden at det berører andre grunde til overførsel i henhold til kapitel V i GDPR. Databeskyttelsesrådet minder nemlig om, at "*en anmodning fra en udenlandsk myndighed ikke i sig selv udgør et retsgrundlag for overførslen*. *Anmodningen kan kun anerkendes, "hvis den er baseret på en gældende international aftale som en traktat om gensidig retshjælp mellem det anmodende tredjeland og Unionen eller en medlemsstat*""[68]. Det er derfor afgørende, at der i britisk lov findes bestemmelser, der i det væsentlige er tilsvarende.

[64] Se WP254 rev.01, s. 6.
[65] Se WP254 rev.01, s. 6.
[66] Se artikel 44 i GDPR, sidste punktum, især: "*Alle bestemmelserne i dette kapitel anvendes for at sikre, at det beskyttelsesniveau, som fysiske personer garanteres i medfør af denne forordning, ikke undermineres.*"
[67] Se Schrems I, præmis 91.
[68] Se bilaget til "Fælles svar fra Databeskyttelsesrådet og EDPS til LIBE-udvalget om konsekvenserne af den amerikanske cloudlovgivning for den europæiske retlige ramme vedrørende beskyttelse af personoplysninger", der blev vedtaget den 10. juli 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

104. I udkastet til afgørelse henviser Europa-Kommissionen til forklaringer fra de britiske myndigheder om, at en udenlandsk dom, hvori der anmodes om oplysninger, i henhold til sædvaneret eller lovgivningen ikke kan fuldbyrdes i Det Forenede Kongerige uden en international aftale, og at overførsel af oplysninger efter anmodning fra en udenlandsk domstol eller administrativ myndighed kræver et overførselsredskab såsom en forordning om tilstrækkeligheden af beskyttelsesniveauet eller passende garantier, medmindre en undtagelse i henhold til artikel 49 i den britiske databeskyttelsesforordning finder anvendelse. Databeskyttelsesrådet har imidlertid ikke modtaget udvekslingerne mellem Europa-Kommissionen og de britiske myndigheder[69] i denne henseende og kan derfor ikke foretage en analyse og uafhængig vurdering af, om de garantier, som de britiske myndigheder giver, er tilstrækkelige til at sikre et i det væsentlige tilsvarende beskyttelsesniveau i forhold til de garantier, der er fastsat i artikel 48 i GDPR.

105. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til at give yderligere forsikringer og specifikke henvisninger til den britiske lovgivning, som sikrer, at det beskyttelsesniveau, der garanteres af den britiske retlige ramme, i det væsentlige svarer til det beskyttelsesniveau, der garanteres i EØS. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at fremlægge skriftlige forklaringer og tilsagn fra de britiske myndigheder med hensyn til gennemførelsen af beskyttelsesforanstaltninger, der i det væsentlige svarer til dem, som er fastsat i artikel 48 i databeskyttelsesforordningen.**

106. **Databeskyttelsesrådet mener, at identifikation af de bestemmelser i den britiske lovgivning, der sikrer et i det væsentlige tilsvarende beskyttelsesniveau i forhold til de garantier, der er fastsat i artikel 48 i databeskyttelsesforordningen, er så meget desto vigtigere på baggrund af de betænkeligheder, der tidligere er blevet fremsat vedrørende anmodninger om adgang til data i Det Forenede Kongerige fra USA's eller andre tredjelandes myndigheder, og i betragtning af at personoplysninger i henhold til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet kan overføres fra EØS til Det Forenede Kongerige uden yderligere garanti eller bindende tilsagn fra modtageren i forbindelse med anmodninger om adgang til oplysninger fra andre tredjelandes myndigheder.**

3.2. Procedure- og håndhævelsesmekanismer

107. På grundlag af de kriterier, der er fastsat i tilstrækkelighedsreferencen, har Databeskyttelsesrådet analyseret følgende aspekter af den britiske databeskyttelsesramme, som er omfattet af udkastet til afgørelse: tilstedeværelse af en velfungerende, uafhængig tilsynsmyndighed, tilstedeværelse af en databeskyttelsesramme, som er i overensstemmelse med EU's ramme, og et system med adgang til passende retsmidler, der giver borgere i EU mulighed for at udøve deres rettigheder og anlægge sager uden at støde på besværlige forhindringer for administrativ og retslig prøvelse.

3.2.1 Kompetent uafhængig tilsynsmyndighed

108. Databeskyttelsesrådet bifalder Europa-Kommissionens bestræbelser på at foretage en grundig undersøgelse af Det Forenede Kongeriges tilsynsmyndigheds oprettelse, funktion og beføjelser i kapitel 2.6 i udkastet til afgørelse. I Det Forenede Kongerige har informationskommissæren (i det følgende benævnt "IC") til opgave at føre tilsyn med og håndhæve overholdelsen af den britiske databeskyttelsesforordning og DPA 2018. I henhold til Schedule 12 i DPA 2018 er IC en "Corporation Sole", dvs. en særskilt juridisk enhed, der varetages af én udnævnt person med støtte fra et kontor, informationskommissæren.

[69] Se fodnote 78 i afgørelsesudkastet.

109. Med hensyn til IC's uafhængighed understreger Databeskyttelsesrådet, at artikel 51 i den britiske databeskyttelsesforordning ikke indeholder den udtrykkelige præcisering af, at IC er en uafhængig offentlig myndighed, som det fremgår af artikel 51 i GDPR vedrørende tilsynsmyndigheder. Databeskyttelsesrådet anerkender dog, at den britiske databeskyttelsesforordning i artikel 52 på tilsvarende vis afspejler de relevante regler vedrørende uafhængighed, som fastsat i artikel 52, stk. 1-3, i GDPR.

110. Databeskyttelsesrådet påpeger endvidere, at artikel 52 i den britiske databeskyttelsesforordning ikke indeholder forpligtelser, der modsvarer artikel 52, stk. 4-6, i GDPR, som udtrykkeligt sikrer, at den pågældende tilsynsmyndighed tildeles de ressourcer, der er nødvendige for effektivt at kunne udføre sine opgaver og udøve sine beføjelser. Databeskyttelsesrådet anerkender dog, at DPA 2018 indeholder bestemmelser, der har til formål at sikre en passende finansiering af ICO[70] samt den omstændighed, at ICO i øjeblikket er en af de største tilsynsmyndigheder sammenlignet med tilsynsmyndigheder i EU/EØS. Da en løbende tildeling af passende ressourcer, navnlig med hensyn til personale og budget[71], er af afgørende betydning for at sikre, at en tilsynsmyndighed fungerer korrekt og kan udføre alle sine opgaver, hvilket også for nylig af Europa-Parlamentet er blevet påpeget som afgørende[72], finder Databeskyttelsesrådet det vigtigt at være særlig opmærksom på den fremtidige udvikling på dette område.

111. **Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at observere udviklingen i tildelingen af ressourcer til ICO, for at afdække forhold, som ville være til skade for en korrekt udførelse af ICO's opgaver.**

3.2.2. Tilstedeværelse af en databeskyttelsesramme, som er i overensstemmelse med EU's ramme

112. Udkastet til afgørelse indeholder en omfattende undersøgelse af de beføjelser, som er tildelt ICO i henhold til artikel 58 i den britiske databeskyttelsesforordning og DPA 2018 med henblik på at sikre overvågning og håndhævelse af lovgivningen. Databeskyttelsesrådet anerkender, at artikel 58 i den britiske databeskyttelsesforordning nøje afspejler de tilsvarende regler vedrørende tilsynsmyndighedernes beføjelser, som er fastsat i artikel 58 i databeskyttelsesforordningen. Med hensyn til beføjelsen til at pålægge administrative bøder afhængigt af omstændighederne i hver enkelt sag indeholder artikel 83 i den britiske databeskyttelsesforordning bestemmelser og maksimumsbeløb, der svarer til dem, som er fastsat i artikel 83 i databeskyttelsesforordningen. Databeskyttelsesrådet mener derfor, at den britiske retlige ramme på området i øjeblikket er i overensstemmelse med de standarder, der er fastsat i den relevante EU-lovgivning. I den forbindelse fremhæver Databeskyttelsesrådet dog, at tilstedeværelsen af *effektive* sanktioner spiller en vigtig rolle for at sikre overholdelse af reglerne[73].

113. **På baggrund af ovenstående opfordrer Databeskyttelsesrådet Europa-Kommissionen til at overvåge effektiviteten af de sanktioner og relevante retsmidler, der er fastsat i den britiske databeskyttelsesramme.**

[70] Se §§ 137, 138 og 182 og Schedule 12, afsnit 9, i DPA 2018.
[71] Se WP 254 rev.01, s. 7.
[72] Europa-Parlamentets beslutning af 25. marts 2021 om Kommissionens evalueringsrapport om gennemførelsen af den generelle forordning om databeskyttelse to år efter dens anvendelse, punkt 15 https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.html.
[73] Se WP 254 rev.01, s. 7.

3.2.3. Databeskyttelsessystemet skal støtte og hjælpe de registrerede med at udøve deres rettigheder og omfatte passende søgsmålsmekanismer

114. En effektiv tilsynsmekanisme, der muliggør uafhængig undersøgelse af klager med henblik på at identificere og straffe overtrædelser af registreredes rettigheder i praksis, samt en effektiv administrativ og retslig klageadgang (herunder skadeserstatning som følge af ulovlig behandling af registreredes personoplysninger), er centrale elementer i vurderingen af, om et databeskyttelsessystem giver et tilstrækkeligt beskyttelsesniveau.

115. Databeskyttelsesrådet bifalder, at ICO fremlægger omfattende oplysninger og retningslinjer på sin hjemmeside med det formål at øge dataansvarliges og databehandleres kendskab til deres forpligtelser og opgaver og som hjælp til at oplyse registrerede om deres rettigheder vedrørende personoplysninger og deres individuelle rettigheder i henhold til den britiske databeskyttelsesforordning og DPA 2018.

116. **Uanset den nuværende situation opfordrer Databeskyttelsesrådet Europa-Kommissionen til løbende at observere den støtte, som ICO yder specifikt til enkeltpersoner, hvis personoplysninger er blevet overført til Det Forenede Kongerige i henhold til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, for at hjælpe dem med at udøve deres rettigheder i henhold til de britiske databeskyttelsesregler.**

4. ADGANG TIL OG BRUG AF PERSONOPLYSNINGER OVERFØRT FRA EU AF OFFENTLIGE MYNDIGHEDER I DET FORENEDE KONGERIGE

4.1. De britiske myndigheders adgang til og brug af personoplysninger med henblik på retshåndhævelse på det strafferetlige område

4.1.1. Retsgrundlag og gældende begrænsninger/garantier

117. Med hensyn til den vurdering, som Europa-Kommissionen har foretaget og dokumenteret i betragtning 132, og i forlængelse af udkastet til afgørelse **om adgang med henblik på retshåndhævelse**, fremlægger Europa-Kommissionen nuancerede og detaljerede oplysninger og når generelt frem til forståelige konklusioner. Databeskyttelsesrådet undlader derfor at gengive de fleste af de faktuelle konklusioner og vurderinger i denne udtalelse. Der er imidlertid visse tilfælde, hvor gengivelsen af de faktiske omstændigheder eller forklaringen af konklusionerne ikke er tilstrækkelig til, at Databeskyttelsesrådet kan tilslutte sig dem.

4.1.1.1. Brug af samtykke

118. Databeskyttelsesrådet noterer sig, at Europa-Kommissionen i fodnote 184 i udkastet til afgørelse[74] anfører, at **brug af samtykke** ikke er relevant i et tilstrækkelighedsscenarie, da oplysningerne ved overførelse ikke indhentes af en retshåndhævende myndighed i Det Forenede Kongerige direkte fra en registreret på grundlag af samtykke. Derfor har Europa-Kommissionen ikke foretaget en vurdering af brugen af samtykke som retsgrundlag i forbindelse med politiarbejde.

119. I denne forbindelse minder Databeskyttelsesrådet om, at artikel 45, stk. 2, litra a), i GDPR kræver en vurdering af en bred vifte af elementer, der ikke er begrænset til overførselssituationen, herunder

[74] Se s. 37 i udkastet til afgørelse.

"*retsstatsprincippet, respekt for menneskerettighederne og de grundlæggende frihedsrettigheder, relevant lovgivning, både generel og sektorbestemt, herunder [...] strafferet*".

120. Databeskyttelsesrådet bemærker på grundlag af oplysningerne fra Europa-Kommissionen i betragtning 38 i udkastet til gennemførelsesafgørelse i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2016/680 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Det Forenede Kongerige (i det følgende benævnt "udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet"), at anvendelsen af samtykke som fastsat i den britiske ordning i forbindelse med retshåndhævelse altid vil kræve, at der anvendes et retsgrundlag. Det betyder, at selvom politiet har lovfæstede beføjelser til at behandle oplysningerne med henblik på en efterforskning, kan politiet under visse særlige omstændigheder (f.eks. indsamling af en DNA-prøve) anse det for hensigtsmæssigt at anmode den registrerede om samtykke.

121. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet at medtage sin analyse af den mulige brug af samtykke i forbindelse med retshåndhævelse, jf. udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet.**

4.1.1.2. Ransagningskendelser og editionskendelser

122. Databeskyttelsesrådet har ingen bemærkninger til politiets indhentning af bevismateriale ved ransagningskendelser og editionskendelser generelt, men det fremgår af betragtning 136 i udkastet til afgørelse, at Europa-Kommissionen i sine betragtninger vedrørende adgang til retshåndhævelse har fokuseret på politiet, og at andre retshåndhævende myndigheders behandling af personoplysninger i mindre grad er blevet undersøgt.

123. Eksempel: Det Forenede Kongeriges Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement[75], hvor det på s. 11 foreslås, at **National Crime Agency** (herefter benævnt "NCA") kan anses som retshåndhævende myndighed af særlig interesse, som blandt andet har bredere efterretningsopgaver. NCA beskriver sin opgave som at samle efterretninger fra en række kilder med henblik på at maksimere mulighederne for analyse, vurdering og taktiske tiltag, herunder fra teknisk aflytning af kommunikation, retshåndhævelsespartnere i Det Forenede Kongerige og oversøiske lande, sikkerheds- og efterretningstjenester[76]. NCA er også en af de vigtigste dialogpartnere for de internationale partnere inden for retshåndhævelse og spiller en central rolle i udvekslingen af kriminalefterretninger[77].

---

[75] Se Det Forenede Kongeriges Government, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, af 13. marts 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Se NCA's hjemmeside, "Intelligence: enhancing the picture of serious organised crime affecting the UK", https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Ikke alle efterretninger, der behandles af NCA, er personoplysninger, men en væsentlig del af dem kan være det. De aktiviteter, der beskrives her, adskiller sig fra de aktiviteter, der generelt udføres af politiet, og derfor vil en vurdering af de retshåndhævende myndigheders adgang til personoplysninger i Det Forenede Kongerige være mangelfuld uden en grundig vurdering af NCA's aktiviteter. Det forekommer rimeligt at sikre, at principperne for databeskyttelse tillægges samme betydning hos alle relevante retshåndhævende myndigheder, og derfor er det vigtigt at have fokus på en særligt datadrevet myndighed som NCA. Derudover fortsættes forklaringen under "et kig på fremtiden", "*[v]i undersøger hele tiden nye muligheder for at samle, udvikle og udvide kapaciteten generelt for at øge både kvantitet og kvalitet i de efterretninger, der kan stilles til rådighed både i Det Forenede Kongerige og i udlandet*". *"Som et led heri udvikler vi den nye National Data*

124. Databeskyttelsesrådet noterer sig endvidere, at regeringens kommunikationskontor (i det følgende benævnt "GCHQ"), hvis aktiviteter typisk hører under Part 4 i DPA 2018, dvs. statens sikkerhed, også indtager en aktiv rolle med hensyn til at mindske den samfundsmæssige og økonomiske skade, som grov og organiseret kriminalitet forårsager for Det Forenede Kongerige, i tæt samarbejde med indenrigsministeriet, NCA, HM Revenue and Customs ("HMRC") samt andre ministerier[78]. Aktiviteterne vedrører bekæmpelse af seksuelt misbrug af børn, svig, andre former for økonomisk kriminalitet, herunder hvidvaskning af penge, kriminel brug af teknologi, internetkriminalitet, organiseret indvandringskriminalitet, herunder menneskehandel samt smugling af narkotika og skydevåben og andre ulovlige smugleraktiviteter.

125. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til at supplere sin analyse med en analyse af de enheder, der arbejder med retshåndhævelse, og som i det daglige arbejde ser ud til særligt at arbejde med indsamling og analyse af data, herunder personoplysninger, og her især NCA. Derudover opfordrer Databeskyttelsesrådet Europa-Kommissionen til at se nærmere på enheder som GCHQ, hvis aktiviteter både vedrører retshåndhævelse og statens sikkerhed, og den retlige ramme, der gælder for disse enheder ved behandling af personoplysninger.**

4.1.1.3. Undersøgelsesbeføjelser med henblik på retshåndhævelse

126. I henhold til kapitel 4 i tilstrækkelighedsreferencen "Væsentlige garantier i tredjelande for adgang til retshåndhævelse og statens sikkerhed med henblik på at begrænse indgreb i grundlæggende rettigheder" påpeger Databeskyttelsesrådet, at *"[i] denne sammenhæng fremsatte retten også en kritisk bemærkning om, at den tidligere safe harbor-afgørelse "ikke indeholdt nogen konklusion om, at der i USA findes regler vedtaget af staten, der har til formål at begrænse indgreb i de grundlæggende rettigheder for de personer, hvis data overføres fra Den Europæiske Union til USA, **indgreb, som de statslige enheder i landet ville være berettigede til at foretage på et legitimt grundlag** såsom den statens sikkerhed""*[79]. I tilstrækkelighedsreferencen anfører Databeskyttelsesrådet, at **alle tredjelande skal overholde de fire væsentlige europæiske garantier**[80] **for adgang til data, uanset om der er tale om** statens sikkerhed eller **retshåndhævelse**, **for at garantierne kan betragtes som tilstrækkelige**, navnlig **skal nødvendigheden og proportionaliteten i det legitime grundlag kunne påvises**.

127. I dette afsnit af udkastet til afgørelse konkluderer Europa-Kommissionen (betragtning 139), at *"eftersom de undersøgelsesbeføjelser, der er fastsat i IPA 2016, er de samme som dem, der er til rådighed for nationale sikkerhedsagenturer, behandles de betingelser, begrænsninger og garantier, der gælder for sådanne beføjelser, nærmere i afsnittet om britiske offentlige myndigheders adgang til og brug af personoplysninger til nationale sikkerhedsformål"*. I forbindelse med anvendelsen af nødvendigheds- og proportionalitetstesten på den del af medlemsstaternes lovgivning, der gør det muligt for offentlige myndigheder at lagre og få adgang til personoplysninger, følger det imidlertid

---

Exploitation Capability med brug af de beføjelser, som tildeles til myndigheden i henhold til Crime and Courts Act, for at kunne sammenkøre, tilgå og bruge data, der ligger hos forskellige myndigheder." [...] "*På den måde øger vi vores agilitet og fleksibilitet med henblik på at imødegå nye trusler og arbejde proaktivt, når vi indsamler og analyserer oplysninger og efterretninger vedrørende nye trusler, så vi kan gribe ind, før truslerne bliver til realitet*."

[78] Se GCHQ's hjemmeside, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime.

[79] Se WP254 rev.01, s. 9.

[80] Se Databeskyttelsesrådets anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger.

af EU-Domstolens retspraksis, at de legitime grundlag, såsom statens sikkerhed eller bekæmpelse af grov kriminalitet, varierer, og at bestemte typer af indgreb derfor i nogle tilfælde kan begrundes og i andre ikke[81].

128. **Databeskyttelsesrådet ønsker derfor en konkret vurdering inden for rammerne af afgørelsen af nødvendigheden og proportionaliteten i de betingelser, begrænsninger og garantier, der er beskrevet i betragtning 174 ff. — et afsnit om foranstaltninger vedrørende nationale sikkerhedsmål — når det drejer sig om at anvende disse betingelser, begrænsninger og garantier i forbindelse med en foranstaltning, der vedrører retshåndhævelse. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til yderligere at præcisere, om den beskrevne lagring af personoplysninger og adgangen hertil med henblik på retshåndhævelse er tilstrækkeligt begrænset til at sikre et beskyttelsesniveau, der i det væsentlige svarer til det, der garanteres i EU.**

4.1.2. Videreanvendelse af de oplysninger, der er indsamlet til retshåndhævelsesformål (betragtning 140-154)

129. Databeskyttelsesrådet bemærker, at den britiske databeskyttelsesramme indeholder garantier og begrænsninger svarende til dem, der er fastsat i EU-retten i forbindelse med videreanvendelse af de oplysninger, der indsamles med henblik på retshåndhævelse.

4.1.2.1. Videreanvendelse til andre retshåndhævelsesformål

130. I DPA 2018 fastsættes det ganske rigtigt, at personoplysninger, der indsamles af en kompetent myndighed med henblik på retshåndhævelse, kan viderebehandles (enten af den oprindelige dataansvarlige eller af en anden dataansvarlig) med henblik på ethvert andet retshåndhævelsesformål, forudsat at den dataansvarlige ved lov er bemyndiget til at behandle oplysninger til det andet formål, og at behandlingen er nødvendig og står i rimeligt forhold til dette formål. Europa-Kommissionen bemærker, at alle de garantier, der er fastsat i Part 3 i DPA 2018, finder anvendelse på den behandling, der foretages af den modtagende myndighed. Databeskyttelsesrådet fremhæver imidlertid, at del 3 i DPA 2018, § 44, stk. 4, § 45, stk. 4, § 48, stk. 3, og § 68, stk. 7, giver mulighed for at begrænse registreredes rettigheder, og § 79 giver mulighed for at udstede certifikater, der bekræfter, at en begrænsning er en nødvendig og forholdsmæssig foranstaltning til beskyttelse af statens sikkerhed. **Databeskyttelsesrådet anbefaler derfor, at Kommissionen yderligere vurderer de mulige konsekvenser af sådanne begrænsninger for beskyttelsesniveauet for personoplysninger i forbindelse med den videre anvendelse af de indsamlede oplysninger. Tilsvarende bør der også foretages yderligere præciseringer af den britiske retlige ramme for en sådan videredeling, navnlig Digital Economy Act 2017 samt Crime and Courts Act fra 2013, der giver mulighed for udveksling af oplysninger med NCA.**

4.1.2.2. Videreanvendelse til andre formål end retshåndhævelse i Det Forenede Kongerige

131. DPA 2018 fastsætter ligeledes, at personoplysninger, der indsamles med henblik på retshåndhævelse, kan behandles til et formål, der ikke er retshåndhævelsesformål, når behandlingen er tilladt ved lov. I dette tilfælde er retsgrundlaget for en sådan deling § 19 i Counter-Terrorism Act 2008. I denne forbindelse bemærker Databeskyttelsesrådet, at anvendelsesområdet og bestemmelserne i § 19 i Counter-Terrorism Act ikke er fuldt ud dækket af Europa-Kommissionens vurdering og kan give mulighed for yderligere anvendelse til bredere formål, navnlig for så vidt angår § 19, stk. 2,, der har følgende ordlyd *"[i]nformation indhentet af en efterretningstjeneste i forbindelse*

[81] Se EU-Domstolens dom af 6. oktober 2020 i de forenede sager C-511/18, C-512/18 og C-520/18, La Quadrature du Net m.fl., ECLI:EU:C:2020:791.

med udøvelsen af en af dens funktioner kan anvendes af den pågældende tjeneste i forbindelse med udøvelsen af dens andre funktioner".

132. Databeskyttelsesrådet bemærker endvidere, at Europa-Kommissionens henvisning til, at kompetente myndigheder er offentlige myndigheder, der skal handle i overensstemmelse med EMRK, herunder artikel 8 heri, således at det sikres, at al dataudveksling mellem de retshåndhævende myndigheder og efterretningstjenesterne er i overensstemmelse med databeskyttelseslovgivningen og EMRK, kan underbygges yderligere ved at udpege de relevante retsakter og love i den britiske retsorden, der klart og præcist beskriver kravene til overensstemmelse.

4.1.2.3. Videreanvendelse ved videreoverførsel uden for Det Forenede Kongerige

133. Selvom Europa-Kommissionen har henvist til, at CLOUD Act-aftalen mellem Det Forenede Kongerige og USA kan have indflydelse på videreoverførsler til USA fra serviceudbydere i Det Forenede Kongerige, fremhæver Databeskyttelsesrådet endvidere, at denne aftales ikrafttræden også kan påvirke videreanvendelse af oplysninger, der er indsamlet gennem videreoverførsler fra retshåndhævende myndigheder i Det Forenede Kongerige, navnlig i forbindelse med udstedelse og fremsendelse af ordrer i henhold til artikel 5 i CLOUD Act-aftalen mellem Det Forenede Kongerige og USA.

134. Mere generelt mener Databeskyttelsesrådet, at indgåelsen af fremtidige bilaterale aftaler med tredjelande med henblik på samarbejde om retshåndhævelse og tilvejebringelse af et retsgrundlag for overførsel af personoplysninger til de pågældende lande også kan få betydelig indflydelse på betingelserne for videreanvendelse af de indsamlede oplysninger, da sådanne aftaler kan påvirke den britiske databeskyttelsesramme i forhold til den vurderede ramme. Databeskyttelsesrådet anbefaler derfor, at Europa-Kommissionen vurderer dette punkt yderligere og udpeger eksisterende internationale aftaler samt præciserer, om bestemmelserne i disse aftaler kan påvirke anvendelsen af den britiske databeskyttelseslovgivning og danne grundlag for yderligere begrænsninger eller undtagelser i forbindelse med videreanvendelse og videregivelse til udlandet af oplysninger, der er indsamlet med henblik på retshåndhævelse. Databeskyttelsesrådet mener, at sådanne oplysninger og vurderinger er af afgørende betydning for at muliggøre en omfattende vurdering af beskyttelsesniveauet i den britiske lovgivningsramme og praksis i forbindelse med videregivelse til og videreanvendelse i udlandet.

4.1.3. Tilsyn

135. Databeskyttelsesrådet bemærker, at tilsynet med de retshåndhævende myndigheder på det strafferetlige område sikres af en kombination af forskellige kommissærer ud over ICO. I udkastet til konklusioner om tilstrækkeligheden af beskyttelsesniveauet nævnes kommissæren for undersøgelsesbeføjelser, kommissæren for opbevaring og anvendelse af biometrisk materiale samt kommissæren for overvågningskameraer. I denne forbindelse skal det bemærkes, at EU-Domstolen gentagne gange har understreget behovet for uafhængigt tilsyn. Kommissæren for undersøgelsesbeføjelser er af særlig betydning i sager om adgang til personoplysninger, der overføres til Det Forenede Kongerige. Databeskyttelsesrådet antager, at kommissæren for undersøgelsesbeføjelser er en såkaldt "retskommissær" på lige fod med andre retskommissærer, der skal henvises til i kapitlet om statens sikkerhed, og at disse retskommissærer har samme uafhængighed som dommere, også når de fungerer som kommissærer. Med hensyn til kommissæren for undersøgelsesbeføjelsers kontor forklarer Europa-Kommissionen i betragtning 245 i udkastet til

afgørelse, at det fungerer uafhængigt som et såkaldt "arm's length body", og at det finansieres af indenrigsministeriet.

136. Databeskyttelsesrådet har i udkastet til afgørelse ikke fundet yderligere vedrørende vurdering af uafhængigheden for kommissæren for opbevaring og anvendelse af biometrisk materiale samt for kommissæren for overvågningskameraer.

137. **Europa-Kommissionen opfordres til yderligere at vurdere retskommissærernes uafhængighed, også i sager, hvor kommissæren ikke (længere) fungerer som dommer, samt til at vurdere uafhængigheden for kommissæren for opbevaring og anvendelse af biometrisk materiale og for kommissæren for overvågningskameraer.**

4.2. Generelle retlige rammer vedrørende databeskyttelse på området vedrørende statens sikkerhed

4.2.1. Certifikater om statens sikkerhed

138. I henhold til § 111 i DPA 2018 kan dataansvarlige ansøge om certifikater om statens sikkerhed udstedt af en minister, et kabinetsmedlem, justitsministeren eller generaladvokaten for Skotland, der bekræfter, at undtagelser fra forpligtelser og rettigheder, der er fastsat i Part 4-6 i DPA 2018, er en nødvendig og forholdsmæssig foranstaltning til beskyttelse af statens sikkerhed. Certifikaterne har til formål at give de dataansvarlige større retssikkerhed og vil være et afgørende bevis på, at statens sikkerhed opretholdes ved behandling af personoplysninger. Det bør dog nævnes, at certifikaterne ikke er et krav for at anvende undtagelser vedrørende statens sikkerhed, men at de er en gennemsigtighedsforanstaltning[82].

139. Databeskyttelsesrådet udleder af Schedule 20 til DPA 2018, § 17 og 18, at et certifikat om statens sikkerhed udstedt i henhold til Data Protection Act 1998 (i det følgende benævnt "det gamle certifikat") havde udvidet virkning ved behandling af personoplysninger i henhold til DPA 2018 frem til den 25. maj 2019. Indtil denne dato blev de gamle certifikater, medmindre de blev erstattet eller tilbagekaldt, behandlet, som om de var udstedt i henhold til DPA 2018.

140. Hvis der imidlertid ikke er nogen udtrykkelig udløbsdato for et certifikat om statens sikkerhed, der er udstedt i henhold til Data Protection Act 1998, antager Databeskyttelsesrådet, at et sådant certifikat fortsat vil have virkning ved sager, der hører under Data Protection Act 1998, medmindre certifikatet tilbagekaldes eller ophæves[83]. Selv om den beskyttelse, som de gamle certifikater giver, er begrænset til behandling af personoplysninger i henhold til Data Protection Act 1998, bemærker Databeskyttelsesrådet, at der kan udstedes nye certifikater om statens sikkerhed i henhold til Data Protection Act 1998 for personoplysninger, der er blevet behandlet i henhold til Data Protection Act 1998[84].

141. **For fuldstændighedens skyld opfordrer Databeskyttelsesrådet Europa-Kommissionen til i sit udkast til afgørelse at præcisere, at certifikater om statens sikkerhed stadig kan udstedes i henhold**

[82] Se Home Office, The Data Protection Act 2018, National Security Certificates guidance, af august 2020, afsnit 4, s. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

[83] Se Home Office, The Data Protection Act 2018, National Security Certificates guidance, af august 2020, s. 5.

[84] Se Home Office, The Data Protection Act 2018, National Security Certificates guidance, af august 2020, afsnit 8, s. 5.

til Data Protection Act 1998. Desuden opfordrer Databeskyttelsesrådet Europa-Kommissionen til i sit udkast til afgørelse at beskrive adgang til retsmidler og tilsynsmekanismer for certifikater udstedt i henhold til Data Protection Act 1998. Endelig opfordrer Databeskyttelsesrådet Europa-Kommissionen til i sit udkast til afgørelse at angive antallet af eksisterende certifikater udstedt i henhold til Data Protection Act 1998 og overvåge dette område tæt.

4.2.2. Ret til berigtigelse og sletning

142. Med hensyn til retten til berigtigelse og sletning noterer Databeskyttelsesrådet sig, at registrerede i overensstemmelse med § 100 og § 149 i DPA 2018 har mulighed for at benytte High Court (i Skotland, Court of Session) til at pålægge en dataansvarlig at berigtige eller slette deres oplysninger uden unødig forsinkelse.

143. **Databeskyttelsesrådet understreger, at udøvelsen af registreredes rettigheder skal sikres effektivt og opfordrer derfor Europa-Kommissionen til i sit udkast til afgørelse at beskrive, hvordan § 100 i DPA 2018 fungerer i praksis, og til at overvåge anvendelsen af dette afsnit tæt.**

4.2.3. Undtagelser vedrørende statens sikkerhed

144. Databeskyttelsesrådet ønsker at henlede opmærksomheden på § 110 i DPA 2018 og navnlig Schedule 11, som fastsætter de specifikke formål, hvor efterretningstjenesterne er berettigede til at afvige fra visse databeskyttelsesprincipper, herunder vedrørende registreredes rettigheder, og ikke er forpligtede til at underrette ICO om brud på persondatasikkerheden[85].

145. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til yderligere at præcisere anvendelsesområdet for fritagelserne, da det er i tvivl om, hvorvidt alle de undtagelser, der er fastsat i Schedule 11 til DPA 2018, er relevante for efterretningstjenesternes arbejde, og om de sikrer ækvivalens med nødvendigheds- og proportionalitetsprincippet**. Især **opfordrer Databeskyttelsesrådet Europa-Kommissionen til at præcisere nærmere, under hvilke omstændigheder en efterretningstjeneste kan henholde sig til § 10 i Schedule 11 til DPA 2018, hvori det hedder, at *"[d]e anførte bestemmelser finder ikke anvendelse på personoplysninger, der er en registrering af den dataansvarliges hensigt i forbindelse med forhandlinger med den registrerede, i det omfang anvendelsen af de anførte bestemmelser sandsynligvis vil skade forhandlingerne."***

4.3. De britiske offentlige myndigheders adgang til og brug af personoplysninger til formål vedrørende statens sikkerhed

146. Som en generel bemærkning anerkender Databeskyttelsesrådet, at staterne har en bred skønsmargen med hensyn til statens sikkerhed, hvilket også anerkendes af Menneskerettighedsdomstolen. Databeskyttelsesrådet minder også om, at artikel 6, stk. 3, i traktaten om Den Europæiske Union, som understreget i de opdaterede anbefalinger om de europæiske væsentlige garantier for overvågningsforanstaltninger[86], fastsætter, at de

[85] Disse formål er forebyggelse og afsløring af "kriminalitet", "oplysninger, der kræves offentliggjort ved lov osv. eller i forbindelse med retssager", "parlamentarisk immunitet", "retslige procedurer", "kongehusets ære og værdighed", "væbnede styrker", "økonomisk velfærd", "tavshedspligt mellem advokater og klienter", "forhandlinger", "fortrolige henvisninger fra den dataansvarlige", "eksamenspapirer og karakterer", "forskning og statistik" og "arkiver i offentlighedens interesse".

[86] Se Databeskyttelsesrådets anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger.

grundlæggende rettigheder, der er stadfæstet i EMRK, udgør generelle principper i EU-retten. Som EU-Domstolen erindrer om i sin retspraksis, udgør konventionen imidlertid ikke et retligt instrument, der formelt er blevet indarbejdet i EU-retten, så længe EU ikke har tiltrådt den[87]. Det niveau for beskyttelse af de grundlæggende rettigheder, der kræves i henhold til artikel 45 i GDPR, skal således fastlægges på grundlag af bestemmelserne i denne forordning, sammenholdt med de grundlæggende rettigheder, der er fastsat i chartret. I henhold til chartrets artikel 52, stk. 3, har de rettigheder, som svarer til de rettigheder, som er sikret ved EMRK, dog samme betydning og omfang som dem, der er fastsat i EMRK. Som anført af EU-Domstolen skal Menneskerettighedsdomstolens retspraksis vedrørende rettigheder, der også er fastsat i chartret, derfor tages i betragtning som en minimumstærskel for beskyttelse ved fortolkning af tilsvarende rettigheder i chartret[88]. I henhold til artikel 52, stk. 3, sidste punktum, i chartret er *"[d]enne bestemmelse ikke til hinder for, at EU-retten yder en mere omfattende beskyttelse."*

147. I den følgende vurdering har Databeskyttelsesrådet derfor taget hensyn til Menneskerettighedsdomstolens retspraksis, for så vidt som chartret, som fortolket af EU-Domstolen, ikke fastsætter et højere beskyttelsesniveau, som foreskriver andre krav end Menneskerettighedsdomstolens retspraksis.

4.3.1. Retsgrundlag, begrænsninger og garantier — undersøgelsesbeføjelser i forbindelse med statens sikkerhed

4.3.1.1. Generelle bemærkninger

148. Databeskyttelsesrådet påpeger, at IPA 2016 er en nyere lov, der ændrede flere bestemmelser i Intelligence Services Act 1994. Den fastsætter, i hvilket omfang visse undersøgelsesbeføjelser kan anvendes til at gribe ind i privatlivets fred[89]. Der foreligger to rapporter fra kommissæren for undersøgelsesbeføjelser, som giver nyttige oplysninger om anvendelsen af denne nye retlige ramme, men der er stadig ikke foretaget en gennemgang af visse aspekter, navnlig vedrørende de anvendte selektorer og søgekriterier.

149. Som en generel bemærkning om IPA 2016 og dens anvendelsesområde fremhæver Databeskyttelsesrådet desuden følgende fire punkter:

150. Med hensyn til **det første punkt** vil Databeskyttelsesrådet med hensyn til lovens særlige kendetegn fremhæve to aspekter:

151. For det første bemærker Databeskyttelsesrådet, at lovgivningen henviser til brede formål for anvendelsen af de procedurer, der er fastsat i IPA 2016, og ikke til de kategorier af personer, som kan være berørt af indsamlingen af data på grundlag af Part 2-7 i IPA 2016. I denne forbindelse minder Databeskyttelsesrådet om, at der bør være en sammenhæng mellem de kategorier af personer, der kan være genstand for tilsynsforanstaltninger, og de formål, der forfølges i henhold til loven, for at definere lovens subjektive anvendelsesområde.

152. Desuden understreger Databeskyttelsesrådet, at definitionen af "teleoperatør", "teletjeneste" og "telekommunikationssystem", som definerer lovens anvendelsesområde, også er meget bred og til en vis grad uklar. Databeskyttelsesrådet fremhæver, at disse begreber, når det gælder anvendelsesområdet for IPA 2016, skal forstås meget bredere end for

[87] Se Schrems II, præmis 98.
[88] Se EU-Domstolens dom af 6. oktober 2020 i de forenede sager C-511/18, C-512/18 og C-520/18, La Quadrature du Net m.fl., ECLI:EU:C:2020:791, præmis. 124.
[89] Se § 1 i IPA 2016.

telekommunikationslovgivningen, som f.eks. defineret i den europæiske kodeks for elektronisk kommunikation[90]. Databeskyttelsesrådet bemærker, at definitionerne af "teletjeneste" og "telekommunikationssystem" i loven med forsæt er brede, således at de også vil være relevante for nye teknologier. På samme måde er definitionen af en teleoperatør også meget bred og kan f.eks. omfatte online-videospil med en chatfunktion eller andre websteder, der kun omfatter sådanne chatvinduer[91].

153. Hertil kommer, at selvom der generelt er beskrevet procedurer for og tilsyn med vurdering af nødvendighed og proportionalitet i indsamling af og adgang til data, er kriterierne for at foretage en sådan vurdering ikke defineret i selve loven. Yderligere bestemmelser kan findes i andre dokumenter, f.eks. adfærdskodekser.

154. Som påpeget i Databeskyttelsesrådets henstilling 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger har EU-Domstolen imidlertid anført, at *"kravet om, at enhver begrænsning i udøvelsen af grundlæggende rettigheder skal være fastlagt ved lov, indebærer, at omfanget af begrænsningen i udøvelse af den pågældende rettighed skal fastlægges i selve det retsgrundlag, der berettiger indgreb i rettighederne"*[92]. Domstolen præciserede nærmere bestemt, at *"[f]or at opfylde kravet om proportionalitet skal lovgivningen fastsætte klare og præcise regler for den pågældende foranstaltnings anvendelsesområde og anvendelse og angive minimumsgarantier, således at de personer, hvis personoplysninger det vedrører, har tilstrækkelige garantier for, at oplysningerne bliver effektivt beskyttet mod risikoen for misbrug. Denne lovgivning skal være retligt bindende i henhold til national ret og skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser en foranstaltning om behandling af sådanne oplysninger kan vedtages, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige*[93]*."*

155. Menneskerettighedsdomstolen understregede også, at det er vigtigt, at lovgivningen er klar for at give borgerne *"tilstrækkelige oplysninger om, under hvilke omstændigheder og på hvilke betingelser offentlige myndigheder har beføjelse til at anvende sådanne foranstaltninger"*[94].

156. **Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til yderligere at vurdere disse aspekter vedrørende den relevante lovgivnings præcision, klarhed og fuldstændighed og til at angive yderligere bestemmelser, der påviser, at den giver et beskyttelsesniveau, som i det væsentlige svarer til det, der sikres i EU med hensyn til lovgivningens kendetegn.**

---

[90] Se artikel 2, stk. 5, i den europæiske kodeks for elektronisk kommunikation, der f.eks. definerer en "interpersonel kommunikationstjeneste" som *"en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer, hvem modtageren eller modtagerne skal være, og omfatter ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste".*

[91] Se Home Office, Code of practice on the interception of communications, March 2018, afsnit 2.5 og efterfølgende, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Se Schrems II, præmis 175 og den deri nævnte retspraksis samt EU-Domstolens dom af 6. oktober 2020 i sag C-623/17, Privacy International mod Secretary of State for Foreign and Commonwealth Affairs m.fl., ECLI:EU:C:2020:790 (herefter benævnt "Privacy International"), præmis 65.

[93] Se Privacy International, præmis 68.

[94] Se Menneskerettighedsdomstolens dom af 4. december 2015, Zakharov mod Rusland, CE:ECHR:2015:1204JUD004714306, præmis 229.

Databeskyttelsesrådet understreger også, at brede definitioner også bør vurderes i forhold til aflytningsforanstaltningernes proportionalitet.

157. Selv om flere af de kompetente efterretningstjenesters interne kodekser delvist omhandler nogle af disse elementer, f.eks. vurdering af nødvendigheden og proportionaliteten ved indsamling af data, understreger Databeskyttelsesrådet desuden, at EU-Domstolens krav til lovgivningens karakter indebærer, at centrale elementer, herunder at enkeltpersoner er sikret adgang til retsmidler, skal indgå i lovgivning, der fastsætter garanterede rettigheder[95]. I Schedule 7, afsnit 6, i IPA 2016, nævnes det, at domstole (og tilsynsmyndigheder) *"tager højde for, at en person ikke tager hensyn til en kodeks ved afgørelsen af et spørgsmål i en sådan sag"* uden at præcisere, om enkeltpersoner ved domstolene (eller tilsynsmyndigheder) kan gøre gældende, at kodekserne er blevet overtrådt. Desuden henviser de elementer, der indtil videre er indeholdt i udkastet til afgørelse, enten til Menneskerettighedsdomstolens anerkendelse af forudsigeligheden i de regler, der er fastsat[96] i kodekserne, snarere end til "muligheden for at gøre dem gældende" ved domstolene, sådan som EU-Domstolen kræver det, eller til det forhold, at de britiske domstole i nogle tilfælde har henvist til kodekser, mens ingen af de nævnte sager illustrerer, at enkeltpersoner har mulighed for at håndhæve rettigheder, der følger af kodekserne. Hvis det konkluderes, at britisk lovgivning ikke i tilstrækkelig grad angiver, under hvilke omstændigheder og på hvilke betingelser en foranstaltning kan vedtages, og at sådanne bestemmelser findes i efterretningstjenesternes interne kodekser, opfordrer Databeskyttelsesrådet derfor Europa-Kommissionen til yderligere at vurdere, om de begrænsninger og garantier, der er fastsat i efterretningstjenesternes forskellige interne kodekser, kan gøres gældende af enkeltpersoner ved en domstol og håndhæves.

158. **Det andet punkt** vedrører det forhold, at bestemmelserne om målrettet indsamling og lagring af kommunikationsdata på den ene side og masseindsamling på den anden side, enten i IPA 2016 eller i anden lovgivning såsom Intelligence Services Act 1994 eller Regulation of Investigatory Powers Act 2000, også finder anvendelse på data, der overføres fra EU til Det Forenede Kongerige. Med hensyn til masseindsamling understreger Databeskyttelsesrådet, at de relevante bestemmelser i britisk lovgivning giver mulighed for indsamling af data uden for Det Forenede Kongerige. Det kan således omfatte data under overførsel fra EØS til Det Forenede Kongerige på grundlag af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet[97]. Desuden bemærker Databeskyttelsesrådet, at Europa-Kommissionen anfører, at "*[d]et skal bemærkes, at opbevaring og indsamling af kommunikationsdata normalt ikke vedrører personoplysninger om registrerede i EU, der overføres til Det Forenede Kongerige i henhold til denne afgørelse. Forpligtelsen til at opbevare eller videregive kommunikationsdata i henhold til Part 3 og 4 i IPA 2016 omfatter data, der indsamles af teleoperatører i Det Forenede Kongerige direkte fra brugerne af en telekommunikationstjeneste*"[98]. Databeskyttelsesrådet fremhæver dog den manglende klarhed med hensyn til, at kun disse operatørers virksomheder, der er beliggende i Det Forenede Kongerige, kan modtage anmodninger fra de kompetente britiske myndigheder, eftersom definitionen af teleoperatør i § 261, stk. 10, i IPA

[95] I den forbindelse fandt EU-Domstolen f.eks., at PPD 28 i USA ikke opfyldte betingelserne, selv om den også indeholdt visse begrænsninger med hensyn til masseindsamling, jf. Schrems II, præmis 181.

[96] Se Menneskerettighedsdomstolens dom af 13. september 2018, Big Brother Watch m.fl. mod Det Forenede Kongerige, ECLI:CE:ECHR:2018:0913JUD005817013 (herefter "Big Brother Watch"), præmis. 325: *"Da IC-kodeksen er et offentligt dokument godkendt af begge kamre i parlamentet og skal tages i betragtning både af dem, der udfører aflytning, og af domstole og retsinstanser, har Domstolen udtrykkeligt accepteret, at dens bestemmelser kan tages i betragtning ved vurderingen af RIPA-ordningens forudsigelighed."*

[97] Se præmis 183 ff. i Schrems II om vurdering af en lovgivning, der giver adgang til oplysninger under overførsel mellem EU og et tredjeland i forbindelse med en afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

[98] Se betragtning 196 i afgørelsesudkastet.

2016 kræver, at "en teleoperatør er en person, der tilbyder eller leverer en telekommunikationstjeneste til personer i Det Forenede Kongerige, *eller som kontrollerer eller leverer et telekommunikationssystem, der (helt eller delvist) er placeret i eller kontrolleres fra Det Forenede Kongerige*". Derfor kan personoplysninger om registrerede i EØS faktisk være berørt, f.eks. i tilfælde af data, der indsamles eller genereres af en virksomhed tilhørende en britisk teleoperatør beliggende i EØS, og som overføres til en virksomhed tilhørende samme operatør beliggende i Det Forenede Kongerige på grundlag af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet (til kommercielle formål) og derefter indsamles i Det Forenede Kongerige af de kompetente offentlige myndigheder.

159. **Databeskyttelsesrådet er derfor af den opfattelse, at vurderingen af disse bestemmelser også er relevant for vurderingen af tilstrækkeligheden af den britiske retlige ramme, og opfordrer Europa-Kommissionen til at præcisere dette aspekt og yderligere vurdere, i hvilket omfang dette er tilfældet. Navnlig opfordrer Databeskyttelsesrådet Europa-Kommissionen til at præcisere sin opfattelse af lovgivningens anvendelsesområde, herunder hvad begrebet "brugere af telekommunikationstjenester" dækker, og hvorvidt der kan anmodes om data fra virksomheder, der drives af teleoperatører uden for Det Forenede Kongerige, for så vidt angår oplysninger om registrerede i EØS, i betragtning af den meget brede definition af teleoperatører.**

160. **Det tredje punkt** vedrører "double lock-proceduren". Databeskyttelsesrådet bemærker, at der er indført en ny "double lock-procedure" i IPA 2016. Ikke desto mindre forstår Databeskyttelsesrådet også, at selvom indsamling af eller adgang til data til formål vedrørende statens sikkerhed eller efterretninger i princippet kun kan finde sted med en kendelse, der er godkendt af en retskommissær, fastsættes det i IPA 2016, at *"i specifikke begrænsede tilfælde er lovlig aflytning uden en kendelse mulig, og kun forudgående tilladelse fra de kompetente IC-myndigheder er påkrævet [se afsnittet om tilsyn], herunder ved aflytninger i overensstemmelse med oversøiske anmodninger (§ 52 i IPA 2016)".* Som understreget nedenfor stemmer dette også overens med Databeskyttelsesrådets betænkeligheder, navnlig med hensyn til oversøisk videregivelse. Desuden bemærker Databeskyttelsesrådet også, at når der er tale om udstyrsinterferens, hvad enten det er målrettet eller masseindsamling, er det også muligt at fravige double lock-proceduren, og at retskommissæren kun har ret til at godkende fornyelse af kendelser vedrørende masseindsamling efter en indledende periode på højst 6 måneder. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til yderligere at vurdere og påvise, at selv i tilfælde, hvor double lock-proceduren ikke finder anvendelse, giver den britiske retlige ramme passende garantier, herunder gennem effektivt efterfølgende tilsyn og adgang til retsmidler for de enkelte personer, til at sikre, at det ydede beskyttelsesniveau i det væsentlige svarer til det, der opnås i EU (se også afsnit 4.3.3 om tilsyn).**

161. Selv om "double lock-proceduren" blev indført med IPA 2016, er Databeskyttelsesrådet fortsat bekymret over visse elementer i den nye lovgivning. Efter præsentationen af de tilsvarende afsnit i udkastet til afgørelse har Databeskyttelsesrådet analyseret følgende typer indsamling af og adgang til data i samme rækkefølge som forelagt af Europa-Kommissionen. Rækkefølgen af de elementer, der vurderes i det følgende, afspejler derfor Databeskyttelsesrådets grad af betænkelighed.

4.3.1.2. Målrettet indsamling og lagring af kommunikationsdata

162. Databeskyttelsesrådet bemærker, at der er to embedsmænd, som kan udstede målrettede tilladelser til at indhente kommunikationsdata: den anvisningsberettigede ved Office for Communications Data Authorisations (i det følgende "kommissæren for undersøgelsesbeføjelser"), en udpeget overordnet embedsmand (en person, der har et foreskrevet embede eller rang i en relevant offentlig myndighed), ud over en retskommissærs godkendelse i visse tilfælde. Det er imidlertid fortsat uklart

for Databeskyttelsesrådet i henhold til loven og den relevante kodeks, nøjagtigt hvilken embedsmand der giver tilladelse til, hvilken type målrettet erhvervelse af kommunikationsdata der er tale om, og i hvilket omfang en udpeget embedsmand kan være tilstrækkeligt uafhængig[99].

163. **Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til yderligere at vurdere dette aspekt og give klarere forklaringer på disse elementer.**

164. Med hensyn til meddelelsen med anmodning om lagring af kommunikationsdata, bemærker Databeskyttelsesrådet også, at sådanne meddelelser kan rettes til en "beskrivelse af operatører". Betegnelsen synes at indebære, at flere operatører samtidig kan anmodes om alle at opbevare data. Indsamlingen er altså ikke målrettet, hvad angår antallet af operatører, men derimod hvad angår navnet på eller beskrivelsen af de personer, organisationer, lokaliteter eller grupper af personer, der udgør "målet", en beskrivelse af undersøgelsens art og en beskrivelse af de aktiviteter, som udstyret anvendes til. Databeskyttelsesrådet fremhæver derfor, at afhængigt af antallet af operatører, der er omfattet af en sådan "beskrivelse af operatører" kan meddelelsen være bredere end det, proceduren for målrettet opbevaring kan synes at indebære. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til yderligere at vurdere dette aspekt og give yderligere garantier for, at meddelelser, selv når de er rettet til flere operatører, fortsat er begrænset til, hvad der er strengt nødvendigt og forholdsmæssigt.**

4.3.1.3. Udstyrsinterferens

165. Databeskyttelsesrådet bemærker, at "udstyrsinterferens" kan afvige fra double lock-proceduren i hastetilfælde[100]. Databeskyttelsesrådet er derfor bekymret over, at formålene med sådan udstyrsinterferens kan være brede, og at kriterierne for uopsættelighed (i hvilket tilfælde retskommissæren ikke er forpligtet til at give forhåndstilladelse efter en vurdering af nødvendigheden og proportionaliteten af udstyrsinterferensen) fortsat er uklare. Eftersom "kendelsen ophører med at have virkning og ikke kan forlænges" i sidstnævnte situation i tilfælde, hvor retskommissæren ikke efterfølgende godkender udstyrsinterferensen, forstår Databeskyttelsesrådet, at de indsamlede data i mellemtiden fortsat er lovligt indsamlet. For at disse oplysninger kan slettes, kan der udstedes en særlig kendelse fra retskommissæren[101].

166. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til yderligere at vurdere betingelserne for at hævde uopsættelighed og til at præcisere de muligheder, som de pågældende registrerede har for at udøve deres rettigheder, samt de eventuelle klagemuligheder, de får tilbudt i forbindelse med "equipment interference"-operationer (udstyrsinterferens), især i hastetilfælde, der bevirker en afvigelse fra double lock-proceduren.**

4.3.1.4. Masseopfangning af data fra bærertjenester

167. Som beskrevet i report of the bulk powers review[102] *"[m]asseopfangning indebærer typisk indsamling af kommunikation under overførsel hos særlige bærertjenester (kommunikationsforbindelser)*". Det officielle faktablad for IPA 2016 beskriver "masseopfangning" som "*processen til indsamling af en kommunikationsmængde efterfulgt af udvælgelse af dele af kommunikationen til gennemgang, gennemlæsning eller gennemlytning, hvor det er nødvendigt og forholdsmæssigt*". Databeskyttelsesrådet bemærker, at "masseopfangning" af data reelt indebærer indsamling af data

[99] Se også infra vedrørende vurderingen af double lock-proceduren og retskommissærens uafhængighed.
[100] Se § 109 i IPA 2016.
[101] Se § 110, stk. 3, litra b), i IPA 2016.
[102] Se Report of the bulk powers review, udarbejdet af Independent Reviewer of Terrorism Legislation, august 2016.

før filtrering ved hjælp af selektorer (simple ved overvågning af enkeltpersoner, der allerede vides at udgøre en trussel, eller komplekse ved identifikation af nye trusler og tidligere ukendte personer af interesse).

168. Erhvervelsen af massekommunikationsdata var også et af de spørgsmål, som EU-Domstolen behandlede i sagen Privacy International, som resulterede i en dom afsagt af Store Afdeling den 6. oktober 2020 (ud over hvorvidt en sådan indsamling af data blev foretaget inden for rammerne af EU-retten, selv af hensyn til statens sikkerhed). IPA 2016 har erstattet den lovgivning, der var genstand for denne dom.

169. Databeskyttelsesrådet bemærker, at der med indførelsen af IPA 2016 i britisk lovgivning nu også kræves en kendelse for masseopfangning af data. Proceduren for udstedelse af denne kendelse afhænger af fastlæggelsen af "operationelle formål". Listen over disse operationelle formål udarbejdes af cheferne for efterretningstjenesterne og godkendes derefter af udenrigsministeren. Selve afgørelsen godkendes af en uafhængig retskommissær, som skal kontrollere, om kendelsen er nødvendig og står i rimeligt forhold til de operationelle formål. Databeskyttelsesrådet forstår, at retskommissæren ikke har beføjelse til at vurdere selve de operationelle formål, men om kendelsen er nødvendig og står i et rimeligt forhold til de operationelle formål, der er anført i kendelsen. Det parlamentariske efterretnings- og sikkerhedsudvalg får udleveret en kopi af listen hver tredje måned, og premierministeren reviderer listen over disse operationelle formål mindst én gang om året.

170. På grundlag af de elementer, som Europa-Kommissionen har fremlagt i udkastet til afgørelse, forekommer det imidlertid vanskeligt at vurdere omfanget af de operationelle formål på listen, samt om de deraf følgende dataindsamlinger overholder den tærskel, som EU-Domstolen har fastsat (f.eks. kan en geografisk begrænsning af dataindsamlingen dække få gader eller hele EØS).

171. Desuden understreger Databeskyttelsesrådet, at data, der er indsamlet ved masseindsamling, kan opbevares i lange perioder (for at være tilgængelige for yderligere adgang ved undersøgelser). Databeskyttelsesrådet bemærker således, at § 150, stk. 5 og 6, i IPA 2016 kun omhandler destruktion af kopier af de indsamlede data, og kun hvis opbevaring ikke er nødvendig eller sandsynligvis ikke vil blive nødvendig af hensyn til statens sikkerhed eller andre grunde, der hører under anvendelsesområdet for § 138, stk. 2, i IPA 2016, eller hvis opbevaringen ikke er nødvendig til flere andre formål[103]. Databeskyttelsesrådet understreger, at disse grunde forekommer meget brede, og at det under alle omstændigheder kun er kopier af de indsamlede data, der nævnes.

172. Databeskyttelsesrådet bemærker endvidere, at IPA 2016 i hastetilfælde også giver mulighed for at ændre kendelser uden forudgående godkendelse fra en retskommissær. Hvis retskommissæren efterfølgende høres inden for tre arbejdsdage og ikke godkender ændringen, bør kendelsen have virkning, som om ændringen ikke var foretaget, og data indsamlet i de mellemliggende dage vil fortsat være indsamlet på lovlig vis[104]. For at disse oplysninger kan slettes, kan der udstedes en særlig kendelse fra retskommissæren[105].

173. **Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at foretage yderligere klarlægning og vurdering af masseaflytning, navnlig udvælgelse og anvendelse af selektorer i forbindelse med masseaflytningsprocedurer, for at klarlægge, i hvilket omfang adgangen til personoplysninger overholder den tærskel, som EU-Domstolen har fastlagt**

[103] Se § 150, stk. 3 og 6, i IPA 2016.
[104] Se § 147 IPA 2016 (del 6, kapitel I).
[105] Se § 181, stk. 3, litra b), i DPA 2016.

(se også nedenstående sektion 4.3.1.7., navnlig vedrørende tilsyn med selektorer), og hvilke garantier der er indført til at beskytte de borgeres grundlæggende rettigheder, hvis data aflyttes i denne forbindelse, herunder med hensyn til dataopbevaringsperioden. En uafhængig vurdering foretaget af kompetente britiske tilsynsmyndigheder ville være særligt nyttig.

174. **Databeskyttelsesrådet understreger også, at det forekommer særligt kritisk, at "overseas-related communications" (oversøisk kommunikation), som falder inden for masseaflytning, synes at indebære, at Det Forenede Kongerige direkte kan aflytte og masseindsamle dataene i EØS, herunder data, der er under overførsel mellem EØS og Det Forenede Kongerige, hvilket ville falde ind under afgørelsesudkastets anvendelsesområde (se nedenstående afsnit 4.3.2 om videreanvendelse af oplysninger indsamlet til formål vedrørende statens sikkerhed og oversøisk videregivelse).**

4.3.1.5. Beskyttelse af og garantier for sekundære data

175. Databeskyttelsesrådet er desuden bekymret over, at den relevante britiske lovgivning vedrørende masseaflytning ikke giver det samme beskyttelsesniveau for alle kommunikationsdata. "Sekundære data", som kan indsamles på grundlag af en masseindsamlingskendelse, er i henhold til § 137 i IPA 2016 både "systemdata", *"som indgår i, indgår som en del af, er vedhæftet til eller logisk tilknyttet til kommunikationen (af afsenderen eller på anden måde)*", og "identifikationsdata", *"som indgår i, indgår som en del af, er vedhæftet til eller logisk tilknyttet til kommunikationen (af afsenderen eller på anden måde), som logisk kan adskilles fra resten af kommunikationen, og som, hvis data var separate, ikke ville afsløre noget om, hvad der kunne antages af være et (eventuelt) budskab i kommunikationen, når der ses bort fra en betydning, der kan tillægges, at kommunikationen er foregået, eller udledes af data vedrørende overførsel af kommunikationen*"[106].

176. Databeskyttelsesrådet bemærker, at disse "sekundære data", også benævnt "metadata"[107], der masseindsamles, ikke synes at være omfattet af de samme sikkerhedsforanstaltninger som data indsamlet med en kendelse vedrørende målrettet indsamling men også som masseindsamlede indholdsdata. Databeskyttelsesrådet bemærker, at udvælgelse af alle typer opfanget indhold er omfattet af flere garantier[108] end udvælgelse af sekundære data[109].

[106] "Systems data" og "identifying data" er defineret i § 263 i IPA 2016.
[107] Se Report of the bulk powers review, udarbejdet af Independent Reviewer of Terrorism Legislation, august 2016.
[108] Se § 152, stk. 1, litra c), og § 152, stk. 3 ff., i IPA 2016.
[108] Se § 152, stk. 1, litra c), og § 152, stk. 3 ff., i IPA 2016.
[109] Se § 152, stk. 1, litra a) og b), i IPA 2016.

177. Desuden understreger Databeskyttelsesrådet, at både Menneskerettighedsdomstolen[110] og EU-Domstolen[111] har sat spørgsmålstegn ved, om sådanne data er mindre følsomme end andre, navnlig indholdsdata. Adfærdskodeksen vedrørende aflytning nævner eksempler på "sekundære data" (både "systemdata" såsom routerkonfigurationer, e-mailadresser eller bruger-ID men også alternative kontoidentifikatorer samt "identifikationsdata", f.eks. mødested i en kalenderaftale, billedoplysninger såsom tidspunkt, dato og sted, hvor billedet er taget). **Databeskyttelsesrådet fremhæver derfor de enslydende vurderinger fra Menneskerettighedsdomstolen og EU-Domstolen og minder om de betænkeligheder, der er udtrykt vedrørende sekundære data, som bør være omfattet af specifikke garantier på grund af dataenes følsomhed**. **Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til nøje at vurdere, om garantierne i britisk lov for denne kategori af personoplysninger sikrer et beskyttelsesniveau, der i det væsentlige svarer til det, der garanteres i EU.**

4.3.1.6. Automatisk behandling af kommunikationsdata

178. Databeskyttelsesrådet bemærker, at efterretningsmyndighederne ikke kun anvender enkle eller komplekse selektorer til at filtrere masseindsamlede data, men at de også kan benytte andre automatiserede databehandlingsværktøjer til at analysere *"store mængder oplysninger, og det sætter agenturerne i stand til at finde forbindelser, mønstre, sammenhænge eller adfærd, der kan påvise en alvorlig trussel, som kræver undersøgelse"*, ifølge Intelligence and Security Committee report 2015[112]. **Databeskyttelsesrådet er opmærksomme på, at denne offentlige rapport vedrører praksis under den tidligere retlige ramme, som efterfølgende blev erstattet af IPA 2016. Rådet er ikke desto mindre af den opfattelse, at det er nødvendigt, at de kompetente britiske tilsynsmyndigheder foretager yderligere uafhængige vurderinger og tilsyn med anvendelsen af automatiserede databehandlingsredskaber, og opfordrer Europa-Kommissionen til yderligere at vurdere dette spørgsmål og de garantier, som i denne forbindelse vil blive givet eller kan gives til de registrerede i EØS.**

---

[110] Se Menneskerettighedsdomstolen, Big Brother Watch, præmis 357, med henvisning til Store Afdeling: *"Selvom Domstolen ikke betvivler, at de omhandlede kommunikationsdata er et vigtigt redskab for efterretningstjenesterne i bekæmpelsen af terrorisme og grov kriminalitet, mener den ikke, at myndighederne har fundet en rimelig balance mellem de konkurrerende offentlige og private interesser ved i sin helhed at undtage dem fra de garantier, der gælder for søgning og undersøgelse af indhold. Selvom Domstolen ikke antyder, at de omhandlede kommunikationsdata kun bør være tilgængelige med henblik på at fastslå, om en person befinder sig på De Britiske Øer eller ej, da dette ville kræve, at der anvendes strengere standarder for de pågældende kommunikationsdata end dem, der gælder for indhold, bør der ikke desto mindre foreligge tilstrækkelige garantier til at sikre, at fritagelsen af de pågældende kommunikationsdata fra kravene i § 16 i RIPA begrænses til det omfang, der er nødvendigt for at afgøre, om en person i øjeblikket befinder sig på De Britiske Øer."*

[111] Se EU-Domstolen, Privacy International, præmis 71: *"Det indgreb, som overføring af trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne indebærer, i den rettighed, som er fastsat i chartrets artikel 7, skal anses for at være særligt alvorligt, henset til bl.a. den følsomme karakter af de oplysninger, som disse data kan give adgang til, og navnlig muligheden for på grundlag heraf at lave en profil af de berørte personer, idet en sådan oplysning er lige så følsom som selve indholdet af kommunikationen. Den er i øvrigt egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant overvågning (jf. analogt dom af 8.4.2014, Digital Rights Ireland m.fl., C-293/12 og C-594/12, EU:C:2014:238, præmis 27 og 37, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 99 og 100).*"

[112] Se Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, 2015, punkt 18, s. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

4.3.1.7. Risici for overholdelse og manglende overholdelse hos de kompetente efterretningsmyndigheder

179. Databeskyttelsesrådet bemærker, at der foreligger detaljerede tilsynsrapporter. De indeholder værdifulde elementer med hensyn til, hvad de vurderer som positiv praksis for overholdelse, samt de identificerede risici for overholdelse og praksis, der ikke er i overensstemmelse med reglerne.

180. I henhold til rapporten fra kommissæren for undersøgelsesbeføjelser for 2019 har flere forhold vedrørende de forskellige kompetente myndigheders anvendelse af den retlige ramme afsløret visse (risici for) uoverensstemmelser fra de kompetente myndigheders side.

181. For det første har Databeskyttelsesrådet bemærket, at kriterierne for klassificering af et datasæt som massedatasæt eller som målrettede data ikke altid synes at være klare for MI5 og SIS selv, navnlig for MI5, hvilket kan føre til, at der ikke anvendes passende garantier for dataene[113]. I sin rapport fra 2019 foreslog kommissæren, at "*der bør sættes fokus på at løse dette spørgsmål*"[114]. Også med hensyn til personoplysninger som massedatasæt bemærker Databeskyttelsesrådet vedrørende GCHQ, at selvom klassifikationen af personoplysninger som massedatasæt synes at være tilfredsstillende (men endnu ikke revideret af kommissæren for undersøgelsesbeføjelser) gav specialteamets interne overensstemmelseskontrol af kendelser i marts 2019 anledning til alvorlige betænkeligheder, idet 50 % af begrundelserne for de masseindsamlingskendelser, der blev gennemgået af GCHQ's complianceteam, ikke opfyldte den krævede standard. Ifølge kommissæren havde complianceteamet påbegyndt arbejdet med at undersøge problemet og efteruddanne personalet for at forbedre dette forhold. Efteruddannelsen i bestemmelserne i IPA 2016 og den supplerende uddannelse, der blev tilbudt via politiske netværk og netværk for regeloverensstemmelse (i det følgende benævnt "PCN"), har forbedret GCHQ's overholdelse af bestemmelserne på området. Kommissæren for undersøgelsesbeføjelser forventer ikke at se manglende overholdelse af standarderne ved fremtidig kontrol, men vil fortsat overvåge området tæt[115]. **Databeskyttelsesrådet er derfor enigt i, at der er behov for, at Europa-Kommissionen foretager yderligere gennemgang og overvågning af de nævnte elementer som led i vurderingen af beskyttelsesniveauet for at sikre, at denne standard forbedres, som understreget i kommissærens rapport, og påpeger, at der også skal tages højde for gennemførelsen og den konkrete anvendelse af den retlige ramme, jf. artikel 45 i GDPR, ved vurderingen af, om et tredjeland i det væsentlige overholder bestemmelserne.**

182. Generelt fremhæver Databeskyttelsesrådet de punkter, som kommissæren for undersøgelsesbeføjelser gør opmærksom på, i forbindelse med "opgavebaserede søgninger", der

---

[113] Se Annual Report of the Investigatory Powers Commissioner 2019 af 15. december 2020, punkt 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: "*Vi har observeret den positive udvikling i [Bulk Oversight Panel (BOP)] og bemærker effekten med hensyn til at styre den interne overholdelse. Vi ønsker fortsat større klarhed om den proces, som MI5 anvender til at foretage indledende undersøgelser af nye datasæt for bedre at forstå beslutninger om at klassificere et datasæt som BPD eller f.eks. som målrettede data. Vi var bekymrede over et enkelt uløst punkt i rapporten fra BOP vedrørende afhjælpning af inkonsekvens ved tildeling af BPD til MI5 og SIS. Det er muligt, at begge agenturer, på baggrund af forskellig anvendelse af data og forskellig opdeling af de foreliggende datasæt, kan være i besiddelse af det samme datasæt eller versioner heraf, og at det lovligt kan kategoriseres som masseindsamling af det ene agentur og målrettede data af det andet. Hvis et af agenturerne fejlagtigt har kategoriseret oplysningerne som et målrettet datasæt, er der risiko for, at disse data opbevares uden passende kendelse og muligvis uden de fornødne garantier.*"

[114] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 8.39.

[115] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.48.

ledes af medarbejdere hos MI5 — som gør det muligt for en efterforsker at foretage mere end én søgning i de massedatasæt, de har til rådighed, og de "*alvorlige risici for manglende regeloverholdelse, der er forbundet med nogle af de teknologiske miljøer, der anvendes af MI5*". Det drejer sig om, hvor data er lagret i systemerne, hvem der har adgang til dem, i hvilket omfang de bliver kopieret eller delt, processer til sletning af data, samt hvor længe data opbevares. Selv om kommissæren anfører, at der er truffet foranstaltninger og indført garantier, forvaltes nogle af disse fortsat manuelt og efter et personligt skøn, og det understreger, at det er afgørende, at "*MI5 fortsat fastholder de nye processer og sikrer tilstrækkelige ressourcer til, at de fungerer effektivt. Hvis MI5 konstaterer øget manglende regeloverholdelse"*[116]**.** Kommissæren for undersøgelsesbeføjelser forventer, at de vil blive gjort opmærksom på dem så hurtigt som muligt. **Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at overvåge disse aspekter tæt i fremtiden.**

183. Med hensyn til GCHQ forstår Databeskyttelsesrådet også ud fra rapporten fra kommissæren for undersøgelsesbeføjelser, at "*ansøgninger om intern godkendelse af operationer, der gennemføres under kendelser vedrørende masseindsamling, har været af svingende kvalitet, og vi har bemærket, at der var behov for bedre kvalitet i udarbejdelsen af ansøgningerne*"[117], samt at begrundelserne for brug af generelle deskriptorer ved målrettet udstyrsinterferens i nogle tilfælde har været for generelle og upræcise[118]. Databeskyttelsesrådet bemærkede også, at kommissæren for undersøgelsesbeføjelser ved masseudstyrsinterferens anbefaler, at "*ansøgninger bør konsekvent og udtrykkeligt beskrive sammenhængen mellem målet og et lovbestemt formål samt efterretningskravene*"[119], at "*alle applikationer klart bør tage højde for mulig utilsigtet dataindsamling samt relevant modvirkning heraf i proportionalitetsvurderingen*"[120], samt at IPC understregede, at der trods fremskridt "*stadig er behov for forbedringer*"[121], og at der også i fremtiden vil være behov for yderligere fokus på området.

184. Med hensyn til masseaflytningsordningen i henhold til Regulation of Investigatory Powers Act 2000 (i det følgende benævnt "RIPA 2000"), som siden er blevet erstattet af bestemmelser i IPA 2016, minder Databeskyttelsesrådet om, at det utilstrækkelige tilsyn, både med udvælgelsen af internetbærertjenester til aflytning og filtrering, søgning og udvælgelse af aflyttede kommunikationer til undersøgelse, var et af de centrale aspekter, som Menneskerettighedsdomstolen anså for at være i strid med artikel 8 i EMRK med hensyn til den tidligere lovgivning om britiske myndigheders undersøgelsesbeføjelser i forbindelse med sagen *Big Brother Watch*, som nu er videregivet til Store Afdeling. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til at kontrollere status i sagen, tage hensyn til disse elementer og præcisere dem i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, hvis Kommissionen vedtager den.**

185. I denne sag var Menneskerettighedsdomstolen: *"ikke overbevist om, at garantierne for udvælgelse af bærertjenester til aflytning og udvælgelse af aflyttet materiale til undersøgelse er tilstrækkeligt robuste til at give tilstrækkelige garantier mod misbrug. Den største bekymring er dog manglen på et robust og uafhængigt tilsyn med selektorer og søgekriterier, der anvendes til filtrering*

[116] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 8.52.
[117] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.2.
[118] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.16 og 10.17.
[119] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.23.
[120] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.23.
[121] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.23.

af den aflyttede kommunikation."[122] Som fremhævet af kommissæren for undersøgelsesbeføjelser, *"var dette resultat en gentagelse af en lignende anbefaling i Intelligence and Security Committees rapport Privacy and Security: A modern and transparent legal framework report fra marts 2015"*[123]. **Databeskyttelsesrådet bifalder også, at kommissæren for undersøgelsesbeføjelser derfor i 2019 foretog en gennemgang af sin tilgang til inspektion af masseaflytning, "*herunder en nøje gennemgang af de teknisk komplekse måder, hvorpå masseaflytning faktisk foregår*"[124], og forpligtede sig til at inkludere "*en detaljeret undersøgelse af de selektorer og søgekriterier, som Menneskerettighedsdomstolen har antydet*"[125], i de kommende inspektioner af masseaflytning fra 2020 og frem. På grund af dette aspekts betydning er Databeskyttelsesrådet bekymret for, at kommissæren for undersøgelsesbeføjelser endnu ikke har foretaget en detaljeret undersøgelse af selektorer og søgekriterier, og opfordrer Europa-Kommissionen til nøje at overvåge udviklingen på dette punkt, især fordi det endnu ikke er klarlagt, hvilken konkret form et sådant tilsyn skal have[126].**

4.3.2. Videreanvendelse af de oplysninger, der er indsamlet til nationale sikkerhedsformål og oversøisk videregivelse

186. Hvad angår den videre anvendelse af de oplysninger, der indsamles af hensyn til statens sikkerhed, henviser Europa-Kommissionen i sin vurdering til § 87, stk. 1, i DPA 2018, hvori det hedder, at "*personoplysninger, der indsamles på denne måde, ikke må behandles på en måde, der er uforenelig med det formål, hvortil de indsamles*". Databeskyttelsesrådet påpeger imidlertid, at denne bestemmelse kan være underlagt nationale sikkerhedsundtagelser i henhold til § 110 i DPA 2018. Databeskyttelsesrådet bemærker endvidere, at lovgivningen giver mulighed for "oversøisk videregivelse", hvad enten det drejer sig om målrettet aflytning og undersøgelse, målrettet erhvervelse og lagring af kommunikationsdata, målrettet udstyrsinterferens eller masseaflytning og masseudstyrsinterferens.

4.3.2.1. Videreanvendelse, oversøisk videregivelse og gældende retlige rammer i Det Forenede Kongerige

187. Europa-Kommissionen har udpeget Part 4 i DPA 2018, navnlig § 109, som relevante bestemmelser, der fastsætter specifikke krav ved videreanvendelse af de indsamlede oplysninger, navnlig når efterretningstjenesterne videregiver personoplysninger til tredjelande eller internationale organisationer. Databeskyttelsesrådet bemærker imidlertid, at § 110 i DPA 2018 indeholder en undtagelse vedrørende national sikkerhed, hvori det præciseres, at visse bestemmelser i DPA 2018 ikke finder anvendelse, hvis en undtagelse fra disse bestemmelser er nødvendig af hensyn til den nationale sikkerhed. De pågældende bestemmelser, der muligvis ikke finder anvendelse, omfatter kapitel 2 i del 4 i DPA 2018 vedrørende databeskyttelsesprincipperne, herunder formålsbegrænsning, samt kapitel 3 i del 4 i DPA 2018 vedrørende registreredes rettigheder. § 109 i DPA 2018 sammenholdt med § 110 i DPA 2018 og de betingelser, hvorunder den finder anvendelse, kan føre til tilfælde, hvor efterretningstjenesternes videregivelse af personoplysninger til tredjelande

[122] Se Menneskerettighedsdomstolen, Big Brother Watch, præmis 347.
[123] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.28.
[124] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.28.
[125] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.28.
[126] Se Annual Report of the Investigatory Powers Commissioner 2019, punkt 10.28: "Inspektionens nøjagtige form skal aftales".

finder sted uden at anvende bestemmelser vedrørende databeskyttelsesprincipperne og de registreredes rettigheder.

188. Som påpeget af Europa-Kommissionen skal en sådan undtagelse vurderes fra sag til sag og kan kun anvendes i det omfang, at anvendelsen af en bestemt bestemmelse ville have negative konsekvenser for den nationale sikkerhed. Udstedelsen af et nationalt certifikat til de britiske efterretningstjenester har til formål at bekræfte, at der kræves en undtagelse for bestemte personoplysninger, der behandles med henblik på at beskytte den nationale sikkerhed. Databeskyttelsesrådet bemærker imidlertid, at det britiske indenrigsministerium i sin vejledning om nationale sikkerhedscertifikater i henhold til DPA 2018 præciserer, at "*[d]et er vigtigt indledende at bemærke, at et certifikat ikke er påkrævet for at kunne anvende undtagelsen vedrørende national sikkerhed. Reelt vil de dataansvarlige i de fleste tilfælde reelt selv afgøre, om undtagelsen vedrørende den nationale sikkerhed skal gøres gældende.*" [127] Desuden fremgår det af det britiske indenrigsministeriums vejledning, at "*certifikater om statens sikkerhed kan gælde for personoplysninger, der specifikt kan identificeres, eller omfatte en bredere kategori af personoplysninger. De kan have fremad- eller tilbagegående virkning.*" [128] "Fritagelsen for national sikkerhed kan derfor finde anvendelse i forbindelse med efterretningstjenesters internationale videregivelse af personoplysninger til tredjelande i mangel af et nationalt sikkerhedscertifikat.

189. Databeskyttelsesrådet bemærker endvidere, at det f.eks. fremgår af certifikat om statens sikkerhed DPA/S27/Security Service[129], at personoplysninger, der behandles "*for, på vegne af, efter anmodning fra eller med hjælp eller bistand fra sikkerhedstjenesten eller*", og "*hvis en sådan behandling er nødvendig for at lette den korrekte udførelse af sikkerhedstjenestens funktioner som beskrevet i § 1 i Security Service Act 1989*", frem til den 24. juli 2024 er undtaget fra de tilsvarende bestemmelser i britisk lovgivning til kapitel V i GDPR i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer. Selvom de øvrige certifikater om statens sikkerhed, der er offentligt tilgængelige, ikke indeholder en undtagelse fra bestemmelserne i § 109 i DPA 2018, skal det erindres, at en del af eller hele teksten til et certifikat om statens sikkerhed kan blive tilbageholdt, hvis offentliggørelsen strider mod hensynet til den nationale sikkerhed eller offentlighedens interesser eller kan bringe en persons sikkerhed i fare.

190. I forbindelse med vurderingen af afgørelsesudkastet i forhold til disse bestemmelser bemærker Databeskyttelsesrådet generelt, at sikkerhedsforanstaltningerne for disse videregivelser udelukkende omfatter kravet om, at modtageren af oplysningerne overholder kravene vedrørende datasikkerhed, omfanget af videregivelsen begrænset til, hvad der er nødvendigt, lagring af data og begrænsning af adgangen til data for et begrænset antal personer. **Databeskyttelsesrådet understreger med hensyn til oversøisk videregivelse, at anvendelsen af undtagelsen efter britisk ret vedrørende statens sikkerhed kan føre til, at der mangler garantier, som kan sikre, at principperne om formålsbegrænsning, nødvendighed og proportionalitet også efterleves, eller at det modtagende tredjeland i tilstrækkelig grad fastlægger eller efterlever rettigheder for borgerne, tilsyn og adgang til retsmidler. Databeskyttelsesrådet anbefaler Europa-Kommissionen at foretage yderligere undersøgelser af de overordnede**

[127] Se Home Office, The Data Protection Act 2018, National Security Certificates guidance, af august 2020, afsnit 3, s. 3.
[128] Se Home Office, The Data Protection Act 2018, National Security Certificates guidance, af august 2020, afsnit 5, s. 4.
[129] Se DPA/S27/Security Service, section 27 DPA 2018, Certificate of the Secretary of State, af 24. juli 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

garantier, som gives i henhold til britisk ret med hensyn til oversøisk videregivelse, navnlig i lyset af anvendelsen af undtagelser begrundet i statens sikkerhed.

4.3.2.2. Oversøisk videregivelse og udveksling af efterretninger inden for rammerne af det internationale samarbejde

191. Databeskyttelsesrådet bemærker også, at Europa-Kommissionen som led i sin vurdering af tilstrækkeligheden ikke tog hensyn til eksisterende internationale aftaler indgået mellem Det Forenede Kongerige og tredjelande eller internationale organisationer, der kan fastsætte specifikke bestemmelser for efterretningstjenesters internationale videregivelse af personoplysninger til tredjelande.

192. Databeskyttelsesrådet understreger også, at Europa-Kommissionens vurdering hovedsagelig bygger på vurderingen af del 4 i DPA 2018, og er navnlig bekymret over, at IPA 2016 fokuserer på "anmodninger" om udveksling af efterretninger med udenlandske partnere, men ikke behandler andre former for udveksling af efterretninger. Databeskyttelsesrådet bemærker i denne forbindelse, at Europa-Kommissionens udkast til afgørelse ikke indeholder henvisning til eller vurdering af sammenhængen mellem den britiske retlige ramme og kommunikationsefterretningsaftalen "UK-US Communication Intelligence Agreement" ("UK-USA-CI-aftalen"). I en nylig erklæring i anledningen af 75-årsdagen for denne aftale, nævnte USA's National Security Agency (i det følgende benævnt "NSA"), at dette partnerskab gør det muligt "*så vidt muligt at udveksle oplysninger mellem de to agenturer med minimale restriktioner*", og at "*dette banebrydende dokument har dannet grundlag for politikker og procedurer for udveksling af kommunikation, oversættelse, analyse og krypteringsoplysninger mellem britiske og amerikanske efterretningseksperter*".[130] Denne aftale dannede også grundlag for andre efterretningspartnerskaber med Australien, Canada, og New Zealand.

193. Aftalens hemmelige karakter og specifikke bestemmelser indebærer alvorlige udfordringer med hensyn til lovgivningens klarhed og forudsigelighed ved videreanvendelse og oversøisk videregivelse af oplysninger indsamlet af britiske myndigheder til nationale sikkerhedsformål. I denne forbindelse minder Databeskyttelsesrådet om, at EU-Domstolen med hensyn til det beskyttelsesniveau, der er garanteret i EU, har understreget, at lovgivning, der indebærer indgreb i den grundlæggende ret til beskyttelse af personoplysninger, skal "*fastsætte klare og præcise regler for anvendelsesområdet for og anvendelsen af en foranstaltning og sikre minimumsgarantier, således at de personer, hvis personoplysninger er omfattet, har garanti for en effektiv og tilstrækkelig beskyttelse af deres personoplysninger mod risiko for misbrug og ulovlig adgang til og brug af oplysningerne. Behovet for at råde over sådanne garantier er så meget desto større, når personoplysningerne undergives automatisk databehandling, og der eksisterer en betydelig risiko for ulovlig adgang til disse oplysninger*"[131]. Databeskyttelsesrådet mener derfor, at Europa-Kommissionen bør overveje virkningen af UK-USA-CI-aftalen som en del af tilstrækkelighedsvurderingen.

194. Menneskerettighedsdomstolen har i sin dom i første afdeling af 13. september 2018 i sagen Big Brother Watch vurderet den britiske ordning for udveksling af efterretninger og navnlig UK-USA-CI-aftalen. Menneskerettighedsdomstolen fastslog, at "*[d]e retlige rammer, der giver de britiske efterretningstjenester mulighed for at anmode udenlandske efterretningstjenester om aflyttet materiale, ikke indgår i RIPA*. *UK-USA-CI-aftalen af 5. marts 1946 indebærer specifikt mulighed for*

[130] Se pressemeddelelse fra NSA, GCHQ and NSA Celebrate 75 Years of Partnership, af 5. februar 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.
[131] Se Schrems I, præmis 91.

udveksling af materialer mellem USA og Det Forenede Kongerige"[132] og fremsatte den betragtning, at der er "*retligt grundlag for at anmode om efterretninger fra udenlandske efterretningstjenester, og at loven er tilstrækkeligt tilgængelig*[133]." Mens Menneskerettighedsdomstolen har konkluderet, at der ikke foreligger overtrædelse af artikel 8[134] i EMRK i forbindelse med ordningen for udveksling af efterretninger, bemærker Databeskyttelsesrådet, at dommen nu er videregivet til Store Afdeling, som endnu ikke har fremsat sin afgørelse. Databeskyttelsesrådet bemærker også, at dommer Koskelo i en delvist samstemmende, delvist afvigende holdning til denne dom, sammen med dommer Turković[135], har konkluderet, at der er tale om en overtrædelse af artikel 8 i EMRK i forbindelse med ordningen for udveksling af efterretninger, idet det hedder, at "*[d]et er let at tilslutte sig princippet om, at enhver ordning, hvorefter efterretninger fra aflyttede kommunikationer indhentes via udenlandske efterretningstjenester, uanset om det sker på grundlag af anmodninger om at foretage en sådan aflytning eller om at formidle resultaterne, ikke må medføre en tilsidesættelse af de garantier, som skal stilles ved overvågning foretaget af de nationale myndigheder (se præmis 216, 423 og 447). Alle andre fremgangsmåder ville være utænkelige".*

195. Som det fremgår af flere rapporter fra medierne og ikkestatslige organisationer[136][137], stammer den seneste offentliggjorte udgave af UK-USA-CI-aftalen fra 1956, og siden da har kommunikationsteknologien og karakteren af signalefterretninger ændret sig betydeligt. Medierapporter har f.eks. afsløret, at data, der overføres via undersøiske kabler til Det Forenede Kongerige, opfanges af GCHQ og gøres tilgængelige for NSA[138].

196. For Databeskyttelsesrådet er et centralt spørgsmål i forbindelse med udveksling af efterretninger, om § 109 i DPA 2018 og bestemmelserne i IPA 2016 fortsat finder anvendelse, når britiske efterretningstjenester handler i overensstemmelse med UK-USA-CI-aftalen. Et andet centralt element, der skal vurderes, er, om bestemmelserne i eller den effektive anvendelse af denne aftale påvirker beskyttelsesniveauet for personoplysninger under overførsel fra EØS til Det Forenede Kongerige eller giver andre tredjelandes efterretningstjenester direkte adgang til og mulighed for erhvervelse af personoplysninger.

197. Ud over de forbehold, der er givet udtryk for med hensyn til "oversøisk videregivelse" på grundlag af del 4 i DPA 2018 og den dertil knyttede undtagelse i forhold vedrørende statens sikkerhed samt anmodninger inden for rammerne af IPA 2016, **er Databeskyttelsesrådet derfor bekymret over andre former for informationsudveksling og videregivelse på grundlag af andre instrumenter, især de forskellige internationale aftaler, som Det Forenede Kongerige har indgået med andre tredjelande, navnlig hvor disse instrumenter fortsat er utilgængelige for offentligheden, såsom UK-USA-CI-aftalen. Virkningen af en sådan**

[132] Se Menneskerettighedsdomstolen, Big Brother Watch, præmis 425.
[133] Se Menneskerettighedsdomstolen, Big Brother Watch, præmis 427.
[134] Se Menneskerettighedsdomstolen, Big Brother Watch, præmis 448.
[135] Se Menneskerettighedsdomstolen, Big Brother Watch, dommer Koskelos delvist samstemmende, delvist afvigende holdning, som deles af dommer Turković.
[136] Se BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes, af 5. marts 2021, https://www.bbc.com/news/uk-56284453.
[137] Se Privacy International, Policy Briefing — UK Intelligence Sharing Arrangements, af april 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] Se The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, af 21. juni 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

aftale kan blive, at de garantier, der gives i forbindelse med adgang og anvendelse af personoplysninger til nationale sikkerhedsformål, omgås.

198. Databeskyttelsesrådet deler det synspunkt, som FN's særlige rapportør, Joe Cannatacci, har givet udtryk for, nemlig at "*[u]dveksling af efterretninger ikke må udgøre en genvej til at indhente eller gøre det lettere for andre at indhente efterretninger uden overholdelse af de nationale garantier eller give udenlandske regeringer med lavere standarder for beskyttelse af privatlivets fred (eller andre menneskerettigheder) mulighed for at indhente efterretninger fra britiske efterretningstjenester, der kan give anledning til menneskerettighedskrænkelser*"[139].

199. **Databeskyttelsesrådet er desuden af den opfattelse, at indgåelsen af bilaterale eller multilaterale aftaler med tredjelande med henblik på efterretningssamarbejde som retsgrundlag for direkte aflytning og indsamling af personoplysninger eller overførsel af personoplysninger til de pågældende lande også kan få betydelig indflydelse på betingelserne for videreanvendelse af de indsamlede oplysninger, eftersom sådanne aftaler sandsynligvis vil berøre den britiske databeskyttelsesramme i den form, hvori den er vurderet.**

4.3.3. Tilsyn

200. Databeskyttelsesrådet understreger betydningen af, at uafhængige tilsynsmyndigheder fører et omfattende tilsyn for at sikre et passende databeskyttelsesniveau. Garantien for tilsynsmyndighedernes uafhængighed som omhandlet i artikel 8, stk. 3, i chartret har til formål at sikre en effektiv og pålidelig kontrol med overholdelsen af reglerne om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

201. Når personoplysninger tilgås og anvendes til nationale sikkerhedsformål, varetages tilsynsfunktionen hovedsagelig af kommissæren for undersøgelsesbeføjelser og retskommissærerne (i det følgende benævnt "retskommissærerne").

202. **Databeskyttelsesrådet anerkender generelt, at indførelsen af retskommissærer med IPA 2016 er en klar forbedring.** I overensstemmelse med ovennævnte anmodning opfordres Europa-Kommissionen til at foretage en mere detaljeret vurdering af **retskommissærernes uafhængighed, og navnlig i hvilket omfang kommissæren for undersøgelsesbeføjelsers uafhængighed og dennes kontors (i det følgende benævnt "IPCO") uafhængighed er juridisk sikret, da dette ikke fremgår af IPA 2016.** Dette er særligt vigtigt, da kommissæren for undersøgelsesbeføjelser træffer afgørelse om klager fra regeringen, hvis en retskommissær har **afvist** en anmodning om en **overvågningsforanstaltning**.

203. Kommissæren for undersøgelsesbeføjelser udfører både forudgående og efterfølgende tilsynsfunktioner. Med hensyn til forudgående tilsyn forstår Databeskyttelsesrådet, at retskommissærernes funktion i individuelle sager er at godkende forskellige overvågningsforanstaltninger, herunder målrettet aflytning og masseindsamling af kommunikationsdata. Databeskyttelsesrådet bemærker endvidere, at forudgående godkendelse af

[139] Se End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, London, af 29. juni 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

overvågningsforanstaltninger ikke på baggrund af EU-Domstolens retspraksis kan tolkes som et absolut krav i forbindelse med tilsynsforanstaltningernes proportionalitet[140].

204. For at vurdere tilsynsniveauets effektivitet mener Databeskyttelsesrådet dog, at der er behov for en yderligere præcisering af de scenarier, hvor en lovlig aflytning uden forudgående godkendelse fra retskommissærerne er mulig.

205. I afgørelsesudkastet nævner Europa-Kommissionen i fodnote 201 og 266 "specifikke begrænsede tilfælde", der er omhandlet i IPA 2016, §§ 44-52, med hensyn til målrettet aflytning. Databeskyttelsesrådet bemærker, at §§ 45-51 i IPA 2016 er undtagelser, der angiveligt ikke anvendes regelmæssigt af efterretningstjenesterne. **Databeskyttelsesrådet forstår** endvidere, at i de **tilfælde, hvor undtagelserne finder anvendelse** (f.eks. telekommunikations- og postvirksomheder), skal retskommissærerne foretage en forhåndsgodkendelse, hvis retshåndhævende myndigheder eller efterretningstjenester **anmoder** om adgang til data, **og opfordrer Europa-Kommissionen til i sin afgørelse at bekræfte, at dette er korrekt**.

206. Databeskyttelsesrådet anerkender, at § 44, stk. 2, i IPA 2016 giver mulighed for aflytning af kommunikation, hvis en af parterne (afsender eller modtager) har givet sit samtykke, og der foreligger en tilladelse i henhold til RIPA 2000 eller Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp. 11), dvs. den tidligere retlige situation før etableringen af retskommissærerne. Databeskyttelsesrådet **opfordrer** Europa-Kommissionen til at præcisere, om dette betyder, at forhåndsgodkendelsesproceduren aldrig finder anvendelse i tilfælde, hvor der foreligger et ensidigt samtykke.

207. Med hensyn til efterfølgende tilsyn er det også vigtigt at kontrollere, at der sikres et effektivt uafhængigt tilsyn uden undtagelsestilfælde, navnlig når forudgående kontrol ikke foretages.

208. Databeskyttelsesrådet bemærker, at der for §§ 48-52 i IPA 2016 foretages en efterfølgende kontrol af retskommissærerne, og **opfordrer Europa-Kommissionen til at præcisere, i henhold til hvilke krav og på hvilket initiativ en sådan efterfølgende kontrol skal foretages**.

209. I henhold til § 229, stk. 4, i IPA 2016 skal kommissæren for undersøgelsesbeføjelser ikke overvåge udøvelsen af visse funktioner. I den forbindelse opfordrer Databeskyttelsesrådet Europa-Kommissionen til at præcisere bestemmelserne i § 229, stk. 4, litra d) og e), i IPA 2016 vedrørende den praktiske betydning for de kontrolmæssige beføjelser, der påhviler kommissæren for undersøgelsesbeføjelser. **Databeskyttelsesrådet er af den opfattelse, at ICO er den kompetente tilsynsmyndighed, hvor undtagelserne i § 229, stk. 4, i IPA 2016 finder anvendelse, og Databeskyttelsesrådet opfordrer Europa-Kommissionen til i sin afgørelse at bekræfte, at dette er korrekt.**

210. **Det ser ud til, at kommissæren for undersøgelsesbeføjelsers rolle i forbindelse med** efterfølgende tilsyn er **begrænset** til at fremsætte henstillinger i tilfælde af manglende overholdelse og til at underrette den registrerede, hvis fejlen er alvorlig, og det er i offentlighedens interesse, at personen underrettes. **Databeskyttelsesrådet opfordrer Europa-Kommissionen til at præcisere, hvordan IPCO effektivt kan sikre overholdelse af lovgivningen.**

[140] Databeskyttelsesrådet bemærker dog også, at EU-Domstolen i forbindelse med ugyldiggørelsen af værnet om privatlivets fred i Schrems II har noteret sig, at den såkaldte FISA-domstol i henhold til amerikansk ret "*ikke tillader individuelle overvågningsforanstaltninger*. *Den tillader snarere overvågningsprogrammer (såsom PRISM og UPSTREAM) på grundlag af årlige certificeringer*" (præmis 179).

211. **Endelig forstår Databeskyttelsesrådet, at berørte personer ikke kan henvende sig direkte til IPCO, men skal indgive en klage til ICO, som dog har begrænsede beføjelser vedrørende statens sikkerhed. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til yderligere at præcisere, hvordan det er juridisk sikret, at IPCO behandler klager i disse sager.**

4.3.4. Adgang til retsmidler

212. På baggrund af EU-Domstolens domme i sagerne Schrems I og Schrems II er det klart, at effektiv retsbeskyttelse som omhandlet i artikel 47 i chartret er af afgørende betydning for at antage, at lovgivningen i et tredjeland er tilstrækkelig. Afgørelserne har også vist, at der i denne forbindelse skal lægges særlig vægt på effektiv retsbeskyttelse ved adgang til personoplysninger i sager vedrørende statens sikkerhed.

213. **Databeskyttelsesrådet anerkender, at Det Forenede Kongerige har etableret retten vedrørende undersøgelsesbeføjelser. Denne ret har ikke kun kompetence til at behandle sager om retshåndhævende myndigheders anvendelse af undersøgelsesbeføjelser, men også efterretningstjenesternes. Derfor er det Databeskyttelsesrådets opfattelse, at retten vedrørende undersøgelsesbeføjelser fungerer som en egentlig domstol som omhandlet i artikel 47 i chartret. Med hensyn til beføjelserne opfordres Europa-Kommissionen til at bekræfte, at retten vedrørende undersøgelsesbeføjelser har alle de beføjelser, der er nævnt i betragtning 262 i afgørelsesudkastet, uanset retsgrundlaget for klagen.**

214. Diskret overvågning foretaget af efterretningstjenesterne vil ofte betyde, at genstanden for overvågningen, den registrerede, er ubekendt med overvågningen og forbliver det. Da Databeskyttelsesrådet i denne forbindelse var nødt til at analysere amerikansk ret, har det mange gange givet udtryk for sin betænkelighed over kravet om "søgsmålskompetence" som fortolket i amerikansk ret i overvågningssager. På denne baggrund bemærker Databeskyttelsesrådet, at klagen vedrørende retten vedrørende undersøgelsesbeføjelser kun kræver påvisning af en "formodning", hvor klageren skal påvise, at vedkommende risikerer at blive genstand for en foranstaltning.

215. Ved analysen af retten vedrørende undersøgelsesbeføjelser lægger Databeskyttelsesrådet også særlig vægt på, at det gentagne gange er blevet konstateret, at retten fungerer i overensstemmelse med EMRK, som fortolket af Menneskerettighedsdomstolen.