Udtalelse 5/2023 om Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i henhold til databeskyttelsesrammen mellem EU og USA

Vedtaget den 28. februar 2023

Sammenfatning

Den 13. december 2022 offentliggjorde Europa-Kommissionen et udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet ("udkast(et) til afgørelse"), som indeholder bilag, der udgør en ny ramme for transatlantisk udveksling af personoplysninger, databeskyttelsesrammen mellem EU og USA ("databeskyttelsesrammen, DPF"), som skal erstatte det tidligere amerikanske privatlivsskjold, som blev erklæret ugyldigt af Den Europæiske Unions Domstol ("Domstolen") den 16. juli 2020 i Schrems II-sagen. Det centrale element i databeskyttelsesrammen er principperne til databeskyttelsesrammen mellem EU og USA, herunder de supplerende principper (under ét "DPF-principperne").

I overensstemmelse med artikel 70, stk. 1, litra s), i Europa-Parlamentets og Rådets forordning (EU) 2016/679[1] ("GDPR") anmodede Kommissionen Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") om en udtalelse om udkastet til afgørelse.

Databeskyttelsesrådet vurderede tilstrækkeligheden af beskyttelsesniveauet i USA på grundlag af gennemgangen af udkastet til afgørelse. Databeskyttelsesrådet vurderede både de kommercielle aspekter og adgangen til og anvendelsen af personoplysninger, der overføres fra EU af offentlige myndigheder i USA.

Databeskyttelsesrådet tog hensyn til EU's gældende retlige ramme for databeskyttelse som fastsat i GDPR samt de grundlæggende rettigheder til privatliv og databeskyttelse som nedfældet i artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 8 i den europæiske menneskerettighedskonvention. Det tog også hensyn til retten til effektive retsmidler og til en upartisk domstol som fastsat i chartrets artikel 47 samt retspraksis vedrørende de forskellige grundlæggende rettigheder.

Databeskyttelsesrådet har desuden taget hensyn til kravene i den reference til tilstrækkeligheden, som Databeskyttelsesrådet har vedtaget[2].

Databeskyttelsesrådets vigtigste mål er at afgive en udtalelse til Kommissionen om tilstrækkeligheden af beskyttelsesniveauet for personer, hvis personoplysninger overføres til USA. Det er vigtigt at anerkende, at Databeskyttelsesrådet ikke forventer, at de amerikanske databeskyttelsesrammer er en nøjagtig gengivelse af den europæiske databeskyttelseslovgivning.

Databeskyttelsesrådet minder imidlertid om, at artikel 45 i GDPR og EU-Domstolens retspraksis for at kunne anses for at sikre et tilstrækkeligt beskyttelsesniveau kræver, at tredjelandets lovgivning sikrer registrerede et beskyttelsesniveau, der i det væsentlige svarer til det, der garanteres i EU.

1.1. Generelle databeskyttelsesaspekter

I henhold til databeskyttelsesrammen kan foretagender i databeskyttelsesrammen i deres overholdelse af DPF-principperne være begrænset i visse tilfælde (f.eks. i det omfang det er nødvendigt for at efterkomme en retsafgørelse eller for at tilgodese offentlighedens interesse). For bedre at kunne påpege virkningen af disse undtagelser på beskyttelsesniveauet for registrerede anbefaler Databeskyttelsesrådet, at Kommissionen i udkastet til afgørelse medtager en præcisering af

[1] 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 (den generelle forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).
[2] Artikel 29-Gruppen, **Error! Hyperlink reference not valid.**.

undtagelsernes anvendelsesområde, herunder de gældende garantier i henhold til amerikansk lovgivning.

Databeskyttelsesrådet bemærker, at bilagenes struktur og nummerering gør det temmelig vanskeligt at finde og henvise til oplysningerne. Dette bidrager til en overordnet kompleks præsentation af den nye ramme, som i bilagene indeholder dokumenter af forskellig juridisk værdi, og som måske ikke fremmer en god forståelse af DPF-principperne hos registrerede, foretagender i databeskyttelsesrammen og EU's databeskyttelsesmyndigheder. Databeskyttelsesrådet understreger også, at terminologien bør anvendes konsekvent i hele databeskyttelsesrammen. På samme måde mangler der en definition af visse væsentlige begreber[3].

Databeskyttelsesrådet glæder sig over ajourføringerne af DPF-principperne[4], som vil udgøre den bindende retlige ramme for foretagender i databeskyttelsesrammen, men bemærker, at på trods af en række ændringer og yderligere forklaringer i betragtningerne til udkastet til afgørelse forbliver de DPF-principper, som foretagenderne i databeskyttelsesrammen skal overholde, i det væsentlige uændrede i forhold til dem, der finder anvendelse under privatlivsskjoldet (som var baseret på Artikel 29-arbejdsgruppens ("Artikel 29-Gruppen") og Databeskyttelsesrådets årlige fælles evalueringer). DPF-principperne er også i vid udstrækning de samme som dem i udkastet til privatlivsskjoldet, som Artikel 29-Gruppen baserede sin udtalelse fra 2016 på[5]. For så vidt angår de DPF-principper, der i det væsentlige er uændrede, finder Databeskyttelsesrådet det ikke nødvendigt at gentage alle de bemærkninger, der tidligere er fremsat af Artikel 29-Gruppen. Databeskyttelsesrådet har besluttet at fokusere på specifikke aspekter, som det anser for at være endnu mere relevante i dag i lyset af udviklingen i det retlige og teknologiske miljø.

Databeskyttelsesrådet bemærker f.eks., at nogle spørgsmål, der tidligere er blevet rejst af Artikel 29-Gruppen og Det Europæiske Databeskyttelsesråd i forbindelse med principperne for privatlivsskjoldet, fortsat er gyldige. Disse vedrører navnlig de registreredes rettigheder (f.eks. visse undtagelser fra retten til indsigt og tidsplanen og de nærmere bestemmelser for retten til at gøre indsigelse), manglen på centrale definitioner, den manglende klarhed med hensyn til anvendelsen af principperne til databeskyttelsesrammen på databehandlere og den brede undtagelse for offentligt tilgængelige oplysninger[6].

Databeskyttelsesrådet vil også gerne gentage, at beskyttelsesniveauet for personer, hvis oplysninger overføres, ikke må undermineres af videreoverførsler fra den oprindelige modtager af de overførte oplysninger[7]. Databeskyttelsesrådet opfordrer endnu en gang Kommissionen til at præcisere, at de garantier, som den oprindelige modtager pålægger importøren i tredjelandet, skal være effektive i lyset af tredjelandets lovgivning forud for en videreoverførsel inden for rammerne af databeskyttelsesrammen.

Den hurtige udvikling inden for automatiseret beslutningstagning og profilering — i stigende grad ved hjælp af AI-teknologier — kræver særlig opmærksomhed. Databeskyttelsesrådet glæder sig over

[3] Dette er tilfældet for udtrykkene "mandatar" og "databehandler". Desuden mangler begrebet "data om menneskelige ressourcer (HR-data)" stadig at blive drøftet med de amerikanske myndigheder.
[4] F.eks. præciseringen af, at nøglekodede oplysninger er personoplysninger.
[5] Artikel 29-Gruppen, Opinion 01/2016 on the EU-U.S.Privacy Shield draft adequacy decision, vedtaget den 13. april 2016 (i det følgende benævnt "Artikel 29-Gruppens udtalelse 01/2016")
[6] EU.U.S. Privacy Shield — Third Annual Joint Review, Databeskyttelsesrådets rapport vedtaget den 12. november 2019, punkt 11.
[7] Reference vedrørende et tilstrækkeligt beskyttelsesniveau, 3.A.9.

Kommissionens henvisninger til specifikke garantier i den relevante amerikanske lovgivning på forskellige områder[8]. Beskyttelsesniveauet for fysiske personer synes imidlertid at variere alt efter, hvilke sektorspecifikke regler — om nogen — der finder anvendelse på den foreliggende situation. Databeskyttelsesrådet fastholder, at der er behov for specifikke regler om automatisk beslutningstagning for at sikre tilstrækkelige garantier, herunder retten for den enkelte til at kende den involverede logik, til at anfægte afgørelsen og til at opnå menneskelig indgriben, når afgørelsen i væsentlig grad påvirker vedkommende.

Databeskyttelsesrådet minder om betydningen af effektivt tilsyn med og håndhævelse af databeskyttelsesrammen og mener, at overensstemmelseskontrol for så vidt angår mere væsentlige krav er afgørende. Disse aspekter vil blive nøje overvåget af Databeskyttelsesrådet, herunder i forbindelse med de periodiske evalueringer. Databeskyttelsesrådet noterer sig de fornyede tilsagn i skrivelserne fra Federal Trade Commission ("FTC") (den føderale handelskommission)[9] og det amerikanske transportministerium ("transportministeriet")[10] for så vidt angår håndhævelse, f.eks. med henblik på at prioritere undersøgelsen af påståede overtrædelser af databeskyttelsesesrammen.

Databeskyttelsesrådet bemærker, at der stilles syv klagemuligheder til rådighed for registrerede i EU, hvis deres personoplysninger behandles i strid med databeskyttelsesrammen. Disse klagemekanismer er de samme som dem, der indgik i det tidligere privatlivsskjold, som havde været genstand for bemærkninger fra Artikel 29-Gruppen[11]. Effektiviteten af disse klagemekanismer vil blive nøje overvåget af Databeskyttelsesrådet, herunder i forbindelse med de periodiske evalueringer.

1.2. Amerikanske offentlige myndigheders adgang til og brug af personoplysninger overført fra Den Europæiske Union

I udkastet til afgørelse konkluderer Europa-Kommissionen, at "ethvert indgreb i offentlighedens interesse, navnlig med henblik på strafferetlig håndhævelse og af hensyn til den nationale sikkerhed, fra de amerikanske offentlige myndigheders side i de grundlæggende rettigheder for de personer, hvis personoplysninger overføres fra Unionen til USA i henhold til databeskyttelsesrammen for EU og USA, vil være begrænset til, hvad der er strengt nødvendigt for at nå det pågældende legitime mål, og at der findes en effektiv retsbeskyttelse mod et sådant indgreb"[12].

Europa-Kommissionen når frem til sin konklusion efter en omfattende vurdering af Executive Order (præsidentielt dekret) 14086, der skærper garantierne for amerikanske signalefterretningsaktiviteter (EO 14086). EO 14086 blev udstedt af den amerikanske præsident den 7. oktober 2022 efter forhandlinger mellem Europa-Kommissionen og den amerikanske regering efter Den Europæiske Unions Domstols (EU-Domstolens) ugyldiggørelse af den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet, kaldet privatlivsskjoldet.

Databeskyttelsesrådet ser med tilfredshed på, at ikke blot ikrafttrædelsen, men også vedtagelsen af afgørelsen bl.a. er betinget af, at alle amerikanske efterretningstjenester vedtager ajourførte politikker og procedurer for gennemførelse af EO 14086. Databeskyttelsesrådet anbefaler Kommissionen at vurdere disse ajourførte politikker og procedurer og dele denne vurdering med Databeskyttelsesrådet.

Med hensyn til statslig adgang til personoplysninger, der overføres til USA, har Databeskyttelsesrådet i sin analyse fokuseret på vurderingen af den nye EO 14086, da den reelt har til formål at tage hånd

[8] Udkast til afgørelse, betragtning 35.
[9] Udkast til afgørelse, bilag IV.
[10] Udkast til afgørelse, bilag V.
[11] Se navnlig Artikel 29-gruppens udtalelse 01/2016, afsnit 2.2.6, litra a).
[12] Udkast til afgørelse, betragtning 195.

om og afhjælpe de mangler, som EU-Domstolen påpegede i sin dom i Schrems II-sagen, da den fastslog, at den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet var ugyldig.

Databeskyttelsesrådet anerkender, at USA's retlige ramme for signalefterretningsaktiviteter er blevet ændret ved vedtagelsen af EO 14086, og det betragter de yderligere garantier i dette dekret som en betydelig forbedring. Med EO 14086 indføres begreberne nødvendighed og proportionalitet i USA's retlige ramme for signalefterretninger, og hvis EU udpeges som et kvalificeret regionalt foretagende for økonomisk integration, indføres der en ny klagemekanisme for EU-borgere. Databeskyttelsesrådet mener, at den nye klagemekanisme er væsentligt forbedret i forhold til den tidligere såkaldte ombudsmandsmekanisme under privatlivsskjoldet. I modsætning til den tidligere retlige ramme, som ikke skabte rettigheder for fysiske personer i EU, således som EU-Domstolen udtrykkeligt bemærkede, skaber den nye EO 14086 sådanne rettigheder, og den giver flere garantier for databeskyttelsesrettens uafhængighed og mere effektive beføjelser til at afhjælpe overtrædelser.

Ved at sammenligne de yderligere garantier i EO 14086 med det, som Databeskyttelsesrådet har udformet som de europæiske væsentlige garantier (EEG'er), som den standard, der er udarbejdet på grundlag af EU-Domstolens og Den Europæiske Menneskerettighedsdomstols retspraksis, har Databeskyttelsesrådet i sin vurdering stadig udpeget en række punkter, hvor der er behov for yderligere præciseringer, og som kræver opmærksomhed eller vækker bekymring. Disse punkter afspejler, at selv om Databeskyttelsesrådet baserede sin udtalelse på dommen i Schrems II-sagen, omfatter anvendelsesområdet for Databeskyttelsesrådets vurdering nødvendigvis betragtninger, der går ud over de specifikke konklusioner i dommen i Schrems II-sagen.

Databeskyttelsesrådet mener, at der er behov for yderligere afklaring af spørgsmål, navnlig vedrørende "midlertidig masseindsamling" og yderligere opbevaring og formidling af de (masse)indsamlede data inden for USA's retlige rammer.

Da testen af væsentlig ækvivalens ikke er en identitetstest, og da de garantier, der indgår i den nye retlige ramme for signalefterretninger, er blevet styrket, er Databeskyttelsesrådets primære fokus og bekymring en vurdering af garantierne i deres helhed efter en holistisk tilgang, der omfatter garantierne for hele behandlingscyklussen, fra indsamling af data til formidling af data, herunder tilsyns- og klageelementer.

I denne forbindelse fremhæver Databeskyttelsesrådet følgende konklusioner:

Databeskyttelsesrådet anerkender, at EO 14086 indfører begreberne nødvendighed og proportionalitet i den retlige ramme for signalefterretninger, men understreger behovet for nøje at overvåge virkningerne af disse ændringer i praksis, herunder evalueringen af interne politikker og procedurer til gennemførelse af garantierne i dekretet på agenturniveau.

Databeskyttelsesrådet glæder sig også over, at EO 14086 indeholder en liste over specifikke formål, hvortil indsamling kan og ikke kan finde sted, samtidig med at det bemærker, at målene kan opdateres med yderligere — ikke nødvendigvis offentlige — mål i lyset af nye krav til den nationale sikkerhed.

Som et minus i de nuværende rammer har Databeskyttelsesrådet navnlig konstateret, at den amerikanske retlige ramme, når den tillader masseindsamling af data i henhold til Executive Order 12333, mangler kravet om forudgående tilladelse fra en uafhængig myndighed som krævet i Menneskerettighedsdomstolens seneste retspraksis, og at den heller ikke foreskriver en systematisk uafhængig efterfølgende kontrol foretaget af en domstol eller et tilsvarende uafhængigt organ. Med hensyn til forudgående uafhængig tilladelse til overvågning i henhold til Section 702 i FISA beklager Databeskyttelsesrådet, at FISA-domstolen ("FISC") ikke gennemgår en programansøgning med henblik

på overholdelse af EO 14086, når den certificerer programmet, der giver tilladelse til målretning mod ikkeamerikanske personer, selv om de efterretningsmyndigheder, der gennemfører programmet, er bundet heraf. Databeskyttelsesrådet er af den opfattelse, at de yderligere garantier i dette dekret ikke desto mindre bør tages i betragtning, herunder af FISC. Databeskyttelsesrådet minder om, at rapporter fra Privacy and Civil Liberties Oversight Board ("PCLOB") (rådet for tilsyn med privatlivets fred og borgerlige rettigheder) vil være særligt nyttige til at vurdere, hvordan garantierne i EO 14086 vil blive gennemført, og hvordan disse garantier anvendes, når data indsamles i henhold til Section 702 i FISA og EO 12333.

Med hensyn til klagemekanismen anerkender Databeskyttelsesrådet betydelige forbedringer med hensyn til appeldomstolen for databeskyttelses (Data Protection Review Court, "DPRC") beføjelser og dens øgede uafhængighed i forhold til ombudsmanden. Databeskyttelsesrådet anerkender også de yderligere garantier, der er fastsat i den nye klagemekanisme, såsom den rolle, som de særlige advokater spiller, når de agerer i klagerens interesser, og PCLOB's gennemgang af klagemekanismen. Under hensyntagen til karakteren af den nationale sikkerhed og de garantier, der er fastsat i EO 14086, er Databeskyttelsesrådet ikke desto mindre bekymret over den generelle anvendelse af DPRC's standardsvar, der underretter klageren om, at der enten ikke er konstateret nogen omfattede overtrædelser, eller at der er truffet en afgørelse, der kræver passende afhjælpning, og at det ikke kan appelleres under ét. I betragtning af betydningen af klagemekanismen opfordrer Databeskyttelsesrådet Kommissionen til nøje at overvåge, hvordan denne mekanisme fungerer i praksis.

Databeskyttelsesrådet forventer, at Kommissionen følger op på sit tilsagn om at suspendere, ophæve eller ændre afgørelsen om tilstrækkeligheden af beskyttelsesniveauet på grund af sagens hastende karakter, navnlig hvis den amerikanske regering beslutter at begrænse de garantier, der er indeholdt i dekretet[13].

Samlet set noterer Databeskyttelsesrådet sig med tilfredshed de væsentlige forbedringer, som dekretet tilbyder i forhold til den tidligere retlige ramme, navnlig med hensyn til indførelsen af principperne om nødvendighed og proportionalitet og den individuelle klagemekanisme for registrerede i EU. I betragtning af de betænkeligheder, der er givet udtryk for, og de nødvendige præciseringer foreslår Databeskyttelsesrådet, at disse betænkeligheder bør imødegås, og at Kommissionen fremlægger de ønskede præciseringer med henblik på at styrke begrundelserne for udkastet til afgørelse og sikre en nøje overvågning af den konkrete gennemførelse af denne nye retlige ramme, navnlig de garantier, den giver, i de fremtidige fælles evalueringer.

[13] Udkast til afgørelse, betragtning 212.

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har

Det Europæiske Databeskyttelsesråd har vedtaget følgende erklæring:

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 ("GDPR")[1],

under henvisning til 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[2],

under henvisning til artikel 12 og artikel 22 i Databeskyttelsesrådets forretningsorden —

VEDTAGET FØLGENDE UDTALELSE

1 INDLEDNING

1.1 Den amerikanske databeskyttelsesramme

1. De Forenede Stater ("USA") og Den Europæiske Union ("EU") har forskellige tilgange til privatlivets fred og databeskyttelse. Privatlivets fred og databeskyttelse i EU er grundlæggende rettigheder, der er sikret ved artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder, mens databeskyttelse i USA generelt behandles ud fra et forbrugerbeskyttelsesperspektiv. Som følge heraf er de lovgivningsmæssige tilgange i USA og EU forskellige[3].

2. USA adskiller sig fra EU's samlede tilgang i GDPR, idet der ikke findes nogen omfattende generel databeskyttelseslovgivning på føderalt plan. Beskyttelsen af privatlivets fred i USA sker snarere gennem en sektortilgang og en statslig tilgang. Nogle specifikke sektorer er f.eks. omfattet af specifikke retsakter, såsom:

   - Health Insurance Portability and Accountability Act (HIPAA)[4]

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EØS-relevant tekst) (EUT L 119 af 4.5.2016, s. 1).
[2] Henvisninger til "medlemsstater" i denne udtalelse skal forstås som henvisninger til "EØS-medlemsstater".
[3] Se også European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, offentliggjort den 13. december 2022 (i det følgende benævnt "udkast(et) til afgørelse"), bilag I, afsnit I.
[4] Health Insurance Portability and Accountability Act of 1996 (HIPAA) er en amerikansk føderal lov. I den fastsættes nationale standarder for at beskytte patienters følsomme sundhedsoplysninger. Målet med HIPAA er at beskytte fysiske personers sundhedsoplysninger tilstrækkeligt, samtidig med der sikres en strøm af sundhedsoplysninger med henblik på levering og fremme af sundhedspleje af høj kvalitet. HIPAA regulerer anvendelsen og videregivelsen af sundhedsoplysninger hos enheder, der er omfattet af reglerne om beskyttelse af privatlivets fred. Dette omfatter også standarder for fysiske personers ret til at forstå og kontrollere, hvordan deres sundhedsoplysninger anvendes.

- Children's Online Privacy Protection Act (COPPA)[5]
- Gramm-Leach-Bliley Act (GLBA)[6]

3. Med hensyn til offentlig adgang til personoplysninger, der overføres fra EU til USA, gælder der en række forskellige retsgrundlag, begrænsninger og garantier. De retlige procedurer for adgang til oplysninger med henblik på retshåndhævelse følger enten direkte af den amerikanske forfatning (fjerde amendment), af love og procesret eller af justitsministeriets retningslinjer og politikker på føderalt niveau eller på delstatsniveau. Adgang til oplysninger til nationale sikkerhedsformål er reguleret af flere retsakter, navnlig Foreign Intelligence Surveillance Act (FISA), Executive Order 12333, det nyligt vedtagne Executive Order 14086 samt Attorney General Regulation ("AG Regulation")[7] om oprettelse af en appeldomstol for databeskyttelse (Data Protection Review Court, "DPRC").

4. Den 13. december 2022 udsendte Kommissionen sit udkast til Kommissionens gennemførelsesafgørelse i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om et tilstrækkeligt beskyttelsesniveau for personoplysninger i henhold til databeskyttelsesrammen mellem EU og USA ("udkast(et) til afgørelse"), som i bilaget indeholder rammen for databeskyttelse mellem EU og USA ("databeskyttelsesrammen"). Af ovennævnte grunde er udkastet til afgørelse ikke baseret på en specifik og omfattende føderal retlig ramme, men på databeskyttelsesrammen.

5. Databeskyttelsesrammen fungerer på følgende måde: *"Det amerikanske handelsministerium ("ministeriet") opstiller principperne til en databeskyttelsesramme mellem EU og USA, herunder de supplerende principper (samlet benævnt "principperne") og bilag I til principperne ("bilag I"), i henhold til dets lovbestemte bemyndigelse med henblik på at fremme og udvikle den internationale handel (United States Code, afsnit 15, § 1512)"*[8].

6. "Principperne" ("principperne til databeskyttelsesrammen") er udviklet i samarbejde med Europa-Kommissionen ("Kommissionen"), industrien og andre interessenter med henblik på at nå målet om at fremme handelen mellem EU og USA[9] og samtidig sikre, at de registrerede sikres et beskyttelsesniveau, der i det væsentlige svarer til det, der garanteres i EU.

7. Principperne i databeskyttelsesrammen beskrives som en "nøglekomponent" i databeskyttelsesrammen. På den ene side udgør de en "brugsklar mekanisme" for dataoverførsler fra

---

https://www.hhs.gov/hipaa/for-professionals/privacy/index.html, https://www.justice.gov/opcl/privacy-act-1974.

[5] Det primære mål med COPPA er at lade forældre kontrollere, hvilke personlige oplysninger der indsamles fra deres børn under 13 år fra operatører af websteder og onlinetjenester rettet mod børn (herunder mobilapps og IoT-enheder såsom intelligent legetøj) eller generelle publikumswebsteder. I henhold til COPPA skal disse operatører underrette forældrene og indhente verificerbart forældresamtykke. Dette gælder også data fra udenlandske børn, hvis webstederne eller tjenesterne drives i USA og er underlagt COPPA. Samtidig finder bestemmelserne også anvendelse på udenlandsk baserede websteder og tjenester, hvis de er rettet mod børn i USA. Se: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions og udkast til afgørelse, bilag IV, s. 3.

[6] Et af målene med Gramm-Leach-Bliley Act er at beskytte forbrugernes privatliv i den finansielle sektor. I henhold til GLB Act skal finansielle institutioner over for deres kunder forklare deres praksis for udveksling af oplysninger og indføre garantier for at beskytte kundeoplysninger (f.eks. for virksomheder, der reguleres af FTC i henhold til FTC's sikkerhedsregel). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

[7] Attorney General Order No. 5517-2022, som ændrer det amerikanske justitsministeriums bestemmelser som bemyndiget og pålagt af EO 14086.

[8] Udkast til afgørelse, bilag I, afsnit I.

[9] *Ibid*.

EU til USA. På den anden side er personoplysninger, der overføres fra EU til USA, sikret og beskyttet som krævet i EU-retten.

8. Databeskyttelsesrammen finder kun anvendelse på amerikanske foretagender, der selv har certificeret sig i henhold til kravene i rammen ("foretagender i databeskyttelsesrammen"). I øjeblikket er dette kun muligt, hvis de henhører under Federal Trade Commission ("FTC") eller det amerikanske transportministerium ("transportministeriet"). I fremtiden kan andre vedtægtsmæssige organer — med kompetence til at føre tilsyn med gennemførelsen af principperne til databeskyttelsesrammen — blive tilføjet i et kommende bilag.

9. Det forklares ved principperne til databeskyttelsesrammen, at rammebetingelserne kan håndhæves af i) FTC i henhold til Section 5 i Federal Trade Commission Act ("FTC Act"), der forbyder urimelige eller vildledende handlinger i eller påvirker handelen[10], ii) transportministeriet i henhold til United States Code, afsnit 49, § 41712, som forbyder transportøren eller rejsebureauet at udøve en urimelig eller vildledende praksis inden for lufttransport med henblik på salg eller lufttransport, eller iii) i henhold til andre love eller administrative bestemmelser, hvorved sådanne handlinger er forbudt.

10. Det påpeges i principperne til databeskyttelsesrammen, at hverken GDPR eller de eksisterende forpligtelser til beskyttelse af privatlivets fred, som ellers finder anvendelse i henhold til amerikansk ret, er begrænset af principperne til databeskyttelsesrammen.

1.2 Rækkevidden af Databeskyttelsesrådets vurdering

11. Udkastet til afgørelse afspejler Kommissionens vurdering af databeskyttelsesrammen, som er resultatet af drøftelser med den amerikanske regering. I overensstemmelse med artikel 70, stk. 1, litra s), i GDPR forventes Databeskyttelsesrådet at afgive en udtalelse om Kommissionens konklusioner vedrørende tilstrækkeligheden af beskyttelsesniveauet i et tredjeland og om nødvendigt bestræbe sig på at fremsætte forslag til løsning af eventuelle problemer.

12. Databeskyttelsesrådet glæder sig over ajourføringerne af principperne til databeskyttelsesrammen[11], som vil udgøre den bindende retlige ramme for foretagender i databeskyttelsesrammen. Databeskyttelsesrådet bemærker imidlertid, at principperne til databeskyttelsesrammen i det væsentlige forbliver de samme som under privatlivsskjoldet[12] (som var baseret på Artikel 29-arbejdsgruppens ("Artikel 29-Gruppen") og Databeskyttelsesrådets årlige fælles evalueringer). Principperne til databeskyttelsesrammen er også i vid udstrækning de samme som dem i udkastet til privatlivsskjoldet, som Artikel 29-Gruppen baserede sin udtalelse fra 2016 på[13] ("Artikel 29-Gruppens udtalelse 01/2016"). For så vidt angår de DPF-principper, der i det væsentlige er uændrede, finder Databeskyttelsesrådet det ikke nødvendigt at gentage alle de bemærkninger, der tidligere er fremsat af Artikel 29-Gruppen. Databeskyttelsesrådet har besluttet at fokusere på specifikke aspekter, som det anser for at være endnu mere relevante i dag i lyset af udviklingen i det retlige og teknologiske miljø.

[10] United States Code, afsnit 15, § 45(a).
[11] F.eks. præciseringen af, at nøglekodede oplysninger er personoplysninger.
[12] Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred (EUT L 207 af 1.8.2016, s. 1).
[13] Artikel 29-Gruppen, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, vedtaget den 13. april 2016 ("Artikel 29-Gruppens udtalelse 01/2016").

13. I overensstemmelse med EU-Domstolens retspraksis[14] omfatter en meget vigtig del af analysen desuden den retlige ordning for statslig adgang til personoplysninger, der overføres til USA.

14. I sin vurdering tog Databeskyttelsesrådet hensyn til den gældende europæiske databeskyttelsesramme, herunder artikel 7, 8 og 47 i EU's charter om grundlæggende rettigheder ("chartret"), som henholdsvis beskytter retten til privatliv og familieliv, retten til beskyttelse af personoplysninger og retten til adgang til effektive retsmidler og til en upartisk domstol, og artikel 8 i den europæiske menneskerettighedskonvention ("EMRK"), der beskytter retten til privatliv og familieliv. Ud over ovenstående tog Databeskyttelsesrådet hensyn til kravene i GDPR, den relevante retspraksis og den reference vedrørende et tilstrækkeligt beskyttelsesniveau, som Databeskyttelsesrådet har vedtaget ("tilstrækkelighedsreferencen")[15].

15. Formålet med dette arbejde er at afgive en udtalelse til Europa-Kommissionen om vurderingen af tilstrækkeligheden af beskyttelsesniveauet i databeskyttelsesrammen. Begrebet "tilstrækkeligt beskyttelsesniveau", som allerede var at finde i direktiv 95/46, er blevet videreudviklet af Domstolen. Det er derfor vigtigt at minde om den standard, som EU-Domstolen fastsatte i sine domme, Schrems I[16] (ugyldiggørelse af "safe harbor"-principperne) og Schrems II[17] (ugyldiggørelse af privatlivsskjoldet).

16. I dommen i Schrems I-sagen fastsatte Domstolen, 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]*"[18]. 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 personoplysninger, 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[19].

17. I sin dom i Schrems II-sagens fastslog Domstolen, at de love, på grundlag af hvilke amerikanske efterretningsmyndigheder kan få adgang til personoplysninger, der overføres til USA (Section 702 i FISA/EO 12333), i uforholdsmæssig grad begrænser de rettigheder, der er fastsat i artikel 7 og 8 i EU's charter om grundlæggende rettigheder (chartret), og derfor ikke er afgrænset på en sådan måde, at de lever op til krav, som i det væsentlige svarer til dem, der er foreskrevet i EU, ved chartrets artikel 52, stk. 1, andet punktum[20].

---

[14] Navnlig med hensyn til: Domstolens dom af 6. oktober 2015, Maximilian Schrems mod Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650, og Domstolens dom af 16. juli 2020, Data Protection Commissioner mod Facebook Ireland Limited and Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] Artikel 29-Gruppen, **Error! Hyperlink reference not valid.**.

[16] Domstolens dom i Schrems I af 6. oktober 2015, Maximilian Schrems mod Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650 ("Domstolens dom i Schrems I-sagen").

[17] Domstolens dom af 16. juli 2020, Data Protection Commissioner mod Facebook Ireland Limited og Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 ("Domstolens dom i Schrems II-sagen").

[18] Domstolens dom i Schrems I-sagen, præmis 73-74.

[19] GDPR **Error! Hyperlink reference not valid.** s. 2.

[20] Domstolens dom i Schrems II-sagen, præmis 184-185.

18. Desuden anførte Domstolen, at den tidligere retlige ramme ikke gav garantier, der i det væsentlige svarer til dem, der kræves i henhold til chartrets artikel 47, da ombudsmandsmekanismen ikke kunne kompensere for det forhold, at hverken PPD-28 eller EO 12333 giver ikkeamerikanske personer effektive retsmidler[21]. Ombudsmanden manglede uafhængighed af den udøvende magt og beføjelse til at vedtage bindende afgørelser om amerikanske efterretningstjenester[22].

19. Med EO 14086, som generelt erstatter PPD-28, blev der indført to nye krav i amerikansk ret, som afspejler Domstolens dom i Schrems II-sagen: På den ene side, at signalefterretningsaktiviteter kun må udføres i det omfang, det er nødvendigt for at fremme en valideret prioriteret indsamling af efterretninger, og kun i det omfang og på en måde, der står i et rimeligt forhold til den validerede efterretningsprioritet, og på den anden side en klagemekanisme.

20. I denne udtalelse vurderer Databeskyttelsesrådet navnlig, i hvilket omfang databeskyttelsesrammen samt den nyligt vedtagne EO 14086 effektivt imødekommer EU-Domstolens konklusioner i dennes dom.

1.3 Generelle kommentarer og betænkeligheder

1.3.1 Vurdering af den nationale lovgivning

21. Databeskyttelsesrådet forstår, at vurderingen i udkastet til afgørelse vedrører DPF-principperne. Databeskyttelsesrådet vil ikke desto mindre hilse visse oplysninger om den amerikanske retlige kontekst, som foretagenderne i databeskyttelsesrammen opererer i, velkommen. Dette vil give mulighed for en bedre forståelse af samspillet mellem databeskyttelsesrammen og amerikansk ret. I bilag I, afsnit 1,[23] fastslås det f.eks., at DPF-principperne ikke "*begrænser andre forpligtelser til at sikre privatlivets fred i amerikansk ret*", uden at beskrive disse forpligtelser.

1.3.2 Internationale forpligtelser, som USA har påtaget sig

22. Ifølge artikel 45, stk. 2, litra c), i GDPR og tilstrækkelighedsreferencen skal Europa-Kommissionen, når den vurderer tilstrækkeligheden af beskyttelsesniveauet i et tredjeland, bl.a. tage hensyn til de internationale forpligtelser, som tredjelandet har påtaget sig, eller andre forpligtelser, der følger af tredjelandets deltagelse i multilaterale eller regionale systemer, navnlig vedrørende beskyttelse af personoplysninger, samt gennemførelsen af sådanne forpligtelser.

23. USA er part i flere internationale aftaler, der sikrer retten til privatlivets fred, såsom den internationale konvention om borgerlige og politiske rettigheder (artikel 17), konventionen om rettigheder for personer med handicap (artikel 22) og konventionen om barnets rettigheder (artikel 16). Desuden tilslutter USA sig som OECD-medlem OECD's ramme for beskyttelse af privatlivets fred, navnlig retningslinjerne for beskyttelse af privatlivets fred og grænseoverskridende udveksling af personoplysninger. Den 14. december 2022 blev OECD's erklæring om offentlig adgang til personoplysninger, som private enheder ligger inde med, vedtaget af ministre og højtstående repræsentanter for OECD-medlemmer og Den Europæiske Union. USA er også part i Budapestkonventionen om IT-kriminalitet.

24. Desuden er USA medlem af det grænseoverskridende system til beskyttelse af privatlivets fred ("CBPR") i landene i det økonomiske samarbejde i Asien-Stillehavsområdet ("APEC"), som er en

[21] Domstolens dom i Schrems II-sagen, præmis 192.
[22] Domstolens dom i Schrems II-sagen, præmis 195.
[23] Udkast til afgørelse, bilag I, afsnit I, sidste punktum.

statsstøttet certificering af databeskyttelse, som virksomheder kan tilslutte sig for at påvise overholdelse af internationalt anerkendte regler om beskyttelse af privatlivets fred. Disse regler om beskyttelse af privatlivets fred er blevet godkendt af APEC-lederne.

25. Databeskyttelsesrådet noterer sig også USA's deltagelse som observatørstat i arbejdet i Europarådets rådgivende udvalg under konvention 108.

26. Databeskyttelsesrådet noterer og glæder sig desuden over de amerikanske organers fortsatte engagement i det nyligt oprettede format "Roundtable of G7 Data Protection and Privacy Authorities" (G7's rundbordsmøde om databeskyttelse og privatlivets fred), som samler uafhængige tilsynsmyndigheder for databeskyttelse og privatlivets fred i G7-landene. I denne forbindelse har de f.eks. støttet den seneste G7-rundbordsmeddelelse fra databeskyttelsesmyndighederne[24], der blev vedtaget den 8. september 2022 i Bonn, Tyskland, og som fokuserede på begrebet "Data Free Flow with Trust".

1.3.3 Fremskridt med hensyn til USA's databeskyttelseslovgivning

27. Databeskyttelsesrådet noterer sig navnlig udviklingen i lovgivningen om databeskyttelse på statsniveau i USA. Databeskyttelsesrådet glæder sig over vedtagelsen af databeskyttelseslove, der er trådt i kraft eller vil træde i kraft senest i 2023 i fem stater (Californien, Colorado, Connecticut, Virginia og Utah)[25]..

28. Databeskyttelsesrådet bemærker også, at der allerede er iværksat tilsvarende initiativer til yderligere statslove i mange andre amerikanske stater.

29. Desuden glæder Databeskyttelsesrådet sig udtrykkeligt over bestræbelserne med hensyn til det tværpolitiske initiativ til en føderal databeskyttelseslov, American Data Privacy and Protection Act (ADPPA).

1.3.4 Rammerne for udkastet til afgørelse

30. I henhold til artikel 1 i udkastet til afgørelse konkluderer Kommissionen, at USA sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til foretagender i USA, og som er opført på "Data Privacy Framework List", som vedligeholdes og offentliggøres af det amerikanske handelsministerium ("handelsministeriet") i overensstemmelse med afsnit I, punkt 3, i bilag I[26].

[24] Rundbordsdiskussion mellem G7-databeskyttelsesmyndigheder og myndigheder for beskyttelse af privatlivets fred, "Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces", 8. september 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

[25] California Consumer Privacy Act (2018 med virkning fra 1. januar 2020), California Privacy Rights Act (2020, med fuld virkning fra 1. januar, 2023), Colorado Privacy Act (2021, med virkning fra 1. juli 2023), Connecticut Data Privacy Act (2022, med virkning fra 1. juli 2023), Virginia Consumer Data Protection Act (2021, med virkning fra 1. januar 2023), Utah Consumer Privacy Act (2022, med virkning fra 31. december 2023).

[26] Udkast til afgørelse, endelige overvejelser, artikel 1, s. 57. Databeskyttelsesrådet forstår, at udkastet til afgørelse ikke vil omfatte overførsler fra enheder, der er beliggende uden for EU, men som er omfattet af GDPR i medfør af artikel 3, stk. 2, i GDPR, til certificerede enheder i USA.

31. Databeskyttelsesrammen er tilgængelig for selskaber under FTC's eller transportministeriets jurisdiktion. Det påpeges, at andre amerikanske lovbestemte organer med tilsvarende beføjelser kan tilføjes i fremtiden[27].

1.3.5 Begrænsninger af pligten til at overholde DPF-principperne

32. I bilag I, afsnit I, punkt 5, fastsættes det, at foretagender i databeskyttelsesrammens overholdelse af DPF-principperne kan være begrænset, bl.a. i) til et niveau, der er tilstrækkeligt til at opfylde kravene med hensyn til den offentlige interesse eller retshåndhævelsen[28] eller den nationale sikkerhed[29] (herunder hvis love eller administrative bestemmelser medfører modstridende forpligtelser), og ii) ved lov, retsafgørelse eller administrative bestemmelser, der medfører udtrykkelige tilladelser, såfremt foretagender i databeskyttelsesrammen i forbindelse med anvendelsen af sådanne tilladelser kan påvise, at de kun overtræder DPF-principperne i det omfang, som er nødvendigt for at tilgodese de altovervejende legitime interesser, som den pågældende tilladelse har til hensigt at fremme.

33. Uden fuldt kendskab til amerikansk ret på både forbunds- og delstatsniveau er det vanskeligt for Databeskyttelsesrådet at foretage en detaljeret vurdering af anvendelsesområdet for de undtagelser, der er anført i dette afsnit. Databeskyttelsesrådet anbefaler derfor, at Kommissionen i udkastet til afgørelse medtager en præcisering af undtagelsernes anvendelsesområde, herunder de gældende garantier i henhold til amerikansk lovgivning, for bedre at kunne afdække virkningen af disse undtagelser på beskyttelsesniveauet for registrerede. Databeskyttelsesrådet understreger også, at Kommissionen bør underrettes om og overvåge anvendelsen og vedtagelsen af enhver lov eller administrativ bestemmelse, der vil påvirke overholdelsen af DPF-principperne.

1.3.6 Ændringer med hensyn til "privatlivsskjoldet"

34. Databeskyttelsesrådet glæder sig over den indsats, der er gjort for at opfylde kravene i dommen i Schrems II-sagen. Ikke desto mindre ville Databeskyttelsesrådet have hilst det velkommen, hvis flere spørgsmål, der blev påpeget i) i Artikel 29-Gruppens udtalelse 01/2016 og ii) i de tidligere fælles evalueringer[30], også ville være blevet behandlet i forbindelse med forhandlingerne om databeskyttelsesrammen.

35. Databeskyttelsesrådet bemærker også, at på trods af en række ændringer og yderligere forklaringer i betragtningerne til udkastet til afgørelse forbliver de DPF-principper, som foretagenderne i databeskyttelsesrammen skal overholde, i det væsentlige uændrede med hensyn til dem, der finder anvendelse under privatlivsskjoldet.

---

[27] Udkast til afgørelse, bilag I, afsnit I, punkt 2.

[28] Se afsnit 3.1 i denne udtalelse for yderligere bemærkninger om anvendelsen af personoplysninger, der er omfattet af databeskyttelsesrammen mellem EU og USA til retshåndhævelsesformål.

[29] Se afsnit 3.2 i denne udtalelse for yderligere bemærkninger om anvendelsen af personoplysninger, der er omfattet af databeskyttelsesrammen mellem EU og USA til nationale sikkerhedsformål.

[30] Årlige evalueringer: EU-U.S. Privacy Shield — First Annual Joint Review, WP 255, Artikel 29-Gruppens rapport vedtaget den 28. november 2017 ("første fælles evalueringsrapport"), EU-U.S. Privacy Shield — Second Annual Joint Review, Databeskyttelsesrådets rapport vedtaget den 22. januar 2019 ("anden fælles evalueringsrapport"), EU-U.S. Privacy Shield — Third Annual Joint Review, Databeskyttelsesrådets rapport vedtaget den 12. november 2019 ("tredje fælles evalueringsrapport").

1.3.7 Manglende klarhed i databeskyttelsesrammens dokumenter

36. Databeskyttelsesrådet bemærker, at bilagenes struktur og nummerering gør det temmelig vanskeligt at finde og henvise til oplysningerne. Dette bidrager til en overordnet kompleks præsentation af den nye ramme, som i bilagene indeholder dokumenter af forskellig juridisk værdi, og som måske ikke fremmer en god forståelse af DPF-principperne hos registrerede, foretagender i databeskyttelsesrammen og EU's databeskyttelsesmyndigheder.

37. Databeskyttelsesrådet understreger også, at terminologien bør anvendes konsekvent i hele databeskyttelsesrammen. Dette er i øjeblikket ikke tilfældet, f.eks. for så vidt angår begrebet "behandling". Nogle af databeskyttelsesrammens dele opregner visse typer databehandlingsaktiviteter i stedet for at anvende udtrykket "behandling". Dette kan føre til retsusikkerhed og mulige smuthuller i beskyttelsen[31].

38. Databeskyttelsesrådet glæder sig over, at definitionerne af nogle af de anvendte termer er medtaget i databeskyttelsesrammen[32]. Dette er imidlertid ikke tilfældet for visse andre væsentlige udtryk såsom i det mindste "mandatar" eller "databehandler", som efter Databeskyttelsesrådets opfattelse berettiger til en klar og specifik definition i bilag I, afsnit I, punkt 8, i databeskyttelsesrammen, og som både USA og EU er enige om, for at undgå forvirring på et senere tidspunkt for foretagender i databeskyttelsesrammen, der er afhængige af databeskyttelsesrammen, tilsynsmyndighederne og offentligheden.

39. Med hensyn til spørgsmålet om divergerende fortolkninger i EU og USA af begrebet data vedrørende menneskelige ressourcer (HR-data) er Databeskyttelsesrådet enig i Kommissionens tredje evalueringsrapport om målet om at fortsætte drøftelserne med de amerikanske myndigheder[33].

2 GENERELLE DATABESKYTTELSESASPEKTER

2.1 Indholdsprincipper

2.1.1 Begreber

40. På grundlag af tilstrækkelighedsreferencen bør der findes grundlæggende databeskyttelsesbegreber og/eller -principper i tredjelandets retlige ramme. Terminologien skal ikke nødvendigvis være den samme som i GDPR, men begreberne bør afspejle og være i overensstemmelse med begreberne i europæisk databeskyttelseslovgivning. GDPR omfatter eksempelvis følgende vigtige begreber: "personoplysninger", "behandling af personoplysninger", "dataansvarlig", "databehandler", "modtager" og "følsomme oplysninger". Databeskyttelsesrådet glæder sig over, at definitionerne af begreberne "personoplysninger", "behandling" og "dataansvarlig" er medtaget i databeskyttelsesrammen, som det var tilfældet i privatlivsskjoldet.

---

[31] For eksempel i) i henhold til ordlyden af udkastet til afgørelse, bilag I, afsnit III, punkt 6.f, vil DPF-principperne kun finde anvendelse, hvis foretagendet "lagrer, anvender eller videregiver" de modtagne oplysninger (dvs. ikke for andre operationer, der er omfattet af udtrykket "behandling", såsom indsamling, registrering, ændring, genfinding, søgning og sletning), og ii) i henhold til udkastet til afgørelse, bilag I, afsnit II, punkt 4.a, vil datasikkerheden kun blive pålagt for foretagender, der "opretter, vedligeholder, anvender eller spreder" personoplysninger.

[32] Udkast til afgørelse, bilag I, afsnit I, punkt 8.

[33] Tredje fælles evalueringsrapport, side 5, 15-16 og 30. Se også arbejdsdokument fra Kommissionens tjenestegrene, der ledsager rapporten fra Kommissionen til Europa-Parlamentet og Rådet om den tredje årlige evaluering af, hvordan EU-USA-privatlivsskjoldet fungerer, s. 17-18.

41. Databeskyttelsesrådet bemærker, at det fortsat er uklart, i hvilket omfang DPF-principperne finder anvendelse på foretagender i databeskyttelsesrammen, der modtager personoplysninger fra EU med henblik på "ren behandling" (benævnt "mandatarer" eller "databehandlere"). I databeskyttelsesrammen skelnes der ikke mellem DPF-principperne, der gælder for mandatarer, og principperne til databeskyttelsesrammen, der gælder for dataansvarlige, mens flere af forpligtelserne i principperne til databeskyttelsesrammen ikke er egnede for mandatarer/databehandlere. For eksempel bør en mandatar/databehandler ikke være i stand til at give fysiske personer alle dele af de fuldstændige oplysninger som krævet i princippet om oplysningspligt (f.eks. de formål, hvortil de indsamler og anvender personoplysninger om dem)[34], da en mandatar/databehandler ikke alene kan afgøre, hvilke midler og formål der skal anvendes til behandlingen[35].

2.1.2 Princippet om formålsbegrænsning

42. I henhold til tilstrækkelighedsreferencen bør personoplysninger i overensstemmelse med GDPR behandles til et specifikt formål og efterfølgende kun anvendes, for så vidt som dette ikke er uforeneligt med formålet med behandlingen.

43. Ifølge princippet om dataintegritet og formålsbegrænsning må et foretagende ikke behandle personoplysninger på en måde, der er uforenelig med de formål, hvortil de er blevet indsamlet eller efterfølgende godkendt af den fysiske person[36]. Databeskyttelsesrådet bemærker, at der anvendes en anden terminologi i henhold til principperne om oplysningspligt, valgfrihed og dataintegritet og formålsbegrænsning. Som bemærket af Artikel 29-Gruppen og til trods for en nyttig præcisering i betragtningerne til udkastet til afgørelse anvendes udtryk som "andre formål", "væsentligt forskellige" formål eller "en anvendelse, der ikke er forenelig med", i databeskyttelsesrammen uden en klar definition af disse begreber, og dette kan føre til retsusikkerhed.

2.1.3 Retten til indsigt, berigtigelse, sletning og indsigelse

44. I databeskyttelsesrammen er de registreredes ret til indsigt, berigtigelse og sletning omfattet af princippet om indsigt[37].

45. Princippet om indsigt forbliver uændret i forhold til privatlivsskjoldet. Derfor er nogle af de punkter, der giver anledning til bekymring i Artikel 29-Gruppens udtalelse 01/2016, stadig gyldige som beskrevet nedenfor.

46. Med hensyn til fysiske personers ret til indsigt finder Databeskyttelsesrådet det nødvendigt at gentage, at detaljerne i forpligtelsen til at behandle anmodninger fra fysiske personer bør indsættes i princippets hovedtekst (de er stadig kun beskrevet i en fodnote[38]).). Det bør også være klart, at der bør gives indsigt i det omfang, et foretagende i databeskyttelsesrammen behandler personoplysninger, og ikke kun når det "lagrer" dem[39]. Efter Databeskyttelsesrådets opfattelse kan den nuværende ordlyd føre til en snæver fortolkning af retten til indsigt.

---

[34] Udkast til afgørelse, bilag I, afsnit II, punkt 1.a.
[35] Se også Artikel 29-Gruppens udtalelse 01/2016, s. 16.
[36] Udkast til afgørelse, bilag I, afsnit II, punkt 5.
[37] Udkast til afgørelse, bilag I, afsnit II, punkt 6 og afsnit III, punkt 8.a.i.
[38] Udkast til afgørelse, bilag I, afsnit III, punkt 8.a.i.1. — fodnote 14.
[39] Udkast til afgørelse, bilag I, afsnit III, punkt 8.d.ii.

47. Med hensyn til listen over undtagelser fra retten til indsigt[40] har nogle stadig tendens til at hælde i retning af foretagender i databeskyttelsesrammens interesser. Databeskyttelsesrådet er fortsat bekymret over, at der i disse tilfælde ikke synes at være noget krav om at tage hensyn til fysiske personers rettigheder og interesser[41].

48. En anden undtagelse, der tidligere har været genstand for bekymring fra Artikel 29-Gruppens side[42], og som for Databeskyttelsesrådet synes at være alt for bred, er undtagelsen fra retten til indsigt i offentligt tilgængelige oplysninger og oplysninger i offentlige registre[43]. Databeskyttelsesrådet har gentagne gange erklæret, at registrerede i henhold til EU-retten altid har ret til indsigt i deres oplysninger, uanset om personoplysningerne er blevet offentliggjort eller ej. Hvis anmodninger om indsigt blev afvist med den begrundelse, at oplysningerne var indhentet fra offentligt tilgængelige kilder eller offentlige registre, ville de pågældende personer miste muligheden for at kontrollere oplysningernes rigtighed og kontrollere, om oplysningerne i det hele taget blev offentliggjort på lovlig vis.

49. Databeskyttelsesrådet minder om, at retten til indsigt er nedfældet i chartrets artikel 8, stk. 2. Selv om dette ikke er en absolut rettighed, er det grundlæggende for retten til beskyttelse af personoplysninger, da det letter udøvelsen af den registreredes øvrige rettigheder, såsom berigtigelse og sletning, og retten til at gøre indsigelse[44].

50. Ud over retten til indsigt og sletning bør registrerede til enhver tid have ret til af vægtige legitime grunde, der vedrører deres særlige situation, at gøre indsigelse mod behandlingen af deres oplysninger under bestemte forhold, der er fastsat i tredjelandets lovgivning[45].

51. Med princippet om valgfrihed giver databeskyttelsesrammen ret til at gøre indsigelse (opt-out) mod videregivelse af personoplysninger til tredjemand eller til anvendelse af personoplysninger til et formål, der er væsentligt forskelligt[46]. Desuden har fysiske personer til enhver tid ret til at vælge ikke at lade deres personoplysninger anvende til direkte markedsføring[47]. Bortset fra i forbindelse med direkte markedsføring er de nærmere bestemmelser, navnlig vedrørende tidspunktet for udøvelsen af retten til at gøre indsigelse, ikke præciseret. Databeskyttelsesrådet opfordrer derfor Kommissionen til at præcisere, hvordan fysiske personer kan udøve deres ret til at gøre indsigelse.

52. Som anført i Artikel 29-Gruppens udtalelse 01/2016 mener Databeskyttelsesrådet, at den blotte henvisning til eksistensen af denne ret i politikken til beskyttelse af privatlivets fred ikke er tilstrækkelig. En individualiseret mulighed for at udøve denne ret bør ikke kun tilbydes i tilfælde af videregivelse eller videreanvendelse af personoplysninger. Databeskyttelsesrådet understreger, at der bør tilbydes en generel ret til at gøre indsigelse af vægtige legitime grunde vedrørende den registreredes særlige situation inden for rammerne af databeskyttelsesrammen. Databeskyttelsesrådet anbefaler, at en sådan ret til at gøre indsigelse garanteres på et givet tidspunkt, og at denne ret ikke er begrænset til anvendelsen af data til direkte markedsføring[48].

---

[40] Udkast til afgørelse, bilag I, litra III.8, litra e).
[41] Artikel 29-Gruppens udtalelse 01/2016, punkt 2.2.5.
[42] Artikel 29-Gruppens udtalelse 01/2016, punkt 2.2.9.
[43] Udkast til afgørelse, bilag I, afsnit III, punkt 15.d-e.
[44] Artikel 29-Gruppens udtalelse 01/2016, punkt 2.2.5.
[45] Reference vedrørende et tilstrækkeligt beskyttelsesniveau, afsnit 3.A.8.
[46] Udkast til afgørelse, bilag I, afsnit II, punkt 2.a.
[47] Udkast til afgørelse, bilag I, afsnit III, punkt 12.a.
[48] Artikel 29-Gruppens udtalelse 01/2016, punkt 2.2.2.

53. Med hensyn til HR-data værdsætter Databeskyttelsesrådet Kommissionens præciseringer vedrørende anvendelsen af principperne om oplysningspligt og valgfrihed i en situation, hvor et certificeret amerikansk foretagende agter at anvende HR-data til et andet, ikkeansættelsesrelateret formål, f.eks. til markedsføringshenvendelser[49]. Databeskyttelsesrådet fastholder imidlertid, at yderligere behandling af HR-data til ikkeansættelsesrelaterede formål i de fleste tilfælde vil blive betragtet som uforenelig med det oprindelige formål, og at samtykke sjældent vil være helt frit, når det gives i et ansættelsesforhold.

54. Databeskyttelsesrådet gentager også Artikel 29-gruppens betænkeligheder med hensyn til undtagelsen fra principperne om oplysningspligt og valgfrihed af HR-data "*i det omfang og i den periode, det er nødvendigt for ikke at skade det pågældende foretagendes muligheder for at foretage forfremmelser eller udnævnelser eller behandle andre personaleanliggender af lignende karakter*"[50], som ifølge Databeskyttelsesrådet forekommer bredt og vagt[51].

2.1.4 Begrænsninger for videreoverførsel

55. Videreoverførsel 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 tilstrækkeligt beskyttelsesniveau, og følger de relevante instrukser ved behandling af oplysningerne på den dataansvarliges vegne. Beskyttelsesniveauet for fysiske personer, hvis personoplysninger overføres, må ikke undermineres af videreoverførslen. Det 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[52].

56. I henhold til databeskyttelsesrammens princip om ansvar for videreoverførsel kan videreoverførsel alene finde sted til begrænsede og bestemte formål på grundlag af en aftale mellem foretagendet i databeskyttelsesrammen og tredjeparten (eller et tilsvarende arrangement i en koncern), og udelukkende hvis denne aftale kræver, at tredjeparten sikrer samme niveau af beskyttelse som det, der er sikret ved DPF-principperne[53].

57. Databeskyttelsesrådet vil gerne gentage de betænkeligheder, der blev givet udtryk for i Artikel 29-Gruppens udtalelse 01/2016 vedrørende undtagelsen fra behovet for aftaler om koncerninterne overførsler mellem dataansvarlige[54]. For så vidt angår HR-data forstår Databeskyttelsesrådet stadig ikke begrundelsen for undtagelsen fra forpligtelsen til at indgå en aftale med en tredjepartsdataansvarlig i tilfælde af videreoverførsler til "lejlighedsvise ansættelsesrelaterede operationelle behov"[55].

---

[49] Udkast til afgørelse, bilag I, afsnit III, punkt 9.b.i, og betragtning 15 og fodnote 27.
[50] Udkast til afgørelse, bilag I, afsnit III, punkt 9.b.iv.
[51] Artikel 29-Gruppens udtalelse 01/2016, punkt 2.2.7.
[52] Reference vedrørende et tilstrækkeligt beskyttelsesniveau, afsnit 3.A.9.
[53] Udkast til afgørelse, bilag I, afsnit II, punkt 3.
[54] Udkast til afgørelse, bilag I, afsnit III, punkt 10.b.i, som henviser til "eller andre koncerninterne instrumenter (f.eks. overholdelses- og kontrolprogrammer)", som tilsyneladende ikke behøver at være bindende.
[55] Udkast til afgørelse, bilag I, afsnit III, punkt 9.e.i, med henvisning til eksempler som f.eks. forsikringsdækning.

58. Databeskyttelsesrådet vil desuden gerne gentage Artikel 29-Gruppens anmodning[56] om, at foretagender, der er bundet af rammen, forud for en videreoverførsel vurderer, at de obligatoriske krav i tredjelandets nationale lovgivning, der finder anvendelse på modtageren, ikke vil undergrave kontinuiteten i beskyttelsen af de registrerede, hvis oplysninger overføres[57].

59. Databeskyttelsesrådet fastholder, at videreoverførsel af personoplysninger til tredjelande kan føre til indgreb i fysiske personer grundlæggende rettigheder, og opfordrer Kommissionen til at præcisere, at de garantier, som den oprindelige modtager pålægger importøren i tredjelandet, skal være effektive i lyset af tredjelandets lovgivning forud for en videreoverførsel inden for rammerne af databeskyttelsesrammen[58].

2.1.5 Automatiske afgørelser og profilering

60. Afgørelser, der alene bygger på automatisk behandling (automatiske individuelle afgørelser), herunder profilering, og som har retsvirkning eller betydeligt påvirker den registrerede, må kun anvendes på visse betingelser, der er fastsat i tredjelandets lovramme. I henhold til europæisk lovgivning omfatter disse betingelser f.eks. krav om indhentning af den registreredes udtrykkelige samtykke eller afgørelsens nødvendighed med henblik på indgåelse af en aftale. Hvis ikke afgørelsen opfylder betingelserne i tredjelandets lovgivning, skal den registrerede have ret til ikke at være omfattet af den. Tredjelandets lovgivning bør under alle omstændigheder indeholde de nødvendige garantier, herunder retten til at blive underrettet om de specifikke grunde til afgørelsen og den logik, der ligger bag, til at rette urigtige eller ufuldstændige oplysninger og til at gøre indsigelse mod en afgørelse, som er truffet på et fejlagtigt grundlag[59].

61. Databeskyttelsesrammen indeholder ingen specifikke retlige garantier, når fysiske personer er genstand for afgørelser, der har retsvirkning eller i væsentlig grad berører dem, og som udelukkende er baseret på automatisk behandling af oplysninger, der har til formål at vurdere visse personlige forhold vedrørende dem, såsom deres erhvervsevne, kreditværdighed, pålidelighed eller adfærd.

62. Som allerede behandlet i Artikel 29-Gruppens udtalelse 01/2016 og af Databeskyttelsesrådet i dets tidligere udtalelser om afgørelser om tilstrækkeligheden af beskyttelsesniveauet vedrørende Japan og Sydkorea[60] finder Databeskyttelsesrådet, at den hurtige udvikling inden for automatiske afgørelser og

---

[56] Artikel 29-Gruppens udtalelse 01/2016, punkt 2.2.3, s. 21.

[57] I lyset af dommen i Schrems II-sagen har Databeskyttelsesrådet yderligere præciseret dataeksportørers og -importørers forpligtelser i forbindelse med videreoverførsel i en række retningslinjer og anbefalinger: Se Databeskyttelsesrådets henstilling 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger (version 2.0, vedtaget den 18. juni 2021), Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger (vedtaget den 10. november 2020), Retningslinjer 04/2021 om adfærdskodekser som redskab til overførsel (version 2.0 Vedtaget den 22. februar 2022), Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (vedtaget den 14. november 2022), Guidelines 07/2022 on certification as a tool for transfers (vedtaget efter offentlig høring den 14. februar 2023).

[58] Artikel 29-Gruppens udtalelse 01/2016, punkt 2.2.3, s. 21.

[59] Reference vedrørende et tilstrækkeligt beskyttelsesniveau, afsnit 3.B.3.

[60] Databeskyttelsesrådets udtalelse 28/2018 vedrørende Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i Japan, vedtaget den 5. december 2018, Databeskyttelsesrådets udtalelse 32/2021 om Europa-Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i republikken Korea, vedtaget den 24. september 2021.

profilering — i stigende grad ved hjælp af AI-teknologier — kræver særlig opmærksomhed i denne henseende[61].

63. Databeskyttelsesrådet noterer sig Kommissionens argumenter om, at fraværet af specifikke regler om automatiske afgørelser i databeskyttelsesrammen sandsynligvis ikke vil påvirke beskyttelsesniveauet for så vidt angår personoplysninger, der er indsamlet i Unionen (eftersom enhver afgørelse baseret på automatisk behandling typisk vil blive truffet af den dataansvarlige i Unionen, som har et direkte forhold til den pågældende registrerede)[62].. Databeskyttelsesrådet er imidlertid af den opfattelse, at det ikke kan udelukkes, at automatiske afgørelser kan anvendes af en amerikansk baseret dataansvarlig på oplysninger, der overføres i henhold til udkastet til afgørelse (f.eks. i forbindelse med beskæftigelse, til vurdering af resultater på arbejdspladsen, forsikring, bolig).

64. Databeskyttelsesrådet glæder sig over Kommissionens henvisninger til specifikke garantier i den relevante amerikanske lovgivning på forskellige områder[63]. Databeskyttelsesrådet mener imidlertid, at beskyttelsesniveauet for fysiske personer synes at variere alt efter, hvilke sektorspecifikke regler — om nogen — der finder anvendelse på den foreliggende situation. Der er risiko for, at visse situationer ikke vil være omfattet, fordi de ikke er omfattet af de nævnte retsakters anvendelsesområde. Desuden er indholdet af individuelle rettigheder i forbindelse med automatiske afgørelser beskrevet forskelligt i de forskellige retsakter.

65. På denne baggrund mener Databeskyttelsesrådet, at der er behov for specifikke regler om automatiske afgørelser i databeskyttelsesrammen for at sikre tilstrækkelige garantier, herunder retten for den enkelte til at kende den involverede logik, til at anfægte afgørelsen og til at opnå menneskelig indgriben, når afgørelsen i væsentlig grad påvirker vedkommende[64].

2.2 Procedure- og håndhævelsesmekanismer

66. Databeskyttelsesrådet bemærker, at databeskyttelsesrammen fortsat er afhængig af et selvcertificeringssystem, selv om Kommissionen henviser til det som et "certificeringssystem".

67. Databeskyttelsesrådet minder om de forbedringer, der er opnået i løbet af de tidligere fælles evalueringer. F.eks. med hensyn til handelsministeriets rolle, for så vidt angår (gen)selvcertificeringsprocessen (...), overvågning af virksomhedernes overholdelse af DPF-principperne (f.eks. gennem stikprøvekontroller, anvendelse af spørgeskemaer om overholdelse) og identifikation og håndtering af falske påstande om deltagelse (f.eks. gennem internetsøgninger).

68. Samtidig havde Artikel 29-Gruppen og Databeskyttelsesrådet udtrykt bekymring over en vis mangel på tilsyn med overholdelsen af kravene i privatlivsskjoldet[65]. Databeskyttelsesrådet er navnlig enigt i Kommissionens konklusioner efter den tredje årlige gennemgang af privatlivsskjoldet om, at handelsministeriets stikprøvekontrol under privatlivsskjoldet var begrænset til formelle krav (f.eks. manglende reaktion fra udpegede kontaktpunkter eller manglende adgang til en virksomheds

[61] Se bl.a. C-634/21, OQ mod Land Hesse (SCHUFA Holding m.fl.), anmodning om præjudiciel afgørelse (verserende).
[62] Udkast til afgørelse, betragtning 33 og 34.
[63] Udkast til afgørelse, betragtning 35.
[64] Se også tredje fælles evalueringsrapport, punkt 76.
[65] Tredje fælles evalueringsrapport, punkt 7.

databeskyttelsespolitik online)[66]. The EDPB considers that . Databeskyttelsesrådet mener, at overensstemmelseskontrol for så vidt angår mere materielle krav er afgørende.

69. Databeskyttelsesrådet minder også om betydningen af effektivt tilsyn (herunder overholdelse af væsentlige krav) og håndhævelse af databeskyttelsesrammen. Dette aspekt vil blive nøje overvåget af Databeskyttelsesrådet, herunder i forbindelse med de periodiske evalueringer.

70. For så vidt angår håndhævelse noterer Databeskyttelsesrådet sig de fornyede tilsagn i skrivelserne fra FTC[67] og transportministeriet[68] om at prioritere undersøgelsen af påståede overtrædelser af databeskyttelsesrammen, træffe passende håndhævelsesforanstaltninger over for enheder, der fremsætter falske eller vildledende påstande om deltagelse, overvåge håndhævelsesafgørelser vedrørende overtrædelser af databeskyttelsesrammen og samarbejde med EU's databeskyttelsesmyndigheder. I denne forbindelse anerkender Databeskyttelsesrådet også, at FTC har tilkendegivet, at den forventer at fokusere sin håndhævelsesindsats yderligere på væsentlige overtrædelser af databeskyttelsesrammen, og at den agter at undersøge (også) på eget initiativ. Disse aspekter vil blive nøje overvåget af Databeskyttelsesrådet, herunder i forbindelse med de periodiske evalueringer.

2.3 Klagemekanismer

71. Databeskyttelsesrådet glæder sig over den klare præsentation i udkastet til afgørelse af de syv klagemuligheder, der gives til registrerede i EU, hvis deres personoplysninger behandles i strid med databeskyttelsesrammen[69].

72. Disse forskellige klagemekanismer er etableret i overensstemmelse med kravene i princippet om klageadgang, håndhævelse og ansvar og det supplerende princip 11 om "bilæggelse af tvister og håndhævelse", der er udstedt af handelsministeriet og nævnt i bilag I til udkastet til afgørelse[70].

73. Som Kommissionen understregede i sit udkast til afgørelse, bør "*den registrerede have adgang til effektive administrative og retslige klagemuligheder*"[71]. Dette afspejler kravet i databeskyttelsesforordningens artikel 45, stk. 2, litra a), hvorefter Kommissionen i sin vurdering af beskyttelsesniveauets tilstrækkelighed i et tredjeland navnlig skal tage hensyn til "effektiv administrativ og retslig prøvelse for de registrerede, hvis personoplysninger overføres"[72]. Der mindes også om dette krav i den generelle forordning om databeskyttelse[73].

74. Databeskyttelsesrådet bemærker, at disse klagemekanismer er de samme som dem, der indgik i det tidligere privatlivsskjold, som havde været genstand for bemærkninger fra Artikel 29-Gruppen[74].

---

[66] Rapport fra Kommissionen til Europa-Parlamentet og Rådet om den tredje årlige evaluering af EU-USA-privatlivsskjoldet (COM(2019) 495 final af 23.10.2019), s. 4.
[67] Udkast til afgørelse, bilag IV.
[68] Udkast til afgørelse, bilag V
[69] Udkast til afgørelse, betragtning 67.
[70] Udkast til afgørelse, bilag I, afsnit II, punkt 7, og afsnit III, punkt 11, og bilag I til bilag I.
[71] Udkast til afgørelse, betragtning 64.
[72] Se også betragtning 141 i GDPR, der henviser til artikel 47 i chartret om grundlæggende rettigheder om adgangen til effektive retsmidler i EU.
[73] Reference vedrørende et tilstrækkeligt beskyttelsesniveau, s. 8.
[74] Se navnlig Artikel 29-Gruppens udtalelse 01/2016, afsnit 2.2.6, litra a).

75. Med hensyn til voldgiftsmekanismen bemærker Databeskyttelsesrådet, at denne mulighed ikke er tilgængelig for så vidt angår undtagelserne fra DPF-principperne[75], og henviser derfor til sin bemærkning i punkt 33.

76. Med hensyn til yderligere muligheder for domstolsprøvelse i henhold til amerikansk lovgivning ønsker Databeskyttelsesrådet også yderligere oplysninger om den nævnte lovgivning[76] og henviser til sin bemærkning i punkt 21.

77. Databeskyttelsesrådet glæder sig desuden over den skrivelse fra FTC, der beskriver dens hensigt om at arbejde tæt sammen med EU's databeskyttelsesmyndigheder[77]. Databeskyttelsesrådet glæder sig også over, at FTC prioriterer klager, selv om det måske ikke giver den registrerede sikkerhed for, at vedkommendes klager vil blive behandlet i alle tilfælde.

78. For så vidt angår muligheden for, at fysiske personer i visse tilfælde kan indgive deres klager til en EU-databeskyttelsesmyndighed, ser Databeskyttelsesrådet gerne yderligere oplysninger om i) hvorvidt EU's databeskyttelsesmyndigheds mulighed for at rådgive om afhjælpende eller kompenserende foranstaltninger kan omfatte anbefalinger om bøder eller anvendelse af undersøgelsesbeføjelser, og ii) i hvilket omfang EU's databeskyttelsesmyndigheds foranstaltninger vil blive taget i betragtning som bevis for håndhævelsesforanstaltninger fra FTC's eller transportministeriets side[78].

79. Effektiviteten af klagemekanismen vil blive nøje overvåget af Databeskyttelsesrådet, herunder i forbindelse med de periodiske evalueringer.

3 AMERIKANSKE OFFENTLIGE MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER OVERFØRT FRA DEN EUROPÆISKE UNION

3.1 Adgang og brug med henblik på retshåndhævelse på det strafferetlige område

3.1.1 De retshåndhævende myndigheders adgang til personoplysninger bør være baseret på klare, præcise og tilgængelige regler

80. Databeskyttelsesrådet glæder sig over de mere detaljerede oplysninger og forklaringer i forhold til den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet, der er fastsat i udkastet til afgørelse med hensyn til de amerikanske offentlige myndigheders adgang til og brug af personoplysninger med henblik på retshåndhævelse på det strafferetlige område. Udkastet til afgørelse, bilag VI, indeholder også en skrivelse fra det amerikanske justitsministerium, afdelingen for straffesager, med en kort oversigt over de primære efterforskningsværktøjer, der anvendes til at indhente kommercielle data og andre registreringsoplysninger fra selskaber i USA med henblik på retshåndhævelse på det strafferetlige eller offentlige (civile og lovgivningsmæssige) område, herunder de adgangsbegrænsninger, der er fastsat af disse myndigheder. Ifølge skrivelsen anvendes alle de retlige processer, der er beskrevet i skrivelsen, til at indhente oplysninger fra selskaber i USA, uden hensyn til den registreredes nationalitet eller bopæl, og de følger enten direkte af den amerikanske forfatning

[75] Udkast til afgørelse, bilag I til bilag I, A.
[76] Udkast til afgørelse, betragtning 85.
[77] Udkast til afgørelse, bilag IV.
[78] Udkast til afgørelse, bilag I, afsnit III, punkt 5.b.iii.

(fjerde amendment), af love og procesret eller af justitsministeriets retningslinjer og politikker. Denne oversigt omfatter ikke de nationale sikkerhedsefterforskningsværktøjer, der anvendes af de retshåndhævende myndigheder i forbindelse med terrorisme og andre efterforskninger vedrørende den nationale sikkerhed[79].

81. Databeskyttelsesrådet bemærker, at udkastet til afgørelse og bilag VI hertil primært omhandler føderale retshåndhævende og regulerende myndigheder[80] og ikke specifikt henviser til lovene i henhold til delstatslovgivningen, som indeholder bestemmelser om, at disse procedurer skal indhente oplysninger. I bilag VI nævnes det også, at "virksomheder kan anfægte anmodninger om oplysninger fra forvaltningsmyndigheder med hjemmel i andre retsgrundlag, afhængigt af sektoren og karakteren af de opbevarede oplysninger", og der gives derudover flere ikkeudtømmende eksempler, såsom Bank Secrecy Act og gennemførelsesbestemmelserne hertil[81], Fair Credit Reporting Act[82] og Right to Financial Privacy Act[83]. Databeskyttelsesrådet bemærker, at det gældende retsgrundlag for en given anmodning om aktindsigt afhænger af arten af de data, der anmodes om, virksomhedens art, arten af de retlige procedurer (strafferetlige, administrative, relateret til andre samfundsinteresser) og arten af den enhed, der anmoder om adgang. Eftersom alle gældende regler om begrænsning af de retshåndhævende myndigheders adgang til oplysninger, der overføres til USA, er baseret på forfatningen, lovgivningen og justitsministeriets gennemsigtige politikker, anerkender Databeskyttelsesrådet tilgængeligheden af disse regler, og det opfordrer Kommissionen til at afspejle dette element i udkastet til afgørelse. Det fremgår af bilag VI, at disse love finder anvendelse uanset den registreredes nationalitet eller bopæl og generelt omfatter kravene vedrørende fjerde amendment (selv om de ofte også går videre og omfatter yderligere beskyttelse).

82. Afslutningsvis noterer Databeskyttelsesrådet sig den mere detaljerede vurdering i udkastet til afgørelse sammenlignet med den tidligere afgørelse om tilstrækkeligheden af beskyttelsesniveauet for så vidt angår adgang for føderale retshåndhævende myndigheder. Med hensyn til de statslige retshåndhævende myndigheders adgang noterer Databeskyttelsesrådet sig også, at den statslige beskyttelse i henhold til bilag VI mindst skal svare til beskyttelsen i den amerikanske forfatning, herunder, men ikke begrænset til, fjerde amendment. Databeskyttelsesrådet opfordrer Kommissionen til at foretage en yderligere vurdering af elementet af statsretlig beskyttelse i forbindelse med fremtidige evalueringer.

3.1.2 De forfulgte legitime formåls nødvendighed og proportionalitet skal kunne påvises

83. Databeskyttelsesrådet noterer sig, at anmodning om adgang til data med henblik på retshåndhævelse generelt kan anses for at forfølge et legitimt mål. Samtidig er sådanne indgreb dog kun acceptable, når de er nødvendige og forholdsmæssige[84].

[79] Udkast til afgørelse, fodnote 1 til bilag VI.
[80] Se udkastet til afgørelse, betragtning 90-93.
[81] United States Code, afsnit 31, § 5318, 31 C.F.R. Kapitel X
[82] United States Code, afsnit 15, § 1681b
[83] United States Code, afsnit 12, §§ 3401-3423.
[84] Se Domstolens dom af 6. oktober 2020 i forenede sager C-511/18, C-512/18 og C-520/18, La Quadrature du Net m.fl., ECLI:EU:C:2020:791 ("Domstolens dom i La Quadrature du Net-sagen"), præmis 140. Se også Den Europæiske Tilsynsførende for Databeskyttelse (EDPS), Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit, 11. april 2017 og EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19. december 2019.

84. Ifølge Domstolens faste retspraksis kræver proportionalitetsprincippet, at de lovgivningsmæssige foranstaltninger, der indfører indgreb i retten til privatlivets fred og til beskyttelse af personoplysninger, "skal være egnede til at gennemføre de lovlige mål, som forfølges med den omhandlede lovgivning, og ikke går videre, end hvad der er nødvendigt og passende for gennemførelsen af disse mål"[85]. Derfor foretages vurderingen af nødvendighed og proportionalitet i princippet altid i forbindelse med en specifik foranstaltning, der er fastsat i lovgivningen.

85. De amerikanske myndigheder præciserer i bilag VI, at forbundsanklagere og føderale efterforskningsagenter kan få adgang til dokumenter og andre optegnelser fra foretagender gennem "flere forskellige former for pålæg, herunder stævninger udstedt af anklagejuryen (grand jury subpoenas), administrative pålæg (administrative subpoenas) og ransagningskendelser", og kan indhente anden kommunikation "i medfør af føderale tilladelser til aflytning i straffesager og til installation af pen-register"[86]. Desuden kan myndigheder med civilretlige og regulerende opgaver udstede pålæg (subpoenas) til foretagender om udlevering af "forretningsoplysninger, elektronisk lagrede oplysninger eller andre konkrete ting ("tangible things")"[87]. Selve processerne er også forklaret i betragtning 90-93 i udkastet til afgørelse. Databeskyttelsesrådet bemærker i denne forbindelse en positiv udvikling, som der henvises til i udkastet til afgørelse i den amerikanske retspraksis vedrørende de elektronisk lagrede oplysninger[88].

86. I bilag VI præciseres det endvidere, at disse retssager ikke er diskriminerende og generelt anvendes til at indhente oplysninger fra "selskaber" i USA, uanset om de er certificeret inden for rammerne af databeskyttelsesrammen mellem EU og USA eller ej, og "uanset den registreredes nationalitet eller bopæl".

87. Desuden indeholder bilag VI konklusioner vedrørende garantierne i henhold til fjerde amendment i den amerikanske forfatning, ifølge hvilke de retshåndhævende myndigheder først og fremmest skal have en dommerkendelse, der afgives på grundlag af dokumentation for begrundet mistanke ("probable cause"), inden ransagning og beslaglæggelse og særlige krav, og der henvises til, at retshåndhævelsen i de specifikke særlige tilfælde, hvor der ikke skal foreligge en kendelse, er betinget af en rimelighedstest i henhold til fjerde amendment[89]. En person, der er genstand for en ransagning, eller hvis formuegoder er genstand for en ransagning, kan anmode om at få afvist alle beviser indhentet ved eller afledt af en ulovlig ransagning, hvis dette bevismateriale føres mod den pågældende under en straffesag[90].

88. Afslutningsvis bemærker Databeskyttelsesrådet, at systemet med efterforskningsmetoder, der anvendes til at indhente kommercielle data og andre registreringsoplysninger fra virksomheder i USA med henblik på strafferetlig håndhævelse eller den offentlige interesse — herunder

[85] Se Domstolens dom af 8. april 2014 i forenede sager C-293/12 og C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238 ("Domstolens dom i Digital Rights Ireland-sagen"), præmis 46 og den deri nævnte retspraksis.
[86] Udkast til afgørelse, bilag VI, s. 2.
[87] Udkast til afgørelse, bilag VI, s. 4.
[88] Se udkast til afgørelse, fodnote 146. I en dom fra 2018 bekræftede USA's højesteret bekræftede, at der også kræves en ransagningskendelse eller en undtagelse, for at de retshåndhævende myndigheder kan få adgang til historiske mobildata, som giver et samlet overblik over en brugers bevægelser, og at brugeren kan have en rimelig forventning om privatlivets fred med hensyn til sådanne oplysninger (Timothy Ivory Carpenter mod USA, No. 16-402, 585 U.S. (2018)).
[89] Se udkast til afgørelse, bilag, bilag VI, s. 2.
[90] Se udkast til afgørelse, betragtning 90.

adgangsbegrænsninger og garantier — udgør et omfattende, men også et komplekst system af foranstaltninger, der bl.a. afspejler USA's regerings føderale karakter.

89. Systemet med retshåndhævelsesforanstaltninger i USA kan derfor anses for generelt at opfylde kravene om nødvendighed og proportionalitet i forhold til de grundlæggende rettigheder til privatliv og databeskyttelse.

3.1.3 Der bør findes en uafhængig tilsynsmekanisme

90. Databeskyttelsesrådet noterer sig, at de fleste af de procedurer, der er beskrevet i udkastet til afgørelse og bilag VI, forudsætter inddragelse af en domstols afgørelse, før myndighederne får adgang til data (f.eks. retsafgørelser om installation af pen-register- og trap and trace-anordninger[91], retsafgørelser om overvågning i henhold til føderal lovgivning om aflytning[92], ransagningskendelser — Federal Rules of Criminal Procedure, regel nr. 41[93]). Det ser imidlertid ikke ud til, at de alle kræver en forudgående inddragelse af en domstol. For eksempel kan civile og regulerende myndigheder "udstede pålæg" (subpoenas)[94]. I disse tilfælde er der imidlertid mulighed for en efterfølgende domstolskontrol af, om pålægget er rimeligt, da "en modtager af et administrativt pålæg kan anfægte håndhævelsen af dette pålæg ved domstolene"[95].

91. Desuden beskrives i udkastet til afgørelse forskellige organers tilsyn med de føderale retshåndhævende myndigheder på det strafferetlige område, lige fra den interne kontrol foretaget af Privacy and Civil Liberties Officers (databeskyttelsesansvarlige) til den eksterne kontrol, der udføres af Inspector General (generalinspektøren) og specifikke udvalg i den amerikanske kongres[96]. Europa-Kommissionen giver nuancerede og detaljerede oplysninger og når generelt frem til forståelige konklusioner. Databeskyttelsesrådet undlader derfor at gengive de faktuelle konklusioner og vurderinger i denne udtalelse.

92. På grundlag af de tilgængelige oplysninger bemærker Databeskyttelsesrådet, at der med hensyn til de retshåndhævende myndigheders adgang til data, som virksomheder i USA er i besiddelse af, er etableret en forholdsvis robust uafhængig tilsynsmekanisme.

3.1.4 Fysiske personer skal have adgang til effektive retsmidler.

93. I henhold til EU-Domstolens retspraksis skal en person have adgang til effektive retsmidler for at opfylde sine rettigheder, når vedkommende mener, at de ikke respekteres eller ikke er blevet respekteret. Domstolen forklarede i Schrems I, at "en lovgivning, der ikke fastsætter nogen mulighed for retssubjektet til at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet [opfylder] ikke det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som denne er sikret ved chartrets artikel 47. Chartrets artikel 47, stk. 1, opstiller således et krav om, at enhver, hvis rettigheder og friheder som sikret af EU-retten er blevet krænket, skal have adgang til effektive retsmidler for en domstol under overholdelse af de betingelser, der er fastsat i denne artikel."[97]

---

[91] Se udkast til afgørelse, betragtning 92.
[92] Se udkast til afgørelse, bilag VI, s. 3.
[93] Se udkast til afgørelse, betragtning 90 og bilag VI, s. 3.
[94] Se udkast til afgørelse, bilag VI, s. 4 samt betragtning 91.
[95] Se udkast til afgørelse, bilag VI, s. 4 samt betragtning 91.
[96] Se udkastet til afgørelse, betragtning 103-106.
[97] Domstolens dom i Schrems I-sagen, præmis 95.

94. Udkastet til afgørelse[98] og bilag VI hertil indeholder yderligere oplysninger om mulige retsmidler i henhold til lov, som vil være til rådighed for fysiske personer, når offentlige myndigheder ulovligt får adgang til deres data.

95. I denne henseende fremgår det ifølge Kommissionen[99], af Administrative Procedure Act (United States Code, afsnit 5, § 702), at enhver person, mod hvem der er begået juridisk uret på grund af et agenturs foranstaltninger, eller som er blevet krænket eller forurettet herved i henhold til en relevant lov, kan begære retslig prøvelse.

96. Desuden fastsættes det i Stored Communications Act (SCA) (vedtaget som afsnit II i Electronic Communications Privacy Act), at enhver person, der krænkes af en overtrædelse af dette kapitel, hvor den adfærd, der udgør overtrædelsen, er begået i en bevidst eller forsætlig tilstand, i forbindelse med et civilt søgsmål kan kræve erstatning fra den person eller enhed, bortset fra USA, som har medvirket til denne overtrædelse, i det omfang det er hensigtsmæssigt[100]. Desuden kan enhver, der lider skade som følge af en forsætlig overtrædelse af det pågældende kapitel eller kapitel 119, anlægge sag ved United States District Court mod USA med henblik på at opnå erstatning[101].

97. Desuden indeholder udkastet til afgørelse også oplysninger om retten til at få indsigt i de amerikanske forbundsorganers optegnelser i henhold til Freedom of Information Act (FOIA)[102] og flere andre love, der giver fysiske personer ret til at anlægge sag mod en amerikansk offentlig myndighed eller embedsmand med hensyn til behandlingen af deres personoplysninger, såsom Wiretap Act, Computer Fraud and Abuse Act, Federal Torts Claim Act, Right to Financial Privacy Act og Fair Credit Reporting Act[103].

98. Databeskyttelsesrådet glæder sig derfor over de præciseringer, som Kommissionen har givet med hensyn til antallet af retsmidler, som enkeltpersoner kan påberåbe sig. Databeskyttelsesrådet opfordrer også Kommissionen til yderligere at præcisere, om disse retsmidler giver den registrerede mulighed for at "få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet" som krævet af EU-Domstolen.

3.1.5 Yderligere anvendelse af de indsamlede oplysninger

3.1.5.1 Yderligere anvendelse af overførte data, som de retshåndhævende myndigheder har adgang til i USA

99. Databeskyttelsesrådet noterer sig med tilfredshed, at udkastet til afgørelse vurderer den videre anvendelse af data, som de retshåndhævende myndigheder har adgang til i USA. Databeskyttelsesrådet beklager dog, at der kun gives ét eksempel på grundene til, at oplysningerne kan videreformidles[104]. I den forbindelse anbefaler Databeskyttelsesrådet, at Kommissionen medtager yderligere præciseringer i udkastet til afgørelse om de gældende principper og garantier for den videre anvendelse af data, såsom dem, der er indeholdt i Privacy Act (United States Code, afsnit 5, § 552a)[105].

[98] Se udkast til afgørelse, betragtning 107-112.
[99] Se udkast til afgørelse, betragtning 109.
[100] United States Code, afsnit 18, § 2707,
[101] United States Code, afsnit 18, § 2712.
[102] Se udkast til afgørelse, betragtning 111.
[103] Se udkast til afgørelse, betragtning 112.
[104] Se udkast til afgørelse, betragtning 102.
[105] Se Attorney General Guidelines for Domestic FBI Operations (AGG-DOM), s. 36, punkt B(1)(g).

3.1.5.2 Videreoverførsler uden for USA

100. Databeskyttelsesrådet bemærker endvidere, at Europa-Kommissionen også har henvist til videreoverførsler fra de retshåndhævende myndigheder i USA til myndigheder i tredjelande, men igen kun med hensyn til Attorney General Guidelines for Domestic FBI Operations AGG-DOM[106]. Databeskyttelsesrådet mener, at sådanne oplysninger og vurderinger er af afgørende betydning for at muliggøre en omfattende vurdering af beskyttelsesniveauet i den amerikanske lovgivningsramme og praksis i forbindelse med international videregivelse og videreanvendelse. Eftersom Kommissionen kun har givet ét begrænset eksempel vedrørende spørgsmålet om videreoverførsler uden for USA som helhed, opfordrer Databeskyttelsesrådet Kommissionen til yderligere at præcisere de gældende regler og garantier for videreoverførsel, yderligere anvendelse og videregivelse af personoplysninger, der er indsamlet med henblik på retshåndhævelse i USA og efterfølgende overført til tredjelande, herunder via internationale aftaler.

3.2 Adgang til og brug af personoplysninger til nationale sikkerhedsformål

101. 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[107], fastsætter, at de 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[108]. 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[109]. 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*."

102. 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.

103. Flere retlige instrumenter giver mulighed for at indsamle og yderligere få adgang til og behandle data for amerikanske efterretningstjenester inden for USA's retlige rammer.

104. Som Europa-Kommissionen minder om i sit udkast til afgørelse, "*kan amerikanske efterretningstjenester kun søge adgang til personoplysninger, der er blevet overført til organisationer, der er beliggende i USA, til nationale sikkerhedsformål i henhold til loven, navnlig i henhold til Foreign*

[106] Se udkast til afgørelse, betragtning 102.
[107] Se Databeskyttelsesrådets anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger.
[108] Se Domstolens dom i Schrems II-sagen, præmis 98.
[109] Se Domstolens dom i La Quadrature du Net-sagen, præmis 124.

Intelligence Surveillance Act (FISA) eller lovbestemmelser, der tillader indsigt via nationale sikkerhedsbreve (National Security Letters (NSL))"[110]. "*Amerikanske efterretningstjenester har også mulighed for at indsamle personoplysninger uden for USA, hvilket kan omfatte personoplysninger i transit mellem Unionen og USA*" i henhold til Executive Order 12333 (EO 12333)[111].

105. Med hensyn til de specifikke dataindsamlingsordninger, navnlig Section 702 i FISA og EO 12333, indeholder EO 14086 nu nye regler for at styrke garantierne for USA's signalefterretningsaktiviteter. Disse generelle regler gælder horisontalt og "*skal gennemføres yderligere ved hjælp af agenturernes politikker og procedurer, der omsætter dem til konkrete retningslinjer for den daglige drift*"[112]. EO 14086 har for det meste erstattet det tidligere præsidentielle direktiv, Presidential Policy Directive 28 ("PPD-28")[113].

106. For at vurdere de retlige rammer for indsamling af, adgang til og yderligere behandling af data til nationale sikkerhedsformål er det derfor vigtigt at undersøge de specifikke retlige rammer for indsamling af data i og uden for USA, dvs. Section 702 i FISA og EO 12333, der som sådan ikke har ændret sig siden den foregående evaluering af privatlivsskjoldet, under hensyntagen til, at det nye Executive Order 14086 indeholder garantier, der også skal gennemføres i forbindelse med indsamling af data på grundlag af specifikke tekster såsom Section 702 i FISA og EO 12333.

3.2.1 Garanti A — Behandling bør være i overensstemmelse med lovgivningen og baseret på klare, præcise og tilgængelige regler

107. Med henblik på sin vurdering af den generelle udformning af dataindsamling af hensyn til den nationale sikkerhed ønsker Databeskyttelsesrådet at minde om den første af de fire såkaldte "europæiske væsentlige garantier", ifølge hvilke "behandling skal være baseret på klare, præcise og tilgængelige regler"[114].

108. I overensstemmelse med EU-Domstolens faste retspraksis skal enhver begrænsning af retten til beskyttelse af personoplysninger være fastlagt i lovgivningen, og det retsgrundlag, som tillader et indgreb i en sådan ret, skal selv definere rækkevidden af den pågældende begrænsning af udøvelsen af den pågældende rettighed[115]. EU-Domstolen mindede også om, at "lovgivning skal være retligt bindende i national ret"[116]. I denne henseende præciseres det i Menneskerettighedsdomstolens praksis, at begrebet "lov" skal forstås i sin materielle betydning og ikke i sin formelle betydning. Det kan omfatte vedtagelse af lavere rangerende love og lovgivningsmæssige foranstaltninger truffet af faglige tilsynsorganer i henhold til uafhængige lovgivningsbeføjelser, som er delegeret til dem af

[110] Se udkast til afgørelse, betragtning 115.
[111] Se udkast til afgørelse, betragtning 117.
[112] Se udkast til afgørelse, betragtning 120.
[113] Dette dekret tilbagekalder PPD-28 med undtagelse af Section 3 og 6 i dette direktiv og det klassificerede bilag til dette direktiv, som fortsat er gældende. Se præsidentens nationale sikkerhedsnotat af 7. oktober 2022.
[114] Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, vedtaget den 10. november 2020. Se præmis 175 og 180 i Schrems II og udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26. juli 2017, § 139, og den deri nævnte retspraksis.
[115] Se Domstolens dom i Schrems II-sagen, præmis 174-175 og den deri anførte retspraksis. Se også for så vidt angår adgang for medlemsstaternes offentlige myndigheder sag C-623/17 Privacy International ECLI:EU:C:2020:790 ("Domstolens dom i Privacy International-sagen"), præmis 65, og Domstolens dom i La Quadrature du Net-sagen, præmis 175.
[116] Domstolens dom i Privacy International-sagen, præmis 68.

parlamentet, og endog uskreven lovgivning. For at være "lov" skal en norm i det mindste være tilstrækkeligt tilgængelig og formuleret med tilstrækkelig præcision[117].

109. Den krævede grad af præcision skal måles i forhold til omfanget af begrænsningen af rettigheden[118]. Med hensyn til lovens "forudsigelighed" mindede Menneskerettighedsdomstolen i dommen i Zakharov-sagen endvidere om, at i forbindelse med hemmelige overvågningsforanstaltninger såsom kommunikationsaflytning, kan "forudsigelighed ikke betyde, at en person kan forudse, hvornår myndighederne sandsynligvis vil aflytte dennes kommunikation, således at vedkommende kan tilpasse sin adfærd i overensstemmelse hermed". Klare og detaljerede regler om hemmelig overvågning er imidlertid afgørende for at forebygge risikoen for vilkårlighed, når den udøvende magt udøves i hemmelighed. "Den nationale lovgivning skal være tilstrækkelig klar til at give borgerne et passende fingerpeg om, under hvilke omstændigheder og på hvilke betingelser de offentlige myndigheder har beføjelse til at anvende sådanne foranstaltninger"[119].

110. Desuden præciserede EU-Domstolen, at vurderingen af gældende tredjelandslovgivning bør fokusere på, om den kan påberåbes og gøres gældende af enkeltpersoner ved en domstol. De rettigheder, der gives til registrerede, bør navnlig kunne anfægtes, og enkeltpersoner skal have rettigheder, der kan håndhæves over for offentlige myndigheder[120], hvilket ikke var tilfældet i forbindelse med det tidligere PPD-28. EO 14086, som ifølge Databeskyttelsesrådet anses for at have samme retsvirkning inden for den amerikanske retsorden som PPD-28 (dvs. bindende for den udøvende magt), giver nu mulighed for at anlægge sag mod offentlige myndigheder. En detaljeret vurdering af de registreredes nye rettigheder, der kan håndhæves, findes i afsnittet om klageadgang.

111. Betragtning 114-152 i udkastet til afgørelse og bilag VII indeholder et resumé af visse aspekter af den gældende retlige ramme, indsamlingsbegrænsninger, begrænsninger for opbevaring og formidling, overholdelse og tilsyn, gennemsigtighed og klagemuligheder. Det amerikanske retssystem for efterretningsaktiviteter består af en række forskellige dokumenter, herunder individuelle rapporter fra agenturer, politikker og procedurer. I den forbindelse fokuserer Databeskyttelsesrådets evaluering på et begrænset antal spørgsmål, som det anser for afgørende.

112. I henhold til betragtning 115-119 i udkastet til afgørelse kan amerikanske nationale sikkerhedsmyndigheder kun få adgang til overførte personoplysninger i henhold til FISA i henhold til andre lovbestemmelser (United States Code, afsnit 12, § 3414, United States Code, afsnit 15, § 1681u-1681v og United States Code, afsnit 18, § 2709) eller i forbindelse med personoplysninger i transit på grundlag af EO 12333. Det fremgår af betragtning 116 og 118 i udkastet til afgørelse, at Kommissionen i forbindelse med de amerikanske nationale sikkerhedsmyndigheders adgang til personoplysninger fokuserer sin vurdering på Section 105, 302, 402, 501 og 702 i FISA (udenlandske efterretningsaktiviteter rettet mod ikkeamerikanske personer uden for USA) og EO 12333 (udenlandske efterretningsaktiviteter vedrørende personoplysninger i transit) som de mest relevante.

[117] Menneskerettighedsdomstolen, Sunday Times mod Det Forenede Kongerige (nr. 1), 26. april 1979, CE:ECHR:1979:0426JUD000653874 ("Menneskerettighedsdomstolens dom i Sunday Times mod Det Forenede Kongerige nr. 1-sagen"), præmis 49.
[118] Menneskerettighedsdomstolens dom i Sunday Times mod Det Forenede Kongerige nr. 1-sagen, præmis 49.
[119] Menneskerettighedsdomstolen, Zakharov mod Rusland, 4. december 2015 ("Menneskerettighedsdomstolens dom i Zakharov-sagen"), præmis 229.
[120] Domstolens dom i Schrems II-sagen, præmis 181.

Databeskyttelsesrådets udtalelse er derfor begrænset til Kommissionens vurdering af disse bestemmelser under hensyntagen til de begrænsninger og garantier, der er fastsat i EO 14086[121].

113. I den forbindelse skal det bemærkes, at alle de retlige instrumenter, der er nævnt i udkastet til afgørelse, er tilgængelige for offentligheden (i og uden for USA) og tilgængelige online. Desuden er de krav, der er fastsat i dekretet, bindende for alle efterretningstjenester[122], og de gælder på en tværgående måde for alle udenlandske efterretningsaktiviteter.

114. Begrebet "signalefterretning" er ikke defineret i EO 14086. Sidstnævnte henviser til definitionerne i EO 12333 med henblik på at fastlægge omfanget af udenlandske efterretninger og kontraefterretninger, som er bredt defineret. Selv om det er blevet fremført, at EO 12333 siden indførelsen af FISA kun kan anvendes til indsamling af data uden for USA's område, minder Databeskyttelsesrådet om, at EO 12333 (som fortsat er intakt) selv mangler tilstrækkelige oplysninger om sit geografiske anvendelsesområde, i hvilket omfang data kan indsamles, opbevares eller videreformidles, om arten af de lovovertrædelser, der kan give anledning til overvågning, samt om typen af oplysninger, der kan indsamles eller anvendes. I princippet kan al indsamling af udenlandske efterretningsdata inden for rammerne af EO 12333 finde sted efter den amerikanske præsidents skøn[123]. Efter Databeskyttelsesrådets opfattelse er hovedformålet med EO 14086 imidlertid at fastsætte grænserne for indsamling og behandling af personoplysninger i forbindelse med udenlandske efterretninger, uanset hvilket overvågningsprogram der anvendes, og hvor data indhentes fra. Det er derfor Databeskyttelsesrådets opfattelse, at de yderligere garantier, der er fastsat i EO 14086, også gælder i forbindelse med overvågningsprogrammer, der gælder for personoplysninger i transit i henhold til EO 12333[124].

115. I denne forbindelse indeholder EO 14086 en liste over 12 legitime mål, der bør forfølges ved indsamling af signalefterretninger, fem mål, for hvilke der ikke må indsamles signalefterretninger[125], samt seks legitime mål for anvendelsen af masseindsamlede data[126]. Mens nogle af dem er ret detaljerede (f.eks. "redning af gidsler"), er andre mere generelle (f.eks. "global sikkerhed"). EO 14086 indeholder også en liste over forbudte mål, som navnlig omfatter fjernelse eller begrænsning af "legitime interesser i beskyttelsen af privatlivets fred"[127]. EO 14086 giver også USA's præsident mulighed for at tilføje andre mål til listen, som det er tilladt at indsamle, og som efter præsidentens afgørelse ikke kan offentliggøres, hvis præsidenten mener, at dette ville udgøre en risiko for USA's nationale sikkerhed[128]. Sådanne ajourføringer kan kun godkendes "i lyset af nye krav til den nationale sikkerhed".

116. Efterretningsagenturerne kan ikke i sig selv påberåbe sig målene som begrundelse for indsamling af signalefterretninger, men de skal til operationelle formål yderligere underbygges i mere konkrete prioriteter, hvor signalefterretninger kan indsamles. EO 14086 beskriver proceduren for validering af de prioriteter, for hvilke signalefterretninger kan indsamles[129]. Databeskyttelsesrådet forstår, at

121 Dette dekret tilbagekalder PPD-28 med undtagelse af Section 3 og 6 i dette direktiv og det klassificerede bilag til dette direktiv, som fortsat er gældende. Se præsidentens nationale sikkerhedsnotat af 7. oktober 2022.
122 Se udkast til afgørelse, betragtning 120.
123 I henhold til artikel II i den amerikanske forfatning henhører ansvaret for den nationale sikkerhed, herunder navnlig indsamling af udenlandske efterretninger, under præsidentens myndighed som øverstbefalende for de væbnede styrker.
124 Se udkast til afgørelse, betragtning 134.
125 Se Executive Order 14086 ("EO 14086"), Section 2(b)(ii)A(1)-(5).
126 Se udkastet til afgørelse, betragtning 134 og EO 14086, Section 2(c)(ii).
127 Se EO 14086, Section 2(b)(ii)(A)(2).
128 Se EO 14086, Section 2(b)(i)(B).
129 Se udkast til afgørelse, betragtning 129.

processen til fastlæggelse af de validerede efterretningsprioriteter i princippet afhænger af direktøren for efterretningstjenesterne, og anerkender, at den som hovedregel bør omfatte en vurdering foretaget af Civil Liberties Protection Officer hos direktøren for National Intelligence (CLPO), som direktøren kan være uenig i, i hvilket tilfælde den "skal omfatte CLPO's vurdering og direktørens synspunkter, når den fremlægger "National Intelligence Priorities Framework" (NIPF) for præsidenten"[130].

117. Databeskyttelsesrådet bemærker imidlertid også, at i henhold til definitionen af "*valideret efterretningsprioritet*" betyder sådanne prioriteter for "*de fleste amerikanske indsamlinger af signalefterretninger*"[131] en prioritet, der er valideret i henhold til Section 2(b)(iii), i dekretet (beskrevet i foregående afsnit). Valideringsprocessen kan i nogle tilfælde afvige fra denne proces under "*snævre omstændigheder*", i hvilket tilfælde formanden eller lederen af et element af efterretningstjenesterne kan fastsætte en prioritet "*så vidt muligt*" i overensstemmelse med kriterierne i samme Section 2(b)(iii)(A)(1)-(3), som omfatter kravet om passende hensyntagen til privatlivets fred og borgerlige frihedsrettigheder for alle personer, men uden inddragelse af CLPO.

118. I EO 14086 pointeres det desuden, at "indsamling af signalefterretninger skal være så skræddersyet som muligt" for at fremme en valideret efterretningsprioritet, og at "efterretningstjenesterne skal overveje tilgængeligheden, gennemførligheden og hensigtsmæssigheden af andre mindre indgribende kilder", ligesom der fastsættes generelle nødvendigheds- og proportionalitetskrav[132].

119. I henhold til Section 5(h), giver EO 14086 desuden ret til at indgive kvalificerede klager til CLPO og til at få CLPO's afgørelser prøvet af appeldomstolen for databeskyttelse (Data Protection Review Court), i overensstemmelse med den klagemekanisme, der er fastsat i dekretets Section 3.

120. FISA's tekst synes at være klarere og mere præcis end EO 12333 for så vidt angår typen af efterretningsoperationer, der kan foreskrives. FISA og EO 12333 skal nu anvendes i lyset af EO 14086 og navnlig under hensyntagen til bl.a. nødvendigheds- og proportionalitetsprincipperne.

121. Kravene i EO 14086 skal gennemføres yderligere ved hjælp af agenturernes politikker og procedurer, der omsætter dem til konkrete retningslinjer for den daglige drift. I den forbindelse giver EO 14086 amerikanske efterretningstjenester en frist på højst et år til at ajourføre deres eksisterende politikker og procedurer (dvs. senest den 7. oktober 2023) for at bringe dem i overensstemmelse med kravene i dekretet. Sådanne ajourførte politikker og procedurer skal udarbejdes i samråd med den amerikanske justitsminister (Attorney General), CLPO og Privacy and Civil Liberties Oversight Board (PCLOB) og gøres offentligt tilgængelige i videst muligt omfang[133].

122. Databeskyttelsesrådet ser med tilfredshed på, at ikke blot ikrafttrædelsen, men også vedtagelsen af afgørelsen bl.a. er betinget af, at alle amerikanske efterretningstjenester vedtager ajourførte politikker og procedurer for gennemførelse af EO 14086. Databeskyttelsesrådet anbefaler Kommissionen at vurdere disse ajourførte politikker og procedurer og dele denne vurdering med Databeskyttelsesrådet.

123. Endelig bemærker Databeskyttelsesrådet i forbindelse med opbevaring af de overførte data, når de er indsamlet til nationale sikkerhedsformål, at EO 14086 sikrer, at de regler, der gælder for amerikanske personers personoplysninger, også finder anvendelse på ikkeamerikanske personers

[130] Se EO 14086, Section 2(b)(iii)(B).
[131] Se EO 14086, Section 4(n).
[132] Se EO 14086, Section 2(c)(i)(A) og (B).
[133] Se EO 14086, Section 2(c)(iv)(B) og (C).

personoplysninger[134]. Af udkastet til afgørelse fremgår det, at disse regler er fastsat i Section 309 i Intelligence Authorization Act for Fiscal Year 2015[135], som i princippet fastsætter en maksimal opbevaringsperiode på fem år for enhver ikkeoffentlig telefonkommunikation eller elektronisk kommunikation, der er erhvervet uden personens samtykke. Databeskyttelsesrådet anbefaler i denne forbindelse, at Kommissionen skaber større klarhed med hensyn til sin vurdering af de opbevaringsregler, der gælder for amerikanske personers personoplysninger, i afgørelsen.

3.2.2 Garanti B — De forfulgte legitime formåls nødvendighed og proportionalitet skal kunne påvises

3.2.2.1 Horisontale garantier i det nye Executive Order 14086 — nødvendighed og proportionalitet

124. Det nye EO 14086, som generelt erstatter PPD-28, har til formål at fastsætte regler for at styrke sikkerhedsforanstaltningerne for amerikanske signalefterretningsaktiviteter, som skal gennemføres yderligere af efterretningsenhederne i deres interne politikker og procedurer.

125. Med EO 14086 indføres to nye krav i amerikansk ret, som afspejler kravene i Domstolens dom i Schrems II-sagen, nemlig at signalefterretningsaktiviteter kun må udføres i det omfang, det er nødvendigt for at fremme en valideret prioriteret indsamling af efterretninger, og kun i et omfang og på en måde, der står i et rimeligt forhold til den validerede efterretningsprioritet[136].

126. Det er Databeskyttelsesrådets opfattelse, at disse elementer er medtaget for at afspejle de nødvendigheds- og proportionalitetsprincipper, der er fastsat i EU-retten og i EU-Domstolens og Den Europæiske Menneskerettighedsdomstols retspraksis, og som har til formål at sikre, at indsamling og behandling af data begrænses til, hvad der er nødvendigt og forholdsmæssigt.

127. I denne forbindelse minder Databeskyttelsesrådet om den planlagte proces for validering af efterretningsprioriteter samt den mulige undtagelse (jf. punkt 116, 117).

128. Databeskyttelsesrådet bemærker endvidere, at disse nødvendigheds- og proportionalitetsprincipper, der er fastsat i dekretet, skal operationaliseres og gennemføres inden for et år i de politikker og procedurer, der gælder for hvert element i efterretningstjenesterne[137].

3.2.2.2 Særlige garantier for indsamling af signalefterretninger

129. Databeskyttelsesrådet bemærker også, at EO 14086 indeholder begrænsninger med hensyn til de mål, for hvilke personoplysninger kan og ikke kan indsamles i forbindelse med indsamling af signalefterretninger[138].

130. Databeskyttelsesrådet glæder sig over, at dekretet fastsætter, at målrettet indsamling bør prioriteres frem for masseindsamling[139]. I forbindelse med indsamling af signalefterretninger opstiller dekretet en liste over 12 mål, for hvilke der kan indsamles data, som skal underbygges yderligere i efterretningsprioriteter (jf. punkt 117), samt en liste over fem mål, for hvilke der ikke må foretages

[134] Udkast til afgørelse, betragtning 150.
[135] Udkast til afgørelse, fodnote 272.
[136] Se EO 14086, Section 2(b)(ii)A og B.
[137] Se EO 14086, Section 2(c)(iv)B.
[138] Se EO 14086, Section 2(b)(i)A,1-12.
[139] Se EO 14086, Section 2(c)(ii)A.

indsamling af signalefterretninger[140]. Disse bestemmelser udgør i princippet en garanti for, at indsamlingen af data er nødvendig.

131. Databeskyttelsesrådet minder dog om, at EO 14086 også giver USA's præsident mulighed for at tilføje andre mål til listen (jf. punkt 114 og 115)[141].

3.2.2.3 Særlige garantier for masseindsamling

132. Domstolen understregede i sin Schrems I-dom, at "*beskyttelsen af den grundlæggende ret til respekt for privatlivet på EU-plan [kræver] særligt, at undtagelserne fra og begrænsningerne af beskyttelsen af personoplysninger holdes inden for det strengt nødvendige*"[142] og fastslog, at "*en lovgivning, der gør det muligt for de offentlige myndigheder på generel vis at få adgang til indholdet af elektronisk kommunikation, [skal] anses for at udgøre et indgreb i det væsentligste indhold af den grundlæggende ret til respekt for privatlivet, således som denne er sikret ved chartrets artikel 7*".

133. I Schrems II-sagen[143] understregede Domstolen med hensyn til sin analyse af masseindsamling i forbindelse med den dermed forbundne læsning af EO 12 333 og PPD-28, navnlig præmis 183-185, som nævnt ovenfor, at muligheden for masseindsamling, "*som inden for rammerne af overvågningsprogrammer baseret på EO 12333 tillader adgang til oplysninger i transit til USA, uden at denne adgang er underlagt noget retsligt tilsyn, afgrænser dog under alle omstændigheder ikke tilstrækkeligt klart og præcist omfanget af en sådan masseindsamling af personoplysninger.* "

134. Databeskyttelsesrådet bemærker derfor, at EU-Domstolen i princippet ikke udelukkede masseindsamling, men at den i sin Schrems II-afgørelse fastslog, at for at en sådan masseindsamling kan finde sted på lovlig vis, skal der være en tilstrækkeligt klar og præcis afgrænsning af omfanget af en sådan masseindsamling.

135. Databeskyttelsesrådet anerkender også, at EO 14086, samtidig med at den erstatter PPD-28, indeholder nye garantier og begrænsninger for indsamling og anvendelse af data indsamlet uden for USA, da begrænsningerne i FISA eller andre mere specifikke amerikanske love ikke finder anvendelse.

136. Med hensyn til masseindsamling af data noterer Databeskyttelsesrådet sig, at det i EO 14086 fastsættes, at masseindsamling fortsat er tilladt. Databeskyttelsesrådet understreger, at definitionen af masseindsamling er den samme som i den tidligere PPD-28: "*Masseindsamling af signalefterretninger er godkendt indsamling af store mængder signalefterretningsdata, der på grund af tekniske eller operationelle forhold foretages uden brug af diskriminanter (f.eks. specifikke identifikatorer, selektorer osv.)*"[144].

137. Efter dommen i Schrems II-sagen præciserede Domstolen ikke præcist, hvilke garantier der var nødvendige for, at masseindsamling kunne finde sted. Databeskyttelsesrådet minder imidlertid om, at EMRK har truffet vigtige afgørelser vedrørende masseindsamling og de relevante garantier i denne forbindelse.

[140] Se EO 14086, Section 2(b)(ii)A,1-5.
[141] Se EO 14086, Section 2(b)(i)B.
[142] Domstolens dom i Schrems I-sagen, præmis 92.
[143] Se Domstolens dom i Schrems II-sagen.
[144] Se EO 14086, Section 4(b).

138. Databeskyttelsesrådet minder om, at masseindsamling ved at give mulighed for indsamling af store mængder data uden forskelsbehandling udgør en større risiko for enkeltpersoner[145] end målrettet indsamling og derfor kræver, at der indføres yderligere garantier.

139. Databeskyttelsesrådet bemærker også, at EU-Domstolen har udviklet yderligere retspraksis vedrørende lagring af trafik- og lokaliseringsdata og efterfølgende adgang til disse data, der opbevares af teleoperatører, herunder af hensyn til den nationale sikkerhed, som, selv om de ikke kan anses for at være direkte anvendelige i denne sammenhæng, i et vist omfang kan være relevante i forbindelse med den nuværende vurdering af masseindsamling i forbindelse med EO 12333.

1) Formålsbegrænsning

140. Dekretet fastsætter, at masseindsamling kun bør finde sted, når det er fastslået, at "de oplysninger, der er nødvendige for at fremme en valideret efterretningsmæssig prioritet, ikke med rimelighed kan indhentes gennem målrettet indsamling"[146], og at "efterretningstjenesternes element anvender rimelige metoder og tekniske foranstaltninger for at begrænse de indsamlede data til, hvad der er nødvendigt for at fremme en valideret efterretningsprioritet, samtidig med at indsamlingen af ikkerelevante oplysninger minimeres"[147]. Ud over disse garantier anerkender Databeskyttelsesrådet også, at anvendelsen af masseindsamlede data skal anvendes med henblik på at nå et eller flere af de seks anførte mål[148]. Databeskyttelsesrådet understreger endvidere, at selv om disse mål er mere detaljerede end dem, der blev fastsat i det tidligere PPD-28, der generelt er erstattet af EO 14086, er omfanget af sådanne indsamlingsmuligheder potentielt brede, dvs. omfatter store mængder data.

141. Databeskyttelsesrådet minder også her om, at EO 14086 også giver USA's præsident mulighed for at tilføje andre mål til listen (jf. punkt115)[149].

2) Forudgående uafhængig godkendelse

142. Databeskyttelsesrådet understreger, at Menneskerettighedsdomstolen lægger stor vægt på forudgående uafhængig godkendelse i forbindelse med masseindsamling af data til nationale sikkerhedsformål. Domstolen fastslog navnlig, at "*for at minimere risikoen for misbrug af beføjelsen til masseaflytning finder Domstolen, at processen skal være underlagt "end-to-end-garantier", hvilket betyder, at der på nationalt plan bør foretages en vurdering af nødvendigheden og proportionaliteten af de foranstaltninger, der træffes, på hvert trin i processen, at masseaflytning bør være betinget af en uafhængig tilladelse fra begyndelsen, når genstanden for og omfanget af operationen er ved at blive fastlagt, og at operationen bør være underlagt tilsyn og uafhængig efterfølgende kontrol. Domstolen mener, at der er tale om grundlæggende garantier, som vil være hjørnestenen i enhver ordning for masseaflytning, der er i overensstemmelse med artikel 8*"[150].

143. Databeskyttelsesrådet bemærker også følgende præmis i denne dom i Store Afdeling, hvor domstolen i Strasbourg endvidere fremhæver, at den "*er enig med afdelingen i, at selv om retskendelse er en*

[145] Se f.eks. Menneskerettighedsdomstolen (Store Afdeling), Big Brother Watch m.fl. mod Det Forenede Kongerige, 25. maj 2021 ("Menneskerettighedsdomstolens dom i Big Brother Watch-sagen"), betragtning 363, hvor domstolen anfører, at den "*ikke er overbevist om, at indsamling af relaterede kommunikationsdata gennem masseaflytning nødvendigvis er mindre indgribende end erhvervelse af indhold*".

[146] EO 14086, Section 2(c)(ii)(A).

[147] EO 14086, Section 2(c)(ii)(A).

[148] EO 14086, Section 2(c)(ii)(B).

[149] Se EO 14086, Section 2(c)(ii)(C).

[150] Se Menneskerettighedsdomstolens dom i Big Brother Watch-sagen, præmis 350.

"vigtig garanti mod vilkårlighed", er det ikke et "nødvendigt krav" (se præmis 318-320 i afdelingens dom). Masseaflytning bør dog godkendes af et uafhængigt organ, dvs. et organ, der er uafhængigt af den udøvende magt"[151].

144. I denne forbindelse bemærker Databeskyttelsesrådet, at dekretet ikke giver en sådan uafhængig forudgående tilladelse til masseindsamling, og at dette heller ikke er foreskrevet i EO 12333 (se afsnittet nedenfor om EO 12333).

3) <u>Opbevaringsregler</u>

145. Databeskyttelsesrådet minder om, at et andet vigtigt sæt garantier er reglerne for varigheden af indsamlingen og opbevaringen af data. I denne forbindelse understregede Menneskerettighedsdomstolen, at "*den nationale lovgivning bør fastsætte en grænse for varigheden af opfangningen, den procedure, der skal følges ved undersøgelse, anvendelse og lagring af de indhentede data, de forholdsregler, der skal træffes, når oplysningerne videregives til andre parter, og de omstændigheder, hvorunder opfangne data kan eller skal slettes eller destrueres*"[152], da disse garantier "*er lige så relevante for masseaflytning*"[153].

146. I denne forbindelse er det Databeskyttelsesrådets opfattelse, at dekretet fastsætter regler for opbevaring af personoplysninger, der er indsamlet gennem signalefterretninger, herunder masseindsamling[154]. Databeskyttelsesrådet bemærker, at i henhold til Section 2(c)(iii)(A) i EO 14086 skal hvert element i efterretningstjenesterne, der håndterer personoplysninger indsamlet ved hjælp af signalefterretninger, fastlægge og anvende politikker og procedurer, der er udformet med henblik på at minimere udbredelsen og opbevaringen af personoplysninger indsamlet gennem signalefterretninger. Disse regler fastsætter imidlertid ikke en specifik opbevaringsperiode, men henviser snarere generelt til de samme gældende regler for opbevaring af data vedrørende amerikanske personer og til situationer, hvor der ikke er truffet en endelig afgørelse om opbevaring. Databeskyttelsesrådet er derfor bekymret over, at disse opbevaringsperioder som for målrettet indsamling (se punkt 122) ikke er klart defineret i dette dekret med hensyn til masseindsamlede data. Databeskyttelsesrådet opfordrer Kommissionen til at dele sin vurdering af nødvendigheden og proportionaliteten af de opbevaringsperioder, der gælder for amerikanske personer, og de tilgængelige oplysninger om opbevaringsperioder i praksis, hvor der ikke er truffet en endelig afgørelse om opbevaring i henhold til amerikansk lovgivning, da udkastet til afgørelse i sin nuværende form blot minder om denne generelle regel i et enkelt kort afsnit[155] og en fodnote[156], som ikke gør det muligt at afgøre, om disse opbevaringsperioder er nødvendige og forholdsmæssige. Eftersom dette, som understreget af Den Europæiske Menneskerettighedsdomstol, er en afgørende garanti for, at registrerede kan udøve deres rettigheder i en kontekst, hvor der træffes en særlig indgribende foranstaltning for i første omgang at indsamle deres data, opfordrer Databeskyttelsesrådet Europa-Kommissionen til at give yderligere præciseringer vedrørende de forskellige opbevaringsperioder i praksis.

4) <u>Garantier vedrørende "formidling"</u>

[151] Se Menneskerettighedsdomstolens dom i Big Brother Watch-sagen, præmis 351.
[152] Se Menneskerettighedsdomstolens dom i Big Brother Watch-sagen, præmis 348.
[153] Se Menneskerettighedsdomstolens dom i Big Brother Watch-sagen, præmis 348.
[154] Se EO 14086, Section 2(c)(iii)A(2)(a)-(c).
[155] Se udkast til afgørelse, punkt 150.
[156] Se udkast til afgørelse, fodnote 271.

147. Databeskyttelsesrådet minder også om, at Menneskerettighedsdomstolen for at sikre effektiviteten af nødvendighed og proportionalitet og princippet om formålsbegrænsning også anerkendte betydningen af lovfæstede regler om yderligere formidling af de indsamlede data, herunder i forbindelse med masseindsamling[157].

148. Section 2(c)(iii)(A)(1)(c) i EO 14086 fastsætter, at oplysninger om ikkeamerikanske personer, der er indsamlet gennem signalefterretningsaktiviteter, kun må videregives, hvis en autoriseret og behørigt uddannet person har en rimelig formodning om, at personoplysningerne vil blive beskyttet på passende vis, og at modtageren har behov for at kende oplysningerne.

149. I betragtning heraf forstår Databeskyttelsesrådet, at bestemmelserne om formidling i EO 14086 ikke indeholder noget udtrykkeligt forbud mod formidling til andre formål end nationale sikkerhedsformål, når det drejer sig om formidling til amerikanske kompetente myndigheder[158]. Databeskyttelsesrådet opfordrer Kommissionen til yderligere at præcisere de gældende regler og garantier i dette tilfælde.

150. Databeskyttelsesrådet er derfor bekymret over, at data indhentet af de kompetente efterretningsmyndigheder derefter kan videregives til USA's kompetente myndigheder med henblik på at bekæmpe kriminalitet, herunder grov kriminalitet, i forbindelse med strafferetlig efterforskning, hvorved de retshåndhævende myndigheder uden yderligere specifikke begrænsninger får mulighed for at indhente data, som det ville have været forbudt for dem at indsamle direkte, og Databeskyttelsesrådet opfordrer derfor Kommissionen til at foretage en yderligere vurdering af dette punkt.

151. I forbindelse med videreoverførsler (formidling til modtagere uden for USA's regering, herunder til en udenlandsk regering eller international organisation[159]) minder Databeskyttelsesrådet om, at det er af den opfattelse, at den beskyttelse, der ydes oplysninger, også bør opretholdes i forbindelse med videreoverførsel, herunder på området national sikkerhed[160].

152. I denne forbindelse fastsætter dekretet visse garantier, nemlig kravet om at tage behørigt hensyn til formålet med formidlingen — om end uden udtrykkeligt at kræve, at formålet med formidlingen også skal være at beskytte den nationale sikkerhed — arten og omfanget af de formidlede personoplysninger og de potentielle skadelige virkninger for den eller de berørte personer, inden oplysningerne formidles.

153. Selv om Databeskyttelsesrådet anerkender, at nogle af disse garantier, navnlig vedrørende "*muligheden for skadelig indvirkning*"[161] på den eller de berørte registrerede, afspejler visse krav i EMRK, understreger det også, at domstolen i Strasbourg desuden kræver en juridisk bindende forpligtelse "*til at analysere og afgøre, om den udenlandske modtager af efterretninger tilbyder et acceptabelt minimumsniveau af garantier*"[162], hvilket Databeskyttelsesrådet ikke udtrykkeligt finder i dekretets bestemmelser om formidling til udenlandske modtagere. Databeskyttelsesrådet opfordrer derfor Kommissionen til yderligere at vurdere dette element.

---

[157] Se Menneskerettighedsdomstolens dom i Big Brother Watch-sagen, præmis 348.
[158] Se EO 14086, Section 2(c)(iii)(A)(1).
[159] Se navnlig EO 14086, Section 2(c)(iii)(A)(1)(d).
[160] Se f.eks. Databeskyttelsesrådet, Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom. Vedtaget den 13. april 2021, afsnit 4.3.2.1 og 4.3.2.2.
[161] Se EO 14086, Section 2(c)(iii)(A)(1)(d).
[162] Se Menneskerettighedsdomstolen (Store Afdeling), sagen Centrum För Rättvisa mod Sverige, 25. maj 2021, præmis 326.

154. Databeskyttelsesrådet bemærker også, at Europa-Kommissionen som led i sin vurdering af tilstrækkeligheden ikke tog hensyn til eksisterende internationale aftaler indgået med tredjelande eller internationale organisationer, der kan fastsætte specifikke bestemmelser for efterretningstjenesters internationale overførsel af personoplysninger til tredjelande. Databeskyttelsesrådet mener, at indgåelsen af bilaterale eller multilaterale aftaler med tredjelande med henblik på efterretningssamarbejde sandsynligvis vil påvirke de retlige rammer for databeskyttelse som vurderet.

155. Databeskyttelsesrådet opfordrer derfor Europa-Kommissionen til at præcisere, om der findes sådanne aftaler, på hvilke betingelser de kan indgås, og vurdere, om bestemmelserne i internationale aftaler kan påvirke beskyttelsesniveauet for personoplysninger, der overføres fra EØS som følge af den lovgivningsmæssige ramme og praksis i forbindelse med videreoverførsel af hensyn til den nationale sikkerhed.

5) Midlertidig masseindsamling til støtte for den indledende tekniske fase af målrettet indsamling

156. Databeskyttelsesrådet minder om, at der under drøftelserne i forbindelse med den seneste fælles gennemgang af privatlivsskjoldet primært var fokus på fortolkningen og anvendelsen af den yderligere grund (situation/scenarie) til masseindsamling, der er omhandlet i første punktum i fodnote 5 i afsnit 2 i PPD-28, hvori det hedder, at "*begrænsningerne i dette afsnit finder ikke anvendelse på signalefterretningsdata, der midlertidigt erhverves for at lette målrettet indsamling*". De amerikanske myndigheder forklarede på daværende tidspunkt betydningen af "*signalefterretningsdata, der midlertidigt erhverves for at lette målrettet indsamling*". Databeskyttelsesrådet forstod på baggrund af disse drøftelser, at denne fodnote betød, at data kan masseindsamles — og uanset de seks planlagte formål — hvis de indsamles midlertidigt, med henblik på at fastlægge en identifikator for et defineret mål. Dette ville således være en yderligere grund til at masseindsamle data, og i dette tilfælde ville kun de generelle principper i Section 1 i PPD-28 stadig have fundet anvendelse. Som nævnt ovenfor fandt EU-Domstolen i sin dom i Schrems II-sagen, at den kombinerede EO 12333 og PPD-28 med hensyn til masseindsamling ikke "*tilstrækkeligt klart og præcist [afgrænser] omfanget af en sådan masseindsamling af personoplysninger*"[163].

157. Databeskyttelsesrådet bemærker, at der stadig er fastsat en undtagelse, der tillader en sådan form for masseindsamling, i EO 14086[164]. Databeskyttelsesrådet glæder sig imidlertid over, at denne undtagelse er blevet indsnævret i forhold til PPD-28, og at der gives yderligere garantier i henhold til EO 14086.

158. Databeskyttelsesrådet forstår, at den nye EO 14086 indeholder garantier, der fortsat finder anvendelse i forbindelse med denne type midlertidig teknisk masseindsamling, navnlig de generelle principper om nødvendighed og proportionalitet i forhold til den validerede efterretningsprioritet, når data indhentes uden forskelsbehandling, inden målrettet indsamling finder sted (Section 2(a)-(b), Section 2(c)(i) i EO 14086). Det er også Databeskyttelsesrådets opfattelse, at en sådan masseindsamling til støtte for en efterfølgende målrettet indsamling af signalefterretninger også er omfattet af de yderligere garantier i subsection (2)(c)(iii) og fremefter[165].

159. Databeskyttelsesrådet minder imidlertid også — jf. punkt 117 ovenfor — om, at definitionen af "*valideret efterretningsprioritet*" giver mulighed for en undtagelsesprocedure, som ikke involverer CLPO under direktøren for National Intelligence.

[163] Domstolens dom i Schrems II-sagen, præmis 183.
[164] Se EO 14086, Section 2(c)(ii)D og udkast til afgørelse, fodnote 226.
[165] Se de foregående afsnit for yderligere oplysninger om disse bestemmelser.

160. Databeskyttelsesrådet bemærker imidlertid stadig, at garantierne i underafsnittet vedrørende masseindsamling ikke finder anvendelse på midlertidig masseindsamling, der anvendes til at understøtte den indledende tekniske fase af målrettet indsamling af signalefterretninger som beskrevet i Section 2(c)(ii)(D) i EO 14086, hvilket navnlig betyder, at masseindsamlet data i denne forbindelse kan anvendes til andre formål end dem, der er anført i subsection 2(c)(ii). Databeskyttelsesrådet ser med tilfredshed på præciseringer i udkastet til afgørelse om de formål, hvortil masseindsamlede data i denne forbindelse kan anvendes, samt vedrørende anvendelsen af de begrænsninger, der er fastsat i subsection 2(c)(i), for indsamling af signalefterretninger generelt (dvs. kun til de legitime mål, der er anført deri) i forbindelse med midlertidig masseindsamling i udkastet til afgørelse.

161. Som konklusion understreger Databeskyttelsesrådet også, at denne undtagelse for midlertidig masseindsamling med henblik på målrettet indsamling og de resterende garantier, der skal anvendes, fortsat er uklar, navnlig med hensyn til, hvilke garantier i EO 14086 der finder anvendelse på hvilken fase (masseindsamling, yderligere målrettet indsamling), og opfordrer Kommissionen til yderligere at vurdere disse elementer og vurdere disse aspekter, også i praksis, i forbindelse med fremtidige fælles evalueringer.

162. Databeskyttelsesrådet beklager endvidere, at selv om begrebet "midlertidigt" har været lidt mere detaljeret i dekretet end i PPD-28, synes det efter Databeskyttelsesrådets opfattelse dog stadig at betyde, at så længe målet ikke er blevet identificeret, kan masseindsamlingen fortsætte. I denne forbindelse minder Databeskyttelsesrådet om nødvendigheden af at have klare og præcise regler, og det understreger her også den centrale garanti, som disse regler udgør for de registrerede.

163. Hvad angår de garantier, der gælder for masseindsamling, er Databeskyttelsesrådet sammenfattende fortsat bekymret over, at der til trods for yderligere garantier i henhold til EO 14086 stadig er mulighed for at masseindsamle data, dvs. uden forskelsbehandling, uden centrale garantier såsom forudgående tilladelse til at indsamle disse data — herunder i en undtagelsessituation med midlertidig teknisk masseindsamling — også under hensyntagen til behovet for yderligere præciseringer og de betænkeligheder, der er givet udtryk for med hensyn til streng formålsbegrænsning vedrørende efterfølgende adgang til data, klare og strenge regler for opbevaring af data og strengere garantier vedrørende formidling af masseindsamlede data, herunder i forbindelse med videreoverførsler.

164. Generelt understreger Databeskyttelsesrådet, at Menneskerettighedsdomstolens ovennævnte afgørelse endnu en gang viser betydningen af et omfattende tilsyn fra uafhængige tilsynsmyndigheders side. Databeskyttelsesrådet understreger, at uafhængigt tilsyn i alle faser af processen med statslig adgang af hensyn til den nationale sikkerhed er en vigtig garanti mod vilkårlige overvågningsforanstaltninger og dermed for vurderingen af et tilstrækkeligt 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. Dette gælder navnlig under omstændigheder, hvor den pågældende på grund af arten af den hemmelige overvågning er forhindret i at anmode om prøvelse eller i at deltage direkte i en eventuel klageprocedure forud for eller under gennemførelsen af overvågningsforanstaltningen.

165. Databeskyttelsesrådet minder om, at det er af den opfattelse, at vurderingen af tilstrækkeligheden afhænger af alle sagens omstændigheder, navnlig effektiviteten af efterfølgende tilsyn og domstolsprøvelse som fastsat i den retlige ramme.

3.2.2.4 Retlige rammer, der organiserer specifikke indsamlinger af hensyn til den nationale sikkerhed for elementerne i efterretningstjenesterne inden for og uden for USA's område

166. I sin dom i Schrems II-sagen understregede EU-Domstolen i forbindelse med Section 702 i FISA, at denne tekst "*på ingen måde lader fremgå, at der er begrænsninger af beføjelsen i medfør af denne bestemmelse til at gennemføre overvågningsprogrammer med henblik på at indhente udenlandske efterretningsoplysninger, og heller ikke, at der er garantier for ikke-amerikanske personer, som potentielt kan være omfattet af disse programmer*"[166]. Den foranledigede Domstolen til at fastslå, at "*[u]nder disse omstændigheder kan denne bestemmelse [...] ikke sikre et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er sikret ved chartret [...], og hvorefter et retsgrundlag, som tillader indgreb i de grundlæggende rettigheder, for at være i overensstemmelse med proportionalitetsprincippet selv skal definere rækkevidden af begrænsningen af udøvelsen af den pågældende rettighed og fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning, og som opstiller en række mindstekrav*"[167].

167. Med hensyn til EO 12333 bemærkede Domstolen, at dekretet "*heller ikke giver de registrerede rettigheder, som kan håndhæves over for de amerikanske myndigheder ved domstolene*"[168], og den konkluderede endvidere, at "*inden for rammerne af overvågningsprogrammer baseret på EO 12333 afgrænser adgangen til oplysninger i transit til USA — uden at denne adgang er underlagt noget retsligt tilsyn — dog under alle omstændigheder ikke tilstrækkeligt klart og præcist omfanget af en sådan masseindsamling af personoplysninger*"[169], efter en analyse af de betingelser, hvorunder masseindsamling kan finde sted i henhold til dette dekret, sammenholdt med PPD-28.

168. Med hensyn til disse specifikke dataindsamlingsordninger indeholder EO 14086 nu nye regler.

3.2.2.4.1 Indsamling af oplysninger til nationale sikkerhedsformål i henhold til Section 702

169. Databeskyttelsesrådet minder om, at konklusionerne vedrørende FISA 702[170] om, at "*ikkeamerikanske personer" i praksis også nyder godt af de begrænsninger for adgang og opbevaring, som de forskellige agenturers procedurer for minimering og/eller målretning kræver på grund af omkostningerne og vanskelighederne ved at identificere og fjerne oplysninger om amerikanske personer for en stor mængde data, hvilket betyder, at hele datasættet typisk håndteres i overensstemmelse med de højere amerikanske datastandarder*", blev hilst velkommen i PCLOB's seneste rapport.

170. Det fremgår af disse konstateringer, at "*programmet ikke fungerer ved masseindsamling af meddelelser*". ODNI's Statistical Transparency Reports for 2014 og 2021 bekræftede denne konklusion. Ifølge PCLOB's rapport anvendes "målrettede selektorer", f.eks. en e-mailadresse eller et telefonnummer, desuden til at målrette overvågningen.

171. Databeskyttelsesrådet minder dog også om, at det i forbindelse med afsnit 702 samtidig blev præciseret i forbindelse med den seneste gennemgang af privatlivsskjoldet, at en "person", der skal identificeres som et mål, kan henvise til flere personer, der anvender den samme identifikator, forudsat at alle disse personer er ikkeamerikanske personer og opfylder de gældende kriterier for målgruppen. Databeskyttelsesrådet minder også om, at under den tredje årlige fælles gennemgang af

[166] Se Domstolens dom i Schrems II-sagen, præmis 180.
[167] Se Domstolens dom i Schrems II-sagen, præmis 180.
[168] Se Domstolens dom i Schrems II-sagen, præmis 182.
[169] Se Domstolens dom i Schrems II-sagen, præmis 183.
[170] Se PCLOB's Report on the Surveillance program operated pursuant of Section 702 FISA, s. 100.

privatlivsskjoldet i 2019 blev der i forbindelse med UPSTREAM-programmet opfordret til at udelukke, at der forekommer massiv og vilkårlig adgang til ikkeamerikanske personers personoplysninger[171].

172. Databeskyttelsesrådet minder desuden om, at det forhold, at indsamlingen i henhold til FISA's Section 702 er begrundet i "*et væsentligt formål med indsamlingen er at indhente udenlandske efterretningsoplysninger*", stadig efterlader en vis usikkerhed med hensyn til dens formålsbegrænsning og nødvendighed. Databeskyttelsesrådet bemærker imidlertid, at i henhold til EO 14086, Section 2(a)(A) og (B), må signalefterretningsaktiviteter kun udføres, når det er fastslået, at aktiviteterne er nødvendige for at fremme en valideret prioritet, og kun i det omfang og på en måde, der står i et rimeligt forhold til en sådan prioritet, og at det skal være så skræddersyet som muligt at fremme den validerede prioritet under behørig hensyntagen til relevante faktorer såsom indsamlingens indgribende karakter, dataenes følsomhed, ikke uforholdsmæssigt stor indvirkning på privatlivets fred og borgerlige frihedsrettigheder. Databeskyttelsesrådet forventer dog yderligere præciseringer af, hvordan dette konkret vil blive gennemført og gjort operationelt, herunder i forbindelse med anvendelsen af FISA's Section 702.

173. I denne forbindelse opfordrede Databeskyttelsesrådet i mangel af direkte adgang til disse oplysninger i sig selv til en uafhængig vurdering af nødvendigheden og proportionaliteten af definitionen af "mål" og af begrebet "udenlandske efterretninger" i Section 702 i FISA (herunder i forbindelse med UPSTREAM-programmet) efter fornyelsen heraf. Databeskyttelsesrådet mener, at dets tidligere opfordring til yderligere uafhængig vurdering af processen for anvendelse af selektorer i specifikke tilfælde ("mål for selektorer") samt til yderligere præcisering i forbindelse med UPSTREAM-programmet er relevant. Under hensyntagen til den nye EO 14086 opfordrer Databeskyttelsesrådet derfor til yderligere oplysninger for også at vurdere og overvåge, hvordan og i hvilket omfang de nyligt indførte principper om nødvendighed og proportionalitet vil blive anvendt i praksis i denne forbindelse, og det forventer, at dette også vil blive vurderet i forbindelse med fremtidige fælles evalueringer.

174. Databeskyttelsesrådet glæder sig over, at det fuldt funktionsdygtige Privacy and Civil Liberties Oversight Board (PCLOB) som et uafhængigt tilsynsagentur har besluttet at gennemføre "et tilsynsprojekt for at undersøge det overvågningsprogram, som den udøvende afdeling opererer i henhold til Section 702 i Foreign Intelligence Surveillance Act (FISA), forud for udløbsdatoen i december 2023 for Section 702 og den kommende offentlige og kongresmæssige overvejelse af en fornyet godkendelse"[172]. Databeskyttelsesrådet glæder sig også over, at "gennemgangen omfatter udvalgte fokusområder, der skal efterforskes, herunder, men ikke nødvendigvis begrænset til, forespørgsler fra amerikanske personer om oplysninger indsamlet i henhold til Section 702 og UPSTREAM-indsamling i henhold til Section 702"[173], og at den "også omfatter en gennemgang af programmets tidligere og forventede værdi og effektivitet samt tilstrækkeligheden af de eksisterende garantier for privatlivets fred og borgerlige rettigheder"[174]. Databeskyttelsesrådet understreger derfor, at det vil være nødvendigt at få adgang til PCLOB's konklusioner i denne rapport om Section 702 for på passende og omfattende vis at kunne vurdere de garantier for privatlivets fred, der ydes og anvendes i forbindelse med dette overvågningsprogram.

---

[171] Se tredje fælles evalueringsrapport, s. 17, punkt 83.

[172] Se NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA).

[173] Se ovenfor.

[174] Se ovenfor.

175. Under hensyntagen til den nye EO 14086 opfordrer Databeskyttelsesrådet desuden til yderligere oplysninger for også at vurdere og overvåge, hvordan og i hvilket omfang de nyligt indførte principper om nødvendighed og proportionalitet samt andre garantier i denne tekst vil blive anvendt i praksis i denne forbindelse.

3.2.2.4.2 Indsamling af data til nationale sikkerhedsformål i henhold til Executive Order 12333

176. Som Domstolen anerkendte i sin dom i Schrems II-sagen, bør analysen af lovene i det tredjeland, for hvilket tilstrækkeligheden vurderes, ikke begrænses til den lovgivning og praksis, der giver mulighed for overvågning inden for det pågældende lands fysiske grænser, men den bør også omfatte en analyse af retsgrundlaget i det pågældende tredjelands lovgivning, som gør det muligt for landet at foretage overvågning uden for dets område for så vidt angår EU-data. De nødvendige begrænsninger for statslig adgang til data bør udvides til også at omfatte personoplysninger "i transit" til det land, for hvilket det er anerkendt, at de er tilstrækkelige.

177. Databeskyttelsesrådet glæder sig over PCLOB's generelle offentlige rapport om Executive Order 12333, som blev offentliggjort i april 2021, men bemærker, at denne rapport fortsat er generel, da de fleste resultater er klassificeret.

178. I denne forbindelse understreger Databeskyttelsesrådet endnu en gang i betragtning af usikkerheden og den manglende klarhed om, hvordan EO 12333 tidligere blev anvendt, og betydningen af at præcisere, hvordan den vil blive anvendt i lyset af den nye EO 14086, betydningen af PCLOB's ventede rapporter om denne tekst[175]. Databeskyttelsesrådet forstår imidlertid, at størstedelen af deres indhold sandsynligvis vil forblive klassificeret, således at ingen yderligere oplysninger om den konkrete drift af EO 12333 og om nødvendigheden og proportionaliteten heraf vil blive tilgængelige hverken for offentligheden eller for Databeskyttelsesrådet.

179. Databeskyttelsesrådet ser derfor især gerne, at PCLOB's rapport om anvendelsen af EO 14086 ikke klassificeres, men er fuldt tilgængelig, når den er afsluttet, herunder om de dele, der vil vurdere, hvordan EO 14086's garantier vil blive anvendt på indsamlingen af data i henhold til EO 12333. Databeskyttelsesrådet opfordrer også Kommissionen til at være særlig opmærksom på dette punkt i forbindelse med de fremtidige fælles evalueringer.

180. Med hensyn til de forskellige retlige instrumenter, der giver mulighed for at indsamle og yderligere få adgang til og behandle data for amerikanske efterretningstjenester inden for USA's retlige rammer, vil Databeskyttelsesrådet generelt hilse nærmere oplysninger om deres samspil med den nye EO 14086 velkommen, og det forventer forsikringer om, at de betænkeligheder, som Databeskyttelsesrådet har givet udtryk for i sine tidligere udtalelser, vil blive løst ved vedtagelsen af disse nye garantier.

181. Databeskyttelsesrådet opfordrer også Kommissionen til at være særlig opmærksom på disse aspekter i forbindelse med de fremtidige fælles evalueringer.

[175] Den generelle rapport om EO 12333 er for det meste klassificeret — kun en kort offentlig udgave er blevet offentliggjort, samt rapporten og anbefalingerne vedrørende CIA's terrorbekæmpelsesaktiviteter udført i henhold til EO 12333, og kun delvist afklassificeret.

3.2.2.4.3 PCLOB's rapport

182. Databeskyttelsesrådet glæder sig over, at EO 14086 også indeholder et krav om, at PCLOB skal udarbejde en rapport om gennemførelsen af dekretet. Databeskyttelsesrådet understreger, at denne rapport bør indeholde en vurdering af denne specifikke mulighed, som dekretet giver for at indsamle data til de formål, der er anført med henblik på målrettet indsamling samt masseindsamling, herunder af tekniske årsager, for bedre at forstå de centrale vilkår i EO 14086, samt hvordan de forstås og anvendes i praksis i de forskellige overvågningsprogrammer. Denne rapport vil også være nødvendig for at vurdere, hvordan dekretet vil blive gennemført i de interne procedurer og politikker i forbindelse med elementerne i efterretningstjenesterne.

3.2.3 Garanti C — Tilsyn

3.2.3.1 Indledning

183. USA's efterretningsaktiviteter er underlagt en tilsynsproces på flere niveauer. Tilsynsstrukturen i USA kan opdeles i internt og eksternt tilsyn. Alle elementer i efterretningstjenesterne har tilsyns- og compliancemedarbejdere, som regelmæssigt fører tilsyn med signalefterretningsaktiviteter, herunder Privacy and Civil Liberties Officers og generalinspektører. Desuden findes der eksterne tilsynsorganer såsom Privacy and Civil Liberties Oversight Board (PCLOB) og Intelligence Oversight Board.

184. Databeskyttelsesrådet minder om, at et indgreb finder sted på tidspunktet for indsamlingen af data, men også på det tidspunkt, hvor en offentlig myndighed får adgang til dataene med henblik på yderligere behandling. Menneskerettighedsdomstolen har flere gange præciseret, at ethvert indgreb i retten til privatlivets fred og databeskyttelse bør være underlagt et effektivt, uafhængigt og upartisk tilsynssystem, som enten en dommer eller et andet uafhængigt organ[176] (f.eks. en administrativ myndighed eller et parlamentarisk organ) stiller til rådighed.

185. Selv om Menneskerettighedsdomstolen har givet udtryk for, at den foretrækker, at en dommer er ansvarlig for at føre tilsyn, udelukkede den ikke, at et andet organ kan være ansvarligt, "*forudsat at myndigheden er tilstrækkelig uafhængig af den udøvende magt*"[177] og *"af de myndigheder, der foretager overvågningen, og at den har tilstrækkelige beføjelser og kompetencer til at udøve en effektiv og løbende kontrol*"[178].

186. Menneskerettighedsdomstolen tilføjede, at "*udnævnelsesmåden og den retlige status for medlemmerne af tilsynsorganet*"[179] skal tages i betragtning ved vurderingen af uafhængigheden.

187. Menneskerettighedsdomstolen præciserede endvidere, at den skal undersøge, om tilsynsorganets aktiviteter er offentligt tilgængelige. Dette kan f.eks. opnås, hvis tilsynsrapporterne til regeringen og de offentlige rapporter årligt præsenteres for parlamentet og drøftes af dette[180].

---

[176] Menneskerettighedsdomstolen, Klass m.fl. mod Tyskland, 6. september 1978 ("Menneskerettighedsdomstolens dom i Klass-sagen"), præmis 17 og 51.

[177] Menneskerettighedsdomstolens dom i Zakharov-sagen, præmis 258, Menneskerettighedsdomstolen, Iordachi m.fl. mod Moldova, 10. februar 2009, præmis 40 og 51, Menneskerettighedsdomstolen, Dumitru Popescu mod Rumænien, 26. april 2007, præmis 70-73.

[178] Menneskerettighedsdomstolens dom i Klass-sagen, præmis 56.

[179] Menneskerettighedsdomstolens dom i Zakharov-sagen, præmis 278.

[180] Menneskerettighedsdomstolens dom i Zakharov-sagen, præmis 283, Menneskerettighedsdomstolen, L. mod Norge, den 9. juni 1990, Menneskerettighedsdomstolen, Kennedy mod Det Forenede Kongerige, 18. maj 2010, præmis 166.

188. Det uafhængige tilsyn med gennemførelsen af overvågningsforanstaltninger blev også taget i betragtning i EU-Domstolens dom i Schrems II-sagen, idet "*FISC's kontrol således [tager] sigte på at efterprøve, om disse overvågningsprogrammer er i overensstemmelse med formålet om at indhente udenlandske efterretningsoplysninger, men den behandler ikke spørgsmålet, "[om, hvorvidt] fysiske personer […] er velegnede mål for indsamling af udenlandske efterretningsoplysninger*"[181].

3.2.3.2 Internt tilsyn

3.2.3.2.1 Generalinspektører

189. Databeskyttelsesrådet anerkender, at generalinspektørerne har fået overdraget en lang række tilladelser, der er nødvendige for at overvåge efterretningsaktiviteterne. Generalinspektørerne har navnlig adgang til alle de oplysninger, der er nødvendige for at vurdere, om agenturernes arbejde generelt er i overensstemmelse med lovgivningen, herunder, men ikke begrænset til, love vedrørende privatlivets fred og databeskyttelse, og de kan udstede pålæg (subpoenas) og modtage edsaflæggelse fra enhver person i forbindelse med undersøgelser af generalinspektørerne.

190. På grundlag af ovenstående mener Databeskyttelsesrådet, at generalinspektørerne generelt har omfattende undersøgelsesbeføjelser. De har imidlertid ingen bindende afhjælpende beføjelser og udsteder kun ikkebindende anbefalinger[182].

191. Databeskyttelsesrådet anerkender, at generalinspektørerne i princippet ikke må forhindres i eller forbydes at indlede, gennemføre og fuldføre evalueringer eller efterforskninger eller i at udstede pålæg under enhver evaluering eller efterforskning[183]. I denne forbindelse bemærker Databeskyttelsesrådet imidlertid, at generalinspektørerne er underlagt den respektive afdelingsleders myndighed, ledelse og kontrol, og at de kan forbyde dem at få adgang til oplysninger, efterforske og blandt andet udstede pålæg i tilfælde, hvor afdelingslederen fastslår, at et sådant forbud er nødvendigt for at beskytte nationale interesser. Afdelingschefen skal imidlertid underrette de ansvarlige udvalg i den amerikanske kongres om udøvelsen af denne beføjelse[184].

192. Databeskyttelsesrådet bemærker, at generalinspektørerne kun kan fjernes af den amerikanske præsident, som skal underrette Kongressen om årsagerne til en sådan fjernelse.

193. Databeskyttelsesrådet bemærker, at der ikke har været væsentlige ændringer af den interne tilsynsmekanisme siden udtalelserne fra Artikel 29-Gruppen og derefter Databeskyttelsesrådet. Databeskyttelsesrådet konkluderer derfor i overensstemmelse med Artikel 29-Gruppens udtalelse 01/2016[185], at der generelt er indført tilstrækkelige interne tilsynsmekanismer.

3.2.3.3 Eksternt tilsyn

194. Databeskyttelsesrådet bemærker, at ud over nedennævnte organer fører forskellige andre organer i den amerikanske regering tilsyn med de amerikanske efterretningsagenturers aktiviteter —

[181] Domstolens dom i Schrems II-sagen, præmis 179.
[182] Udkast til afgørelse, betragtning 105.
[183] Inspector General Act fra 1978, Section 3(a).
[184] Se f.eks. Inspector General Act fra 1978, Section 8 (for det amerikanske forsvarsministerium (Department of Defence), Section 8E (for justitsministeriet), Section 8G (d)(2)(A),(B) (for NSA), United States Code, afsnit 50, Section 403q(b) (for CIA), Intelligence Authorization Act For Fiscal Year 2010, Section 405(f) (for efterretningstjenesterne).
[185] Artikel 29-Gruppens udtalelse 01/2016.

eksempelvis Intelligence Oversight Board (IOB) eller kongressens udvalg. Sidstnævnte kan foretage deres egne undersøgelser og rapporter.

3.2.3.3.1 Privacy and Civil Liberties Oversight Board (PCLOB)

195. Databeskyttelsesrådet anerkender PCLOB's omfattende tilsynsrolle i forbindelse med den nye klagemekanisme og gennemførelsen af EO 14086.

196. For det første omfatter dets nye funktioner høring af den amerikanske justitsminister vedrørende udnævnelsen af dommerne ved DPRC og de særlige advokater. For det andet vil PCLOB gennemgå klageproceduren hvert år, dvs. klagemekanismens behandling af kvalificerede klager. Dette omfatter bl.a., om CLPO og DPRC har behandlet kvalificerede klager rettidigt, og om de opnår fuld adgang til nødvendige oplysninger og fungerer i overensstemmelse med EO 14086 samt efterretningstjenesternes overholdelse af de afgørelser, der er truffet af CLPO og DPRC.

197. Desuden skal PCLOB høres, mens efterretningsagenturerne ajourfører deres interne politikker og procedurer for at gennemføre EO 14086. Desuden vil PCLOB foretage en evaluering af de ajourførte politikker og procedurer og vurdere, om de er i overensstemmelse med EO 14086[186]. Selv om PCLOB's konklusioner ikke er bindende i snæver forstand, er lederen af hvert element i efterretningstjenesterne forpligtet til omhyggeligt at overveje og gennemføre eller på anden måde behandle alle anbefalinger i en sådan evaluering i overensstemmelse med gældende ret[187]. Databeskyttelsesrådet opfordrer Kommissionen til at være særlig opmærksom på, om og hvordan PCLOB's anbefalinger er blevet gennemført på agenturniveau i fremtidige evalueringer, hvis udkastet til afgørelse vedtages.

198. Databeskyttelsesrådet minder om, at PCLOB, da det er uafhængigt, "tilskyndes til" men ikke er forpligtet til at kontrollere, om de garantier, der er fastsat i EO 14086, tages behørigt i betragtning, og om efterretningstjenesterne fuldt ud opfylder kravene i forbindelse med klageproceduren. Det er imidlertid Databeskyttelsesrådets opfattelse, at PCLOB i sin supplerende forklaring til Databeskyttelsesrådet såvel som offentligt[188] har erklæret, at det vil påtage sig den rolle, der er fastsat i EO 14086.

199. Databeskyttelsesrådet glæder sig endvidere over, at resultaterne af PCLOB's rapporter efter planen skal offentliggøres. I betragtning af at de forskellige organer inden for klagemekanismen og efterretningstjenesterne i princippet har til opgave at gennemføre anbefalingerne i PCLOB's rapporter eller på anden måde tage hånd om dem, anerkender Databeskyttelsesrådet, at disse anbefalinger spiller en vigtig rolle med hensyn til beskyttelse af privatlivets fred.

200. Databeskyttelsesrådet bemærker, at PCLOB's adgang til oplysninger er begrænset, hvis den amerikanske præsident tillader, at afdelinger, agenturer eller enheder i USA's regering[189] gennemfører "skjulte handlinger"[190].

---

[186] EO 14086, Section 2(c)(iv) og Section 2(c)(v).
[187] EO 14086, Section 2(c)(v)(B).
[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.
[189] United States Code, afsnit 42, § 2000ee(g)(5), United States Code, afsnit 50, § 3093(a).
[190] I henhold til United States Code, afsnit 50, § 3093(e)(1) betyder udtrykket "skjult handling" en aktivitet eller aktiviteter, der udøves af USA's regering med henblik på at påvirke politiske, økonomiske eller militære forhold i udlandet, hvor det er hensigten, at den amerikanske regerings rolle ikke vil være synlig eller offentligt anerkendt, men det omfatter ikke 1) aktiviteter, hvis primære formål er at indhente efterretninger, traditionelle kontraspionageaktiviteter [...].

201. I forlængelse af sine tidligere udtalelser mener Databeskyttelsesrådet, at PCLOB er et uafhængigt organ, hvis anbefalinger har været et vigtigt bidrag til reformer i USA, og hvis rapporter har været en særlig nyttig kilde til at forstå, hvordan de forskellige overvågningsprogrammer fungerer, som et væsentligt element i tilsynsstrukturen.

202. Databeskyttelsesrådet beklagede imidlertid i sin tredje årlige fælles evaluering af det tidligere EU-USA-privatlivsskjold, at PCLOB kun gav Databeskyttelsesrådet de samme oplysninger som den brede offentlighed. Det var desuden beklageligt, at PCLOB ikke udsendte yderligere rapporter om PPD-28 for at følge op på sin første rapport med henblik på at fremlægge yderligere oplysninger om, hvordan garantierne i PPD-28 anvendes, samt en generel ajourført rapport om Section 702 i FISA.

203. Databeskyttelsesrådet glæder sig derfor over PCLOB's meddelelse til Databeskyttelsesrådet om, at en opfølgningsrapport om Section 702 i FISA kan forventes offentliggjort i den nærmeste fremtid. Databeskyttelsesrådet er desuden tilfreds med, at PCLOB har informeret om sit tilsagn om at tillade offentliggørelse af sine rapporter vedrørende EO 14086. Databeskyttelsesrådet minder imidlertid om, at videregivelse af uklassificerede rapporter er reguleret af amerikansk lovgivning og skal koordineres med efterretningstjenesternes agenturer og ikke kan besluttes af PCLOB på eget initiativ.

204. Hvis udkastet til afgørelse vedtages, minder Databeskyttelsesrådet derfor om, at Databeskyttelsesrådets sikkerhedsgodkendte eksperter i fremtidige evalueringer af databeskyttelsesrammen mellem EU og USA om nødvendigt bør kunne gennemgå yderligere dokumenter og drøfte yderligere klassificerede elementer for at sikre, at oplysningerne i rapporterne kan vurderes på passende vis, samtidig med at der tages hensyn til relevante nationale sikkerhedsinteresser og gældende beskyttelse af privatlivets fred.

205. Databeskyttelsesrådet glæder sig over PCLOB's uafhængighed og tilsyn med de nationale efterretningstjenester, som skal overholde PCLOB's anbefalinger eller på anden måde tage hånd om dem, hvilket vil blive anført i PCLOB's rapport til den amerikanske kongres.

206. Under hensyntagen til Den Europæiske Menneskerettighedsdomstols krav vedrørende offentlig kontrol[191] om, at rapporterne fra et tilsynsorgan skal forelægges for og drøftes af Parlamentet, finder Databeskyttelsesrådet det tilstrækkeligt, at PCLOB mindst hvert halve år forelægger sine rapporter for den amerikanske præsident og navnlig kongressens udvalg i Senatet og Repræsentanternes Hus[192], som er de parlamentariske organer i USA's parlament.

3.2.3.3.2 Foreign Intelligence Surveillance Court (FISC)

207. Foreign Intelligence Surveillance Court er ansvarlig for tilsynet med indsamlingen af personoplysninger i henhold til Section 702 i FISA[193], og FISC's afgørelser kan appelleres til Foreign Intelligence Surveillance Court of Review (FISCR).

208. FISC fører tilsyn med certificeringsprocessen for indsamling af udenlandske efterretningsoplysninger i henhold til Section 702 i FISA og tillader elektronisk overvågning, fysisk søgning og andre efterforskningsforanstaltninger til udenlandske efterretningsformål[194]. FISC godkender også

[191] Menneskerettighedsdomstolens dom i Zakharov-sagen, præmis 283, Menneskerettighedsdomstolen, L. mod Norge, 9. juni 1990, Menneskerettighedsdomstolen, Kennedy mod Det Forenede Kongerige, 18. maj 2010, præmis 166.
[192] United States Code, afsnit 42, § 2000ee(e).
[193] United States Code, afsnit 50, § 1881(a).
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court.

procedurerne for målretning, minimering og søgning i certifikaterne, som er juridisk bindende for amerikanske efterretningstjenester[195]. Hvis FISC konstaterer, at kravene ikke er opfyldt, kan FISC helt eller delvist afvise certificeringen og kræve, at procedurerne ændres.

209. Hvis der konstateres overtrædelser af målretningsprocedurerne, kan FISC pålægge den relevante efterretningstjeneste at træffe afhjælpende foranstaltninger[196]. Sådanne afhjælpende foranstaltninger spænder fra individuelle til strukturelle foranstaltninger, f.eks. fra afslutning af dataindsamling og sletning af ulovligt indsamlede data til en ændring i indsamlingspraksis, herunder med hensyn til retningslinjer for og uddannelse af personale.

210. Databeskyttelsesrådet anerkender, at det i EO 14086 fastsættes, at CLPO og DPRC skal indberette overtrædelser til Assistant Attorney General for National Security, som skal indberette disse overtrædelser til FISC[197].

211. Som EU-Domstolen bemærkede i sin Schrems II-afgørelse, tillader FISC ikke individuelle tilsynsforanstaltninger. I stedet tillader den overvågningsprogrammer[198]. Databeskyttelsesrådet fastholder derfor sin bekymring over, at FISC ikke sikrer et effektivt retligt tilsyn af målretningen mod ikkeamerikanske personer, hvilket ikke synes at være løst med den nye EO 14086.

212. Med hensyn til forudgående uafhængig tilladelse[199] til overvågning i henhold til Section 702 i FISA beklager Databeskyttelsesrådet — sådan som det forstår udkastet til afgørelse[200] og forklaringerne fra den amerikanske regering — at FISC ikke synes at være bundet af de yderligere garantier i EO 14086, når det certificerer programmer, der tillader målretning mod ikkeamerikanske personer. Databeskyttelsesrådet er af den opfattelse, at de yderligere garantier i dette dekret ikke desto mindre bør tages i betragtning i denne forbindelse. Databeskyttelsesrådet minder om, at rapporter fra PCLOB vil være særligt nyttige til at vurdere, hvordan garantierne i EO 14086 vil blive gennemført, og hvordan disse garantier anvendes, når data indsamles i henhold til Section 702 i FISA.

3.2.4 Garanti D — Fysiske personer skal have adgang til effektive retsmidler.

213. Databeskyttelsesrådet minder om, at fysiske personers effektive rettigheder, der kan håndhæves, er af grundlæggende betydning for at kunne fastslå et tilstrækkeligt databeskyttelsesniveau i et tredjeland. Registrerede skal have adgang til effektive retsmidler for at opfylde deres rettigheder, når de mener, at disse ikke respekteres eller ikke er blevet respekteret. EU-Domstolen forklarede i sine domme i Schrems I- og II-sagerne, at "en lovgivning, der ikke fastsætter nogen mulighed for retssubjektet til at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet, [opfylder] ikke det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som denne er sikret ved chartrets artikel 47"[201].

---

[195] United States Code, afsnit 50, § 1881a(i).
[196] United States Code, afsnit 50, § 1803(h).
[197] EO 14086, Section 3(c)(i)(D), EO 14086, Section 3(d)(i)(F).
[198] Domstolens dom i Schrems II-sagen, præmis 179.
[199] For så vidt angår masseindsamling af data under EO 12333, hvor FISC ikke er kompetent, er Databeskyttelsesrådet bekymret for, at der ikke er indført en procedure for forudgående godkendelse af masseindsamling af data (se også garanti B).
[200] Udkast til afgørelse, betragtning 165.
[201] Domstolens dom i Schrems I-sagen, præmis 95, Domstolens dom i Schrems II-sagen, præmis 187.

214. Det amerikanske system vedrørende retsmidler indeholder en vigtig begrænsning, der gør det meget vanskeligt at anlægge sag til prøvelse af den amerikanske regerings overvågningsforanstaltninger ved de almindelige domstole. I henhold til den amerikanske forfatning skal en person dokumentere sin søgsmålskompetence ("standing"), dvs. fastslå en "konkret, specifik og faktisk eller overhængende skade"[202]. I overvågningssager synes et sådant krav at blive ophævet på grund af manglende underretning af personer, der er genstand for overvågning, selv efter at disse foranstaltninger er ophørt.

215. I denne forbindelse glæder Databeskyttelsesrådet sig over, at EO 14086 indfører en særlig klagemekanisme til at håndtere og behandle klager fra ikkeamerikanske personer vedrørende amerikanske signalefterretningsaktiviteter. Under denne nye mekanisme finder kravet om søgsmålskompetence ikke anvendelse: I henhold til Section 4(k)(ii) i EO 14086 behøver ansøgeren ikke at påvise, at vedkommendes data faktisk har været genstand for amerikanske signalefterretninger. Registrerede kan således påberåbe sig de garantier, der er fastsat i EO 14086, herunder dem, der er fastsat i andre relevante love og bestemmelser som omhandlet i Section 4(d)(iii), i EO 14086[203]. I den forbindelse tilføjer den nye mekanisme en klagemulighed, som ellers ikke ville eksistere.

216. Den nye mekanisme består af to niveauer: På det første niveau kan fysiske personer indgive en klage til Civil Liberties Protection Officer (CLPO) hos Office of the Director of National Intelligence. På det andet niveau har fysiske personer mulighed for at appellere CLPO's afgørelse til et nyoprettet organ, den såkaldte Data Protection Review Court (DPRC). De følgende afsnit fokuserer primært på det andet trin i klagemekanismen. Databeskyttelsesrådet mener, at CLPO som fungerende regeringsembedsmand ikke har en tilstrækkelig grad af uafhængighed af den udøvende magt og derfor ikke i sig selv i tilstrækkelig grad kan opfylde de krav, der følger af chartrets artikel 47. Denne vurdering er blevet bekræftet af Kommissionen ved flere lejligheder.

3.2.4.1 Kan oprettelsen af DPRC på grundlag af et dekret i sig selv være tilstrækkelig

217. DPRC er ikke en almindelig domstol, der er oprettet af kongressen i henhold til artikel III i den amerikanske forfatning, men er baseret på et dekret (Executive Order) udstedt af den amerikanske præsident. Selv om Databeskyttelsesrådet er opmærksom på og generelt glæder sig over de underliggende overvejelser, nemlig at undgå kravet om at dokumentere søgsmålskompetence (se også punkt 215), rejser dette et grundlæggende spørgsmål: Kan en sådan klagemekanisme (overhovedet) opfylde kravene i chartrets artikel 47? I henhold til denne bestemmelse skal enhver, hvis rettigheder og friheder som sikret af EU-retten er blevet krænket, have adgang til effektive retsmidler for en domstol, der forudgående er oprettet ved lov.

218. Mens den engelske ordlyd af chartrets artikel 47 henviser til en "tribunal", foretrækker andre sprogversioner ordet "domstol"[204]. I Schrems II gentog Domstolen, at "retssubjekterne skal have mulighed for at gøre brug af retsmidler ved en uafhængig og upartisk domstol med henblik på at få adgang til personoplysninger, som vedrører de pågældende, eller til at få sådanne oplysninger berigtiget eller slettet"[205]. I forbindelse med vurderingen af, om databeskyttelsesniveauet er tilstrækkeligt, finder Domstolen imidlertid, at en effektiv retsbeskyttelse mod sådanne indgreb ikke kun kan sikres af en domstol, men også af et organ, der giver garantier, der i det væsentlige svarer til

[202] Clapper mod Amnesty International USA, 568 U.S. 398 (2013) II. s. 10.
[203] EO 14086, Section 5(h), giver udtrykkeligt registrerede ret til at indgive klager i overensstemmelse med klagemekanismen.
[204] F.eks. "Gericht" i den tyske udgave.
[205] Domstolens dom i Schrems II-sagen, præmis 194.

dem, der kræves i henhold til chartrets artikel 47[206]. På samme måde hedder det i EMRK, at "enhver, hvis rettigheder og friheder er blevet krænket, skal have adgang til effektive retsmidler for en national myndighed"[207], hvilket ifølge Menneskerettighedsdomstolens faste praksis ikke nødvendigvis behøver at være en judiciel myndighed[208]. De beføjelser og processuelle garantier, som en myndighed har, navnlig om den er uafhængig af den udøvende magt og sikrer en retfærdig rettergang, er derimod relevante for vurderingen af effektiviteten af det retsmiddel, der er indbragt for denne myndighed[209]. Det ser ud til, at ingen af de to domstole baserer deres vurdering på rent formelle kriterier, men anser de materielle garantier for afgørende.

219. I Schrems II-sagen har Domstolen lagt særlig vægt på effektiv klageadgang på området for adgang til personoplysninger vedrørende national sikkerhed. Databeskyttelsesrådet noterer sig, at Domstolen i den forbindelse imidlertid ikke drøftede elementet "forudgående oprettet ved lov" i chartrets artikel 47, selv om ombudsmandsmekanismen i privatlivsskjoldet heller ikke var baseret på amerikansk lovgivning. I stedet for at behandle dette spørgsmål vurderede Domstolen forskellige aspekter af sin tilstrækkelighedstest, såsom manglen på afhjælpende beføjelser. Schrems II-dommen indeholder således ingen retningslinjer for vurderingen af "forudgående oprettet ved lov" i henhold til chartrets artikel 47. Der er imidlertid andre afgørelser, hvori Domstolen har udtalt sig om dette spørgsmål. I overensstemmelse med Menneskerettighedsdomstolens faste retspraksis i denne henseende mindede Domstolen i sine sager C-487/19 og C-132/20 om, at årsagen til indførelsen af udtrykket "forudgående oprettet ved lov" er at forhindre, at organisationen af retssystemet i et demokratisk samfund overlades til den udøvende magts skøn, og at sørge for, at dette område reguleres af en lov, der er vedtaget af den lovgivende magt på en måde, som er i overensstemmelse med de regler, der danner rammen for udøvelsen af dens kompetence[210]. Som det fremgår af denne udtalelse, er retten til en domstol, der forudgående er oprettet ved lov, tæt forbundet med garantien for uafhængighed.

220. På denne baggrund konkluderer Databeskyttelsesrådet, at i forbindelse med vurderingen af beskyttelsesniveauets tilstrækkelighed er den specifikke klagemekanisme, der er oprettet i henhold til EO 14086, i modsætning til klageadgang ved artikel III-domstole ikke i sig selv utilstrækkelig. Analysen af beskyttelsesniveauet i denne henseende afhænger af, om de garantier, der er fastsat i EO 14086 og suppleret af AG Regulation, i tilstrækkelig grad sikrer DPRC's uafhængighed i forhold til de øvrige beføjelser.

221. Kommissionen bør løbende overvåge, om reglerne i EO 14086 og dens supplerende bestemmelser, navnlig dem, der har til formål at fremme DPRC's uafhængighed, gennemføres fuldt ud og fungerer effektivt i praksis. Desuden bør eventuelle ændringer af rammen nøje gennemgås med henblik på indvirkningen på Kommissionens vurdering i henhold til udkastet til afgørelse. I denne forbindelse bemærker Databeskyttelsesrådet, at ændringer af EO 14086 og AG Regulation kan udløse en vedtagelse af umiddelbart gældende gennemførelsesretsakter, der suspenderer, ophæver eller ændrer afgørelsen om tilstrækkeligheden af beskyttelsesniveauet[211].

---

[206] Se Domstolens dom i Schrems II-sagen, præmis 197.

[207] Artikel 13 i den europæiske menneskerettighedskonvention.

[208] Menneskerettighedsdomstolens dom i Klass-sagen, præmis 67, Menneskerettighedsdomstolens dom i Big Brother Watch-sagen, præmis 359.

[209] Menneskerettighedsdomstolens dom i Klass-sagen, præmis 67, Menneskerettighedsdomstolens dom i Big Brother Watch-sagen, præmis 359.

[210] Se Domstolen, C-487/19, dom af 6. oktober 2021, W.Ż, ECLI:EU:C:2021:798 og C-132/20, dom af 29, marts 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, præmis 129 og præmis 121.

[211] Udkast til afgørelse, betragtning 212.

3.2.4.2 Tilstrækkelig uafhængighed af den udøvende magt

222. I sin dom i Schrems II-sagen understregede Domstolen, at domstolenes eller organets uafhængighed skal sikres, navnlig i forhold til den udøvende magt, med alle nødvendige garantier, herunder med hensyn til betingelserne for nedlæggelse eller tilbagekaldelse af udpegningen. Mere specifikt har Domstolen kritiseret, at ombudsmanden blev udnævnt af og direkte rapporterer til den amerikanske udenrigsminister (Secretary of State). Ombudsmanden blev anset for at være en integrerende del af det amerikanske udenrigsministerium. Domstolen fandt også, at der ikke var nogen særlige garantier vedrørende nedlæggelse eller tilbagekaldelse af udpegningen af ombudsmanden, hvilket undergraver ombudsmandens uafhængighed af den udøvende magt.

223. Databeskyttelsesrådet anerkender, at bestemmelserne i EO 14086 og den supplerende AG Regulation ikke pålægger DPRC en indberetningspligt over for justitsministeren, som det ville være tilfældet i et underordnet forhold. DPRC er heller ikke underlagt justitsministerens "daglige tilsyn"[212]. Disse garantier er en betydelig forbedring i forhold til privatlivsskjoldet. DPRC er imidlertid oprettet inden for den udøvende magt, nemlig justitsministeriet. Navnlig af denne grund vil gennemførelsen og den effektive funktion af garantierne i praksis være afgørende for at afgøre, om DPRC — selv om den ikke er en integreret del af justitsministeriet — som en enhed, der ikke desto mindre er placeret i den udøvende magt, kan anses for at være tilstrækkeligt uafhængig i praksis. Databeskyttelsesrådet opfordrer Kommissionen til nøje at overvåge, om disse garantier afspejles fuldt ud i praksis. Desuden foreslår Databeskyttelsesrådet at præcisere udtrykket "dagligt tilsyn" med henblik på, at "dommere" i DPRC ikke er underlagt nogen form for tilsyn. Kommissionen har bekræftet, at "dagligt tilsyn" skal forstås i denne forstand.

224. I forlængelse af ovennævnte beskyttelsesforanstaltninger indeholder databeskyttelsesrammen mellem EU og USA visse garantier vedrørende udnævnelse og afskedigelse af DPRC's "dommere". Selv om de udnævnes af den amerikanske justitsminister, er deres udnævnelse baseret på de kriterier, der anvendes til at vurdere ansøgere til føderale dommerstillinger, og den indebærer en høring af PCLOB. Afskedigelse af "dommere" inden udløbet af deres embedsperiode eller fra en igangværende procedure er kun mulig under snævert definerede omstændigheder, der, som Databeskyttelsesrådet forstår, er modereret af de bestemmelser, der gælder for føderale dommere[213]. Anvendelsen af disse regler er endnu et skridt i retning af at styrke DPRC's uafhængige stilling, hvilket igen vil være afgørende at gennemføre i praksis. Det fremgår imidlertid ikke klart af udkastet til afgørelse, om og hvordan disse krav vil blive overholdt i USA. På grundlag af yderligere forklaringer fra Kommissionen og den amerikanske regering forstår Databeskyttelsesrådet, at PCLOB kan behandle ovennævnte bestemmelser i sin årlige evaluering af klageproceduren, og at ansvaret for at overvåge og sikre overholdelse af alle retlige krav fra generalinspektøren i justitsministeriet omfatter kravene i EO 14086 og forskrifterne om oprettelse af DPRC. Databeskyttelsesrådet opfordrer Kommissionen til at præcisere dette aspekt i udkastet til afgørelse. Når det er sagt, bør Kommissionen tage hensyn til disse garantier, når den overvåger den faktiske praksis for behandling af personoplysninger som vurderet i udkastet til afgørelse.

225. Udkastet til afgørelse behandler ikke spørgsmålet om, hvorvidt og i givet fald på hvilke betingelser den amerikanske præsident har beføjelse til at afskedige eller fjerne "dommere" fra DPRC. Det er Databeskyttelsesrådets opfattelse, at en sådan beføjelse ikke ville findes, som forklaret af Europa-

[212] AG Regulation, § 201.7(d).
[213] EO 14086, Section 3(d)(iv), AG Regulation § 201.7.

Kommissionen og bekræftet af repræsentanter for den amerikanske regering. Databeskyttelsesrådet foreslår at præcisere dette aspekt i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.

226. "Dommerne" i DPRC udnævnes for fire år med mulighed for forlængelse og må på tidspunktet for deres første udnævnelse ikke have været ansat i den udøvende magt i de foregående to år[214]. I deres embedsperiode som "dommere" i DPRC må de ikke have andre officielle pligter eller ansættelse i den amerikanske regering[215]. I modsætning til amerikanske føderale dommere kan de dog deltage i udenretslige aktiviteter, herunder forretningsaktiviteter, finansielle aktiviteter, almennyttige finansieringsaktiviteter, betroede aktiviteter og udøvelse af advokatvirksomhed, hvis sådanne aktiviteter ikke griber ind i en upartisk udførelse af deres opgaver eller DPRC's effektivitet eller uafhængighed[216]. Retsvæsenets uafhængighed følger ikke kun af fraværet af instrukser, men også af personlig uafhængighed. I denne forbindelse er faktorer som embedsperioden, muligheden for at blive genudnævnt og risikoen for interessekonflikter relevante. Den periode på fire år, der er fastsat i henholdsvis EO 14086 og AG Regulation, er f.eks. kortere end embedsperioden for dommere ved EU-Domstolen (seks år med mulighed for genudnævnelse) og Menneskerettighedsdomstolen (ni år uden mulighed for genudnævnelse), men giver som sådan ikke anledning til alvorlig bekymring. Databeskyttelsesrådet er ikke bekendt med nogen retspraksis, der pålægger en minimumsperiode i denne henseende[217]. Databeskyttelsesrådet anerkender også, at muligheden for at deltage i udenretslige aktiviteter er betinget af, at de ganske enkelt ikke fører til interessekonflikter, der bringer DPRC's forpligtelser i fare. Databeskyttelsesrådet forstår af den amerikanske regerings supplerende forklaringer, at disse krav også er underlagt PCLOB's og justitsministeriets generalinspektørs evaluering og overvågning (se punkt 226 ovenfor). Hvordan dette krav vil blive anvendt og demonstreret i praksis, bør også behandles som led i de fælles evalueringer.

227. I henhold til Section 3(d)(i)(B) i EO 14086 skal alle "dommere" i DPRC være sikkerhedsgodkendte for at kunne få adgang til klassificerede oplysninger, dvs. for at kunne udøve deres funktion med at træffe afgørelse i sager om statens sikkerhed[218]. Nogle europæiske love og bestemmelser om sikkerhedsgodkendelse fritager derimod dommere fra kravet om sikkerhedsgodkendelse, i det omfang de udfører retslige opgaver, idet en sådan detaljeret kontrol kan være i strid med retsvæsenets uafhængighed[219]. Det fremgår af den amerikanske regerings forklaringer, at selv om en kandidat til udnævnelse til dommer ved en amerikansk domstol underkastes en grundig undersøgelse, er en føderal dommer efter at være blevet udnævnt til føderal dommer ved en amerikansk domstol ikke forpligtet til at indhente en sikkerhedsgodkendelse for at få adgang til klassificerede dokumenter, der er relevante for sagen.

228. Efter Databeskyttelsesrådets opfattelse afslører ovennævnte omstændigheder delvist forskelle mellem en amerikansk føderal dommers stilling og status og en "dommer" i DPRC. De fastsatte garantier giver imidlertid ikke anledning til at betvivle DPRC's uafhængighed. Databeskyttelsesrådet opfordrer indtrængende Kommissionen til, hvis udkastet til afgørelse vedtages, at prioritere ovennævnte sikkerhedsforanstaltninger i forbindelse med den første fælles evaluering af databeskyttelsesrammen mellem EU og USA. Databeskyttelsesrådet forventer endvidere, at

[214] AG Regulation § 201.3(a).
[215] AG Regulation § 201.3(c).
[216] AG Regulation § 201.7(c).
[217] Se også, mutatis mutandis, Menneskerettighedsdomstolen (Store Afdeling), sagen Centrum För Rättvisa mod Sverige, 25. maj 2021, præmis 346.
[218] Se også AG Regulation § 201.11(b) og udkast til afgørelse, betragtning 177.
[219] F.eks. § 2(3) i den tyske lov om sikkerhedsgodkendelse.

Kommissionen følger op på sit tilsagn om at suspendere, ophæve eller ændre afgørelsen, hvis den vedtages, i fald den amerikanske regering vælger at begrænse de garantier, der er indeholdt i dekretet[220].

3.2.4.3 DPRC's beføjelser

3.2.4.3.1 Adgang til oplysninger

229. En effektiv retsbeskyttelse kræver, at en domstol har tilstrækkelige undersøgelsesbeføjelser til at prøve den anfægtede foranstaltning. I Kadi II-sagen fastslog Domstolen vedrørende chartrets artikel 47, at Den Europæiske Unions retsinstanser skal sikre, at en afgørelse træffes på et tilstrækkeligt solidt faktuelt grundlag[221]. Domstolen fastslår, at "det påhviler Unionens retsinstanser under denne undersøgelse i givet fald at anmode Unionens kompetente myndighed om at fremlægge de med henblik på en sådan undersøgelse relevante oplysninger eller beviser, uanset om de er fortrolige"[222], hvorved "oplysningernes eller bevisernes hemmelige eller fortrolige karakter ikke kan gøres gældende"[223].

230. I henhold til betragtning 181 i udkastet til afgørelse gennemgår DPRC CLPO's afgørelser, der som minimum er baseret på referatet af CLPO's undersøgelse, samt alle oplysninger og indlæg fra klageren, den særlige advokat eller en efterretningstjeneste. I udkastet til afgørelse hedder det endvidere, at DPRC har adgang til alle nødvendige oplysninger, som den kan indhente gennem CLPO. Dette er baseret på bestemmelsen i § 201.9, litra b), i AG Regulation, som bemyndiger DPRC til at "anmode om, at ODNI CLPO supplerer fortegnelsen med specifikke forklarende eller tydeliggjorte oplysninger, og at ODNI CLPO træffer yderligere faktuelle konklusioner, hvor det er nødvendigt, for at DPRC-panelet kan foretage sin evaluering". Det er Databeskyttelsesrådets opfattelse, at DPRC's vurdering derfor ikke på nogen måde er begrænset til CLPO's konklusioner på det første niveau af den nye klagemekanisme. Tværtimod kan DPRC anmode om både yderligere juridiske oplysninger og, hvad der er vigtigt, yderligere faktuelle omstændigheder med henblik på sin analyse af, om en omfattet overtrædelse har fundet sted. Samtidig bemærker Databeskyttelsesrådet også, at disse generelt omfattende undersøgelsesbeføjelser ikke omfatter direkte adgang til data, der opbevares om personen. Kommissionen har forklaret, at CLPO altid vil fungere som formidler, når DPRC har brug for yderligere oplysninger. DPRC's adgang til de oplysninger, der er nødvendige for selvstændigt at træffe afgørelse om en anmodning om evaluering, hviler derfor i et vist omfang på CLPO's fremlæggelse af de nødvendige oplysninger. Databeskyttelsesrådet anerkender, at CLPO har en forpligtelse til at "yde den nødvendige støtte" til DPRC, og efterretningstjenesterne er forpligtet til at give CLPO adgang til de oplysninger, der er nødvendige for at foretage DPRC's evaluering[224]. Databeskyttelsesrådet bemærker imidlertid også, at CLPO ikke selv er uafhængig og foretager den indledende undersøgelse af en klage i første fase af klageproceduren. Databeskyttelsesrådet glæder sig derfor over, at PCLOB i forbindelse med sin årlige evaluering af klagemekanismen vil kontrollere, om DPRC har fået fuld adgang til alle nødvendige oplysninger[225]. Databeskyttelsesrådet opfordrer desuden Kommissionen til at medtage

[220] Udkast til afgørelse, betragtning 212.
[221] CJEU, forenede sager C-584/10 P, C-593/10 P og C-595/10 P, Europa-Kommissionen m.fl. mod Yassin Abdullah Kadi, dom af 18. juli 2013 ("Domstolens dom i Kadi II-sagen"), præmis 119.
[222] Domstolens dom i Kadi II-sagen, præmis 120.
[223] Domstolens dom i Kadi II-sagen, præmis 125.
[224] EO 14086, Section 3(c)(i)(H) og Section 3(d)(iii).
[225] EO 14086, Section 3(e)(i).

dette aspekt i de fælles evalueringer, hvis udkastet til afgørelse vedtages, for at undersøge konsekvenserne af dette system i praksis.

3.2.4.3.2 Afhjælpende beføjelser

231. En af de centrale mangler ved privatlivsskjoldet, som førte til Domstolens ugyldiggørelse af det i Schrems II-sagen, var manglen på bindende afhjælpende beføjelser for ombudsmanden. Domstolen fandt, at "der er ingen oplysninger om, at ombudsmanden har beføjelse til at træffe bindende afgørelser i forhold til disse tjenester"[226]. Det blotte (politiske) tilsagn fra den amerikanske regering om, at efterretningstjenesterne ville rette op på enhver overtrædelse af de gældende regler, som ombudsmanden havde konstateret, var ikke tilstrækkeligt til at sikre et beskyttelsesniveau, der i det væsentlige svarer til det, der er sikret ved chartrets artikel 47.

232. I henhold til den nye klagemekanisme har de afgørelser, der træffes af CLPO og DPRC, derimod bindende virkning[227]. Databeskyttelsesrådet anerkender på den ene side, at denne myndighed ikke er begrænset til specifikke foranstaltninger, men tillader "passende afhjælpning" for "fuldt ud at afhjælpe" en konstateret overtrædelse. Navnlig nævnes det udtrykkeligt i Section 4(a) i EO 14086, at ulovligt indsamlede data slettes. På den anden side bemærker Databeskyttelsesrådet, at ordlyden af Section 4(a), i EO 14086 skaber en vis usikkerhed med hensyn til processen med at fastlægge en sådan "passende afhjælpning". Selv om en foranstaltning bør udformes med henblik på fuldt ud at afhjælpe en overtrædelse, bør det også overvejes, hvordan "en overtrædelse af den art, der er konstateret, sædvanligvis er blevet håndteret"[228]. Betydningen og virkningen af et sådant krav er uklar. Databeskyttelsesrådet opfordrer derfor Kommissionen til nøje at overvåge de afhjælpende foranstaltninger, der vedtages i praksis.

3.2.4.4 Indgivelse af en klage i henhold til den nye klagemekanisme

233. Den klagemekanisme, der er oprettet i henhold til EO 14086, finder kun anvendelse på kvalificerede klager indgivet af den relevante offentlige myndighed i en kvalificeret stat vedrørende amerikanske signalefterretningsaktiviteter i forbindelse med enhver omfattet overtrædelse[229]. For at kunne nyde godt af denne retsbeskyttelse skal flere betingelser derfor være opfyldt.

3.2.4.4.1 Betegnelse som kvalificeret stat

234. For det første skal det land eller den regionale organisation for økonomisk integration, hvorfra oplysningerne blev overført til USA, være blevet udpeget som en kvalificeret stat forud for den dataoverførsel, der ligger til grund for klagen[230]. Det er klart afgørende, at den tilgængelige klagemekanisme er til rådighed, når afgørelsen om tilstrækkeligheden af beskyttelsesniveauet træder i kraft. Derfor fastsættes det i betragtning 196 i udkastet til afgørelse, at afgørelsens ikrafttræden bl.a. er betinget af, at Unionen udpeges som en godkendt organisation/et godkendt organ med henblik på klagemekanismen. Kommissionen synes faktisk at antage, at udpegelsen vil finde sted forud for vedtagelsen af afgørelsen, da udkastet allerede omfatter en pladsholder til den amerikanske

[226] Domstolens dom i Schrems II-sagen, præmis 196.
[227] EO 14086, henholdsvis Section 3(c)(ii) og Section 3(d)(ii).
[228] EO 14086, Section 4(a).
[229] EO 14086, Section 3(a).
[230] EO 14086, Section 4(d)(i) og 4(k)(i).

justitsministers udpegelse af EU[231] (i stedet for at medtage udpegelsen som en betingelse i den dispositive del af udkastet til afgørelse).

3.2.4.4.2 Krænkelse af privatlivets fred og borgernes interesser og "søgsmålskompetence"

235. En "kvalificeret klage" skal være baseret på en påstået "omfattet overtrædelse", hvilket igen kræver en overtrædelse, der krænker klagerens individuelle privatliv og borgerlige interesser[232]. Det er Databeskyttelsesrådets opfattelse, baseret på yderligere forklaringer fra Kommissionen, at "krænkelse" ikke indebærer nogen form for begrænsning af antageligheden af en klage. Som Kommissionen har anført, vil en sådan krænkelse snarere vedrøre enhver klage vedrørende behandling af personoplysninger i forbindelse med signalefterretningsaktiviteter i strid med de bestemmelser, der er omhandlet i Section 4(d)(iii), f.eks. garantierne i EO 14086. Databeskyttelsesrådet beklager, at dette ikke er specificeret i teksten til udkastet til afgørelse, og opfordrer Kommissionen til yderligere at præcisere begrebet "krænkelse" for at sikre, at enhver krænkelse af de registreredes rettigheder vurderes og afhjælpes, og at der ikke er noget niveau af "alvor", der skal påvises for at få adgang til klage og passende afhjælpning.

236. Som allerede nævnt kræver en klage i henhold til EO 14086 ikke, at ansøgeren påviser sin søgsmålskompetence (jf. punkt 215)[233]. Databeskyttelsesrådet glæder sig over præciseringen i Section 4(k) i EO 14086 om, at der vil blive anvendt en "antagelsestest", og at det ikke er nødvendigt at påvise, at klagerens data faktisk er blevet tilgået gennem signalefterretningsaktiviteter. Indførelsen af klagemekanismen er et vigtigt skridt, da kravet om søgsmålskompetence gør det meget vanskeligt at anfægte overvågningsforanstaltninger ved de almindelige domstole i USA.

237. På grundlag af ovenstående overvejer Databeskyttelsesrådet ikke at anvende de almindelige domstole, som udkastet til afgørelse også henviser til[234], for at sikre et tilstrækkeligt beskyttelsesniveau[235]. I denne forbindelse minder Databeskyttelsesrådet om de bekymringer, som det allerede har givet udtryk for mange gange i forbindelse med kravet om søgsmålskompetence ved de almindelige domstole[236]. På grundlag af yderligere udtalelser fra den amerikanske regering er det desuden Databeskyttelsesrådets opfattelse, at selv om EO 14086 ikke er til hinder for at anlægge sag ved domstolene med generel kompetence, er det usikkert, hvordan en sådan domstol vil anvende dette dekret. Dette spørgsmål kan undersøges nærmere i forbindelse med fremtidige evalueringer, hvis udkastet til afgørelse vedtages.

3.2.4.4.3 Klageproceduren

238. Databeskyttelsesrådet støtter i princippet proceduren for videresendelse af en klage gennem medlemsstaternes tilsynsmyndigheder og mener fortsat, at identifikationen af klageren bør finde sted på EU's område. I lighed med ombudsmandsmekanismen i privatlivsskjoldet fastsætter udkastet til afgørelse imidlertid, at en registreret, der ønsker at indgive en sådan klage, skal indgive den til en tilsynsmyndighed i en EU-medlemsstat, der er kompetent til at føre tilsyn med nationale sikkerhedstjenester og/eller offentlige myndigheders behandling af personoplysninger[237]. I denne

[231] Udkast til afgørelse, fodnote 320.
[232] EO 14086, Section 4(k)(i) og 4(d)(ii).
[233] Clapper mod Amnesty International USA, 568 U.S. 398 (2013) II. s. 10.
[234] Udkast til afgørelse, betragtning 187 ff.
[235] Se også Domstolens dom i Schrems II-sagen, præmis 191 og 192.
[236] Se Artikel 29-Gruppens udtalelse 01/2016, s. 43.
[237] Udkast til afgørelse, betragtning 169.

forbindelse minder Databeskyttelsesrådet om de betænkeligheder, som det allerede gav udtryk for i udtalelsen fra Artikel 29-Gruppen om privatlivsskjoldet, f.eks. potentielle vanskeligheder for fysiske personer med at identificere den kompetente myndighed i betragtning af de mange forskellige tilsynsmekanismer i de nationale sikkerhedstjenester i medlemsstaterne[238]. Under hensyntagen til de nationale databeskyttelsesmyndigheders inddragelse i anvendelsen af og tilsynet med databeskyttelsesrammen mellem EU og USA er det mere hensigtsmæssigt at kanalisere klager gennem dem.

3.2.4.5 DPRC's afgørelse

239. Når gennemgangen af klagerens ansøgning er afsluttet, må DPRC ikke afsløre, om klageren var omfattet af amerikanske signalefterretningsaktiviteter. I stedet underrettes klageren om, at "gennemgangen enten ikke afdækkede nogen omfattede overtrædelser, eller Data Protection Review Court traf en afgørelse, der krævede passende afhjælpning"[239]. Dette standardsvar tjener det generelt legitime formål at beskytte følsomme oplysninger om amerikanske efterretningsaktiviteter. Databeskyttelsesrådet er imidlertid bekymret over, at EO 14086 ikke giver mulighed for undtagelser fra standardsvaret fra DPRC.

240. I Kadi II-sagen skulle Domstolen tage stilling til de modstridende interesser i statshemmeligheder på den ene side og retfærdige og så vidt muligt kontradiktoriske procedurer på den anden side. Domstolen fastslog, at det under omstændigheder, hvor bydende nationale sikkerhedsmæssige hensyn er til hinder for, at visse oplysninger eller visse beviser meddeles den berørte person, ikke desto mindre påhviler retsinstanserne under domstolsprøvelsen at anvende fremgangsmåder, der tager hensyn til berettigede sikkerhedsmæssige hensyn for så vidt angår karakteren af og kilderne til oplysningerne og hensynet til, at den retsundergivne i tilstrækkeligt omfang sikres respekten for sine processuelle rettigheder, såsom retten til at blive hørt og kontradiktionsprincippet[240]. Domstolen præciserede endvidere, at det tilkommer retsinstanserne, når de foretager en prøvelse af alle de faktiske og retlige omstændigheder, som Unionens kompetente myndighed har fremlagt, at vurdere, om de af myndigheden påberåbte grunde rettelig er til hinder for en sådan meddelelse[241]. Viser det sig, at de af Unionens kompetente myndighed anførte grunde faktisk er til hinder for, at den berørte person meddeles oplysninger eller beviser, skal der foretages en passende afvejning mellem de krav, der følger af retten til en effektiv domstolsbeskyttelse, og de krav, der er forbundet med national sikkerhed[242]. Med henblik på en sådan afvejning er det tilladt at gøre brug af muligheder såsom at meddele et sammendrag af indholdet af de omhandlede oplysninger eller beviser[243]. Selv om rettens konstateringer ikke stiller krav til den afgørelse, der træffes af en domstol, men snarere vedrører den kompetente myndigheds afgørelse og afviklingen af retssager, giver de et fingerpeg om afvejningen af ovennævnte interesser i forbindelse med retten til effektiv retsbeskyttelse. For yderligere vejledning kan der også henvises til Big Brother Watch-sagen, hvori Menneskerettighedsdomstolen, der henviste til en retfærdig rettergang og navnlig til princippet om en kontradiktorisk procedure, fastslog, at afgørelser truffet af et judicielt eller på anden måde uafhængigt organ skal begrundes[244].

---

[238] Artikel 29-Gruppens udtalelse 01/2016, s. 48 og 49.
[239] EO 14086, Section 3(d)(i)(H). I EO 14086 fastsættes dette svar også for CLPO.
[240] Domstolens dom i Kadi II-sagen, præmis 125.
[241] Domstolens dom i Kadi II-sagen, præmis 126.
[242] Domstolens dom i Kadi II-sagen, præmis 128.
[243] Domstolens dom i Kadi II-sagen, præmis 129.
[244] Menneskerettighedsdomstolens dom i Big Brother Watch-sagen, præmis 359.

241. Databeskyttelsesrådet anerkender, at DPRC's afgørelser er begrundede. DPRC er udtrykkeligt forpligtet til at udstede en skriftlig afgørelse med angivelse af sine konstateringer og angivelse af eventuelle passende afhjælpende foranstaltninger[245]. Databeskyttelsesrådet bemærker desuden, at den pågældende vil blive underrettet, hvis oplysningerne i forbindelse med en prøvelse ved DPRC er blevet afklassificeret[246]. Databeskyttelsesrådet anerkender også den rolle, som de særlige advokater, der er fastsat i den nye klagemekanisme, spiller, og som omfatter at slå til lyd for klagerens interesse i sagen[247]. I lyset af ovennævnte konsekvenser af Domstolens og Den Europæiske Menneskerettighedsdomstols retspraksis og i betragtning af, at DPRC's afgørelse ikke kan appelleres, men er endelig[248], er Databeskyttelsesrådet imidlertid betænkelig ved den generelle anvendelse af DPRC's standardsvar. Databeskyttelsesrådet minder om, at PCLOB uafhængigt vil evaluere, hvordan den nye klagemekanisme fungerer, og opfordrer Kommissionen til at være særlig opmærksom på dette spørgsmål, herunder PCLOB's vurdering af dette aspekt, i forbindelse med fremtidige revisioner af afgørelsen, hvis den vedtages.

4 GENNEMFØRELSE OG OVERVÅGNING AF UDKASTET TIL AFGØRELSE

242. Med hensyn til overvågningen og evalueringen af udkastet til afgørelse bemærker Databeskyttelsesrådet Domstolens retspraksis, idet "[h]enset til den omstændighed, at det beskyttelsesniveau, som et tredjeland sikrer, kan ændre sig, påhviler det endvidere Kommissionen efter vedtagelse af en afgørelse i henhold til [artikel 45 i GDPR] at undersøge med regelmæssige mellemrum, om konstateringen vedrørende det tilstrækkelige beskyttelsesniveau, som er sikret i det pågældende tredjeland, stadig er faktisk og retligt begrundet. En sådan undersøgelse skal under alle omstændighed foretages, når oplysninger bevirker, at der opstår tvivl i denne henseende."[249]

243. Databeskyttelsesrådet bemærker desuden, at det i skrivelsen fra handelsministeriet fastsættes, at handelsministeriet og andre amerikanske agenturer, alt efter hvad der er relevant, vil afholde regelmæssige møder med Kommissionen, interesserede EU-databeskyttelsesmyndigheder og relevante repræsentanter for Databeskyttelsesrådet[250].

244. Databeskyttelsesrådet mener, at den statslige beskyttelse i forbindelse med retshåndhævende myndigheders adgang, undtagelsen for midlertidig masseindsamling med henblik på USA's nationale sikkerhedsmyndigheders målrettede indsamling, anvendelsen i praksis af de nyligt indførte principper om nødvendighed og proportionalitet, herunder i forbindelse med UPSTREAM-programmet, samspillet mellem EO 14086 og de forskellige amerikanske retlige instrumenter, der gør det muligt for amerikanske efterretningstjenester at indsamle og yderligere behandle personoplysninger, gennemførende interne politikker og procedurer, hvordan der også vil blive taget hensyn til disse garantier i forbindelse med det tilsyn, som FISC fører, og hvordan klagemekanismen vil fungere effektivt, og spørgsmålet om videreoverførsler, automatiske afgørelser, materielt og effektivt tilsyn med og håndhævelse af DPF-principperne samt effektiv klageadgang vil kræve særlig opmærksomhed i løbet af de næste periodiske evalueringer.

[245] AG Regulation, § 201.9(g).
[246] EO 14086, Section 3(d)(v).
[247] AG Regulation, § 201.8(g).
[248] AG Regulation, § 201.9(g).
[249] Domstolens dom i Schrems I-sagen, præmis 76. Se også udkast til afgørelse, artikel 3, stk. 4.
[250] Udkast til afgørelse, bilag III.

245. Databeskyttelsesrådet bemærker, at evalueringen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet vil finde sted et år efter datoen for meddelelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet til medlemsstaterne og efterfølgende mindst hvert fjerde år[251]. Med henblik på yderligere at styrke den løbende overvågning af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet opfordrer Databeskyttelsesrådet Kommissionen til at foretage de efterfølgende evalueringer mindst hvert tredje år.

246. Med hensyn til den praktiske inddragelse af Databeskyttelsesrådet og dets repræsentanter i forberedelsen og gennemførelsen af fremtidige periodiske evalueringer gentager Databeskyttelsesrådet, at al relevant dokumentation bør deles skriftligt med Databeskyttelsesrådet, herunder korrespondance, i tilstrækkelig god tid inden evalueringerne. Som det var tilfældet med de gennemgange, der foretages under privatlivsskjoldet, anbefaler Databeskyttelsesrådet, at de nærmere bestemmelser for evalueringen fastsættes og aftales mellem Kommissionen, den amerikanske regering og Databeskyttelsesrådet senest tre måneder før evalueringen.

247. Databeskyttelsesrådet noterer sig endvidere og glæder sig over, at betragtning 212 i udkastet til afgørelse indeholder eksempler på ændringer, der underminerer det beskyttelsesniveau, som kan begrunde indledningen af en "nødophævelsesprocedure", der fokuserer på ændringer, som kan forekomme i forbindelse med Executive Order 14086 og den relaterede AG Regulation.

På Det Europæiske Databeskyttelsesråds vegne

Formand

(Andrea Jelinek)

[251] Udkast til afgørelse, artikel 3, stk. 4.