

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2023/1795**af 10. juli 2023****i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om et tilstrækkeligt beskyttelsesniveau for personoplysninger inden for EU-USA-databeskyttelsesrammen***(meddelt under nummer C(2023)4745)***(EØS-relevant tekst)**

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

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

ud fra følgende betragtninger:

1. INDLEDNING

- (1) I forordning (EU) 2016/679 ⁽²⁾ fastsættes reglerne for overførsel af personoplysninger fra en dataansvarlig eller databehandler i Unionen til tredjelande og internationale organisationer, i det omfang overførslen falder inden for forordningens anvendelsesområde. Reglerne for internationale dataoverførsler er fastsat i forordningens kapitel V. Strømmen af personoplysninger til og fra lande uden for EU er af afgørende betydning for udbygningen af den grænseoverskridende samhandel og det internationale samarbejde, men det beskyttelsesniveau, som personoplysninger sikres i Unionen, må ikke undermineres af overførsler til tredjelande eller internationale organisationer ⁽³⁾.
- (2) I henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 kan Kommissionen ved hjælp af en gennemførelsesretsakt fastslå, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. I så fald kan personoplysninger overføres til et tredjeland uden yderligere godkendelse, som fastsat i artikel 45, stk. 1, og betragtning 103 til forordning (EU) 2016/679.
- (3) Som omhandlet i artikel 45, stk. 2, i forordning (EU) 2016/679 skal vedtagelsen af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet finde sted på grundlag af en omfattende analyse af det pågældende tredjelandets retsorden, både hvad angår de regler, der finder anvendelse på dataimportøren, og de begrænsninger og garantier, der gælder med hensyn til offentlige myndigheders adgang til personoplysninger. Kommissionen skal i sin vurdering fastslå, om det pågældende tredjeland sikrer et beskyttelsesniveau, som »i det væsentlige svarer« til det, der sikres i Unionen (betragtning 104 til forordning (EU) 2016/679). Om det er tilfældet, skal vurderes ud fra EU-lovgivningen, navnlig forordning (EU) 2016/679, samt Den Europæiske Unions Domstols (Domstolen) praksis ⁽⁴⁾.

⁽¹⁾ EUT L 119 af 4.5.2016, s. 1.⁽²⁾ Af hensyn til overskueligheden findes der i bilag VIII en liste over forkortelser, der anvendes i denne afgørelse.⁽³⁾ Jf. betragtning 101 til forordning (EU) 2016/679.⁽⁴⁾ Jf. senest sag C-311/18, Facebook Ireland og Schrems (*Schrems II*) ECLI:EU:C:2020:559.

- (4) Som Domstolen fastslog i sin dom af 6. oktober 2015 i sag C-362/14, Maximilian Schrems mod Data Protection Commissioner ⁽⁹⁾ (*Schrems*), indebærer dette ikke, at der skal findes et identisk beskyttelsesniveau. Navnlig kan de midler, som det pågældende tredjeland anvender til at beskytte personoplysninger, være forskellige fra de midler, som gennemføres inden for Unionen, så længe de i praksis viser sig at være effektive med henblik på at sikre et tilstrækkeligt beskyttelsesniveau ⁽¹⁰⁾. Standarden for tilstrækkelighed er derfor ikke, at EU-reglerne duplikeres afsnit for afsnit. Testen består nærmere i, om det udenlandske system som helhed sikrer det krævede beskyttelsesniveau gennem kerneindholdet i retten til privatlivets fred og den effektive gennemførelse, overvågning og håndhævelse heraf ⁽¹¹⁾. I henhold til denne dom bør Kommissionen desuden ved anvendelsen af denne standard navnlig vurdere, om det pågældende tredjelands retlige ramme indeholder regler, hvorved det tilsigtes at begrænse indgreb i de grundlæggende rettigheder hos de personer, hvis oplysninger bliver videregivet fra Unionen, hvilke indgreb de statslige enheder i dette land er beføjede til at foretage, når der herved forfølges legitime mål, såsom statens sikkerhed, og yder effektiv domstolsbeskyttelse mod indgreb af denne art ⁽¹²⁾. Det Europæiske Databeskyttelsesråds reference vedrørende et tilstrækkeligt beskyttelsesniveau (Adequacy Referential), der skal præcisere denne standard yderligere, giver også vejledning i denne henseende ⁽¹³⁾.
- (5) Den gældende standard med hensyn til et sådant indgreb i de grundlæggende rettigheder til privatlivets fred og databeskyttelse blev yderligere præciseret af Domstolen i dom af 16. juli 2020 i sag C-311/18, Data Protection Commissioner mod Facebook Ireland Limited og Maximilian Schrems (*Schrems II*), som ugyldiggjorde Kommissionens gennemførelsesafgørelse (EU) 2016/1250 ⁽¹⁴⁾ om en tidligere transatlantisk ramme for datastrømme, EU's og USA's værn om privatlivets fred (privatlivsskjoldet). Domstolen fandt, at de begrænsninger af beskyttelsen af personoplysninger, som følger af USA's nationale lovgivning om de amerikanske offentlige myndigheders adgang til og brug af sådanne oplysninger, der overføres fra Unionen til USA af hensyn til den nationale sikkerhed, ikke var afgrænset på en sådan måde, at de lever op til krav, som i det væsentlige svarer til dem, der er foreskrevet i EU-retten, hvad angår nødvendigheden og proportionaliteten af sådanne indgreb i retten til databeskyttelse ⁽¹⁵⁾. Domstolen fandt ligeledes, at der ikke var tilvejebragt et retsmiddel for et organ, som giver personer, hvis oplysninger overføres til USA, garantier, der i det væsentlige svarer til dem, der kræves i henhold til chartrets artikel 47 om adgang til effektive retsmidler ⁽¹⁶⁾.
- (6) Efter *Schrems II*-dommen indledte Kommissionen drøftelser med den amerikanske regering med henblik på en eventuel ny afgørelse om tilstrækkeligheden af beskyttelsesniveauet, som ville opfylde kravene i artikel 45, stk. 2, i forordning (EU) 2016/679 som fortolket af Domstolen. Som et resultat af disse drøftelser vedtog USA den 7. oktober 2022 det præsidentielle dekret om fremme af garantier i de amerikanske signalefterrettningsaktiviteter (Executive Order 14086 »Enhancing Safeguards for US Signals Intelligence Activities« (EO 14086)), som suppleres af en forordning om Data Protection Review Court udstedt af den amerikanske justitsminister (Attorney General) (justitsministerens forordning) ⁽¹⁷⁾. Desuden er den ramme, der finder anvendelse på kommercielle enheder, som behandler oplysninger overført fra Unionen i henhold til denne afgørelse – »EU-USA-databeskyttelsesrammen« – blevet ajourført.
- (7) Kommissionen har nøje analyseret amerikansk lovgivning og praksis, herunder EO 14086 og justitsministerens forordning. På grundlag af konklusionerne i betragtning 9-200 konkluderer Kommissionen, at USA sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der i henhold til EU-USA-databeskyttelsesrammen overføres fra en dataansvarlig eller en databehandler i Unionen ⁽¹⁸⁾ til certificerede organisationer i USA.

⁽⁹⁾ Sag C-362/14, Maximilian Schrems mod Data Protection Commissioner (*Schrems*), ECLI:EU:C:2015:650, præmis 73.

⁽¹⁰⁾ *Schrems*, præmis 74.

⁽¹¹⁾ Jf. meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden, COM(2017) 7 af 10.1.2017, afsnit 3.1., s. 6-7.

⁽¹²⁾ *Schrems*, præmis 88-89.

⁽¹³⁾ Det Europæiske Databeskyttelsesråd, Adequacy Referential, WP 254 rev. 01. Kan findes på følgende link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

⁽¹⁴⁾ Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12.7.2016 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, 1.8.2016, s. 1).

⁽¹⁵⁾ *Schrems II*, præmis 185.

⁽¹⁶⁾ *Schrems II*, præmis 197.

⁽¹⁷⁾ 28 CFR Part 302.

⁽¹⁸⁾ Nærværende afgørelse er relevant for EØS. I henhold til aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS-aftalen) udvides Den Europæiske Unions indre marked til at omfatte de tre EØS-stater Island, Liechtenstein og Norge. Det Blandede EØS-Udvalgs afgørelse om indarbejdelse af forordning (EU) 2016/679 i bilag XI til EØS-aftalen blev vedtaget af Det Blandede EØS-Udvalg den 6.7.2018 og trådte i kraft den 20.7.2018. Forordningen er således omfattet af nævnte aftale. Med henblik på afgørelsen skal henvisninger til EU og EU-medlemsstaterne derfor forstås således, at de også omfatter EØS-staterne.

- (8) Denne afgørelse indebærer, at overførsel af personoplysninger fra dataansvarlige og databehandlere i Unionen ⁽¹⁵⁾ til certificerede organisationer i USA kan finde sted uden yderligere godkendelse. Den berører ikke den direkte anvendelse af forordning (EU) 2016/679 på sådanne organisationer, når betingelserne vedrørende nævnte forordnings geografiske anvendelsesområde, jf. forordningens artikel 3, er opfyldt.

2. EU-USA-DATABESKYTTELSESRAMMEN

2.1 Personligt og materielt anvendelsesområde

2.1.1 Certificerede organisationer

- (9) EU-USA-databeskyttelsesrammen er baseret på et certificeringssystem, hvorved amerikanske organisationer forpligter sig til at overholde en række principper for beskyttelse af privatlivets fred — »principperne i EU-USA-databeskyttelsesrammen«, herunder de supplerende principper (tilsammen: principperne) — udstedt af det amerikanske handelsministerium og indeholdt i bilag I til denne afgørelse ⁽¹⁶⁾. For at være berettiget til certificering i henhold til EU-USA-databeskyttelsesrammen skal en organisation være underlagt de undersøgelses- og håndhævelsesbeføjelser, der er tillagt Federal Trade Commission (den føderale handelskommission, FTC) eller det amerikanske transportministerium ⁽¹⁷⁾. Principperne finder anvendelse straks efter certificering. Som forklaret nærmere i betragtning 48-52 skal organisationer under EU-USA-databeskyttelsesrammen hvert år recertificere deres overholdelse af principperne ⁽¹⁸⁾.

2.1.2 Definition af personoplysninger og begreberne »dataansvarlig« og »mandatar«

- (10) Den beskyttelse, der ydes i henhold til EU-USA-databeskyttelsesrammen, gælder for alle personoplysninger, der overføres fra Unionen til organisationer i USA, som har certificeret deres overholdelse af principperne over for handelsministeriet, med undtagelse af oplysninger, der indsamles med henblik på offentliggørelse, radio- eller TV-udsendelser eller andre former for offentlig kommunikation af journalistisk materiale og oplysninger, der stammer fra tidligere offentliggjort materiale, der opbevares i et pressearkiv ⁽¹⁹⁾. Sådanne oplysninger kan derfor ikke overføres på grundlag af EU-USA-databeskyttelsesrammen.
- (11) I principperne defineres personoplysninger på samme måde som i forordning (EU) 2016/679, dvs. som »oplysninger, som kan henføres til en bestemt identificeret eller identificerbar person, som er omfattet af databeskyttelsesforordningen, som modtages fra EU af en organisation i USA, og som er registreret på en hvilken som helst måde« ⁽²⁰⁾. De omfatter derfor også pseudonymiserede (eller »kodede«) forskningsdata (herunder når nøglen ikke deles med den modtagende amerikanske organisation) ⁽²¹⁾. På samme måde defineres begrebet behandling som »enhver operation eller række af operationer — med eller uden brug af elektronisk databehandling — som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse eller formidling og slettelse eller tilintetgørelse« ⁽²²⁾.
- (12) EU-USA-databeskyttelsesrammen finder anvendelse på organisationer i USA, der betragtes som dataansvarlige (dvs. som en person eller en organisation, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger) ⁽²³⁾ eller databehandlere (dvs. mandatarer for den dataansvarlige) ⁽²⁴⁾. Databehandlere i USA skal være kontraktligt forpligtede til udelukkende at handle på den dataansvarlige i EU's anvisning og bistå denne med at besvare anmodninger fra fysiske personer, der udøver deres

⁽¹⁵⁾ Denne afgørelse berører ikke de krav i forordning (EU) 2016/679, der finder anvendelse på de enheder (dataansvarlige og databehandlere) i Unionen, der overfører oplysningerne, f.eks. vedrørende formålsbegrænsning, dataminimering, gennemsigtighed og datasikkerhed (jf. ligeledes artikel 44 i forordning (EU) 2016/679).

⁽¹⁶⁾ Jf. i denne forbindelse *Schrems*, præmis 81, hvori Domstolen bekræftede, at et selvcertificeringssystem kan sikre et tilstrækkeligt beskyttelsesniveau.

⁽¹⁷⁾ Bilag I, afsnit I, punkt 2. FTC har bred jurisdiktion over kommercielle aktiviteter, med visse undtagelser, f.eks. med hensyn til banker, luftfartsselskaber, forsikringsvirksomhed og teletjenesteudbydere. Fælles transportaktiviteter (selv om afgørelsen fra U.S. Court of Appeals for the Ninth Circuit af 26. februar 2018 i *FTC v. AT&T* har bekræftet, at FTC har jurisdiktion over sådanne enheders ikke-fælles luftfartsaktiviteter). Se også bilag IV, fodnote 2. Transportministeriet har kompetence til at håndhæve luftfartsselskabers og rejsebureauers overholdelse (for lufttransport), se bilag V, afsnit A.

⁽¹⁸⁾ Bilag I, afsnit III, punkt 6.

⁽¹⁹⁾ Bilag I, afsnit III, punkt 2.

⁽²⁰⁾ Bilag I, afsnit I, punkt 8.a.

⁽²¹⁾ Bilag I, afsnit III, punkt 14.g.

⁽²²⁾ Bilag I, afsnit I, punkt 8.b.

⁽²³⁾ Bilag I, afsnit I, punkt 8.c.

⁽²⁴⁾ Se f.eks. bilag I, del II.2.b, og afsnit II.3.b og 7.d, som gør det klart, at agenter handler på vegne af en dataansvarlig efter dennes instrukser og i henhold til specifikke kontraktlige forpligtelser.

rettigheder i henhold til principperne ⁽²⁵⁾. I forbindelse med udlicitering af databehandling skal databehandlere indgå en aftale med den underkontraherede databehandler, der sikrer det samme niveau af beskyttelse som i principperne, og sørge for, at den gennemføres korrekt ⁽²⁶⁾.

2.2 Principperne i EU-USA-databeskyttelsesrammen

2.2.1 Formålsbegrænsning og valgfrihed

- (13) Enhver behandling af personoplysninger skal være lovlig og rimelig. Personoplysninger skal indsamles til et specifikt formål og efterfølgende udelukkende anvendes, såfremt dette ikke er uforeneligt med behandlingsformålet.
- (14) I EU-USA-databeskyttelsesrammen sikres dette ved forskellige principper. For det første må en organisation i henhold til *princippet om dataintegritet og formålsbegrænsning*, i lighed med artikel 5, stk. 1, litra b), i forordning (EU) 2016/679, ikke behandle personoplysninger på en måde, der strider imod det formål, hvortil de oprindeligt er blevet indsamlet, eller det formål, der efterfølgende er blevet godkendt af den registrerede ⁽²⁷⁾.
- (15) For det andet skal organisationen, inden det anvender personoplysninger til et nyt (ændret) formål, der er væsentligt forskelligt, men stadig foreneligt med det oprindelige formål, eller videregiver dem til tredjemand, i overensstemmelse med *princippet om valgfrihed* ⁽²⁸⁾, give den registrerede mulighed for at modsætte sig anvendelsen af oplysningerne på en klar, åbenlys og let tilgængelig måde. Det er vigtigt at bemærke, at dette princip ikke træder i stedet for det udtrykkelige forbud mod uforenelig behandling ⁽²⁹⁾.

⁽²⁵⁾ Bilag I, afsnit III, punkt 10.a. Se også vejledningen udarbejdet af det amerikanske handelsministerium i samråd med Det Europæiske Databeskyttelsesråd under privatlivsskjoldet, som præciserede de forpligtelser, der påhviler amerikanske databehandlere, som modtager personoplysninger fra Unionen i henhold til rammen. Da disse regler ikke har ændret sig, er denne vejledning/FAQ fortsat relevant under EU-USA-databeskyttelsesrammen (<https://www.privacyshield.gov/article?id=Processing-FAQs>).

⁽²⁶⁾ Bilag I, afsnit II, punkt 3.b.

⁽²⁷⁾ Bilag I, afsnit II, punkt 5.a. Formål, der er forenelige med behandling, kan omfatte revision og bekæmpelse af svig eller andre formål, der stemmer overens med en fornuftig persons forventninger på baggrund af konteksten for indsamlingen (jf. bilag I, fodnote 6).

⁽²⁸⁾ Bilag I, afsnit II, punkt 2.a. Dette gælder ikke, når en organisation videregiver personoplysninger til en databehandler, der handler på dens vegne og efter dens anvisninger (bilag I, afsnit II, punkt 2.b). I dette tilfælde skal organisationen dog have indgået en aftale og sikre overholdelse af *princippet om ansvar for videreoverførsel*, som beskrevet nærmere i betragtning 43. Desuden kan princippet om *valgfrihed* (og princippet om *oplysningspligt*) begrænses, når personoplysninger behandles i forbindelse med due diligence (som led i en potentiel fusion eller overtagelse) eller revisioner, i det omfang og så længe det er nødvendigt for at opfylde lovbestemte krav eller tilgodesee vigtige samfundsinteresser, eller i det omfang og så længe anvendelsen af disse principper vil være til skade for organisationens legitime interesser i forbindelse med due diligence-undersøgelser eller -revisioner (bilag I, afsnit III, punkt 4). Supplerende princip 15 (bilag I, afsnit III, punkt 15.a og b) indeholder også en undtagelse fra princippet om *valgfrihed* (samt fra principperne om *oplysningspligt* og *ansvar for videreoverførsel*) for personoplysninger fra offentligt tilgængelige kilder (medmindre dataeksportøren i EU angiver, at oplysningerne er underlagt begrænsninger, der kræver anvendelse af disse principper) eller personoplysninger indsamlet fra registre, der er tilgængelige for offentligheden generelt (såfremt de ikke sammenføres med oplysninger i ikkeoffentlige registre, og såfremt alle betingelser for indsigt overholdes). Tilsvarende indeholder supplerende princip 14 (bilag I, afsnit III, punkt 14.f) en undtagelse fra *princippet om valgfrihed* (samt fra *principperne om oplysningspligt* og *ansvar for videreoverførsel*) for behandling af personoplysninger foretaget af virksomheder, der fremstiller farmaceutiske eller medicinske anordninger, med henblik på deres produktsikkerheds- og kontrolaktiviteter, i det omfang princippernes overholdelse falder sammen med overholdelsen af de gældende lovkrav.

⁽²⁹⁾ Det gælder alle overførsler af oplysninger inden for rammerne af EU-USA-databeskyttelsesrammen, også oplysninger, der er indsamlet i forbindelse med ansættelsesforhold. En certificeret organisation i USA kan dermed i princippet benytte oplysninger om menneskelige ressourcer til andre, ikke-ansættelsesrelaterede formål (f.eks. i forbindelse med markedsføring), men den skal overholde forbuddet mod uforenelig behandling, og en sådan brug må udelukkende ske i overensstemmelse med *principperne om oplysningspligt og valgfrihed*. En organisation kan undtagelsesvist anvende personoplysninger til et yderligere kompatibelt formål uden om princippet om *oplysningspligt* og *valgfrihed*, men kun i det omfang og så længe, det er nødvendigt for at undgå at skade organisationens evne til at foretage fremmeelser, udnævnelser eller andre lignende ansættelsesbeslutninger (se bilag I, afsnit III.9.b, nr. iv)). Forbuddet for den amerikanske organisation mod at straffe den ansatte for at have truffet et sådant valg, herunder en eventuel begrænsning af ansættelsesmuligheder, vil sikre, at den ansatte trods det hierarkiske forhold og dennes naturlige afhængighed ikke er underlagt et pres og dermed frit kan træffe et reelt frit valg. Jf. bilag I, afsnit III, punkt 9.b, nr. i.

2.2.2 *Behandling af særlige kategorier af personoplysninger*

- (16) Der skal forefindes særlige garantier i forbindelse med behandling af »særlige kategorier« af oplysninger.
- (17) I overensstemmelse med *princippet om valgfrihed* findes der særlige garantier for behandling af »følsomme oplysninger«, dvs. personoplysninger om helbredsforhold, race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmedlemskab, oplysninger om seksuelle forhold eller andre oplysninger, som modtages fra tredjemand, og som af den pågældende tredjemand betegnes og behandles som følsomme ⁽³⁰⁾. Det betyder, at certificerede organisationer vil behandle alle oplysninger, der betragtes som følsomme i henhold til EU's databeskyttelseslovgivning (herunder oplysninger om seksuel orientering, genetiske data og biometriske data), som følsomme i henhold til EU-USA-databeskyttelsesrammen.
- (18) Generelt skal organisationer indhente de pågældende personers udtrykkelige samtykke (dvs. opt in), hvis oplysningerne skal anvendes til et andet formål end det, hvortil de oprindeligt er blevet indsamlet, eller som de pågældende personer efterfølgende har givet tilladelse til, eller hvis de skal videregives til tredjemand ⁽³¹⁾.
- (19) Et sådant samtykke skal ikke indhentes under begrænsede omstændigheder, som kan sammenlignes med undtagelser i henhold til EU's databeskyttelseslovgivning, f.eks. hvis behandlingen af følsomme oplysninger er i en persons vitale interesse, er nødvendig for at fastslå et retskrav, eller er nødvendig i forbindelse med medicinsk behandling eller diagnosticering ⁽³²⁾.

2.2.3 *Oplysningernes nøjagtighed, minimering og sikkerhed*

- (20) Oplysningerne skal være nøjagtige og om nødvendigt holdes ajour. De skal være tilstrækkelige og relevante og ikke for omfattende i forhold til de formål, hvortil de behandles, og de må i princippet ikke opbevares i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de behandles.
- (21) I henhold til *princippet om dataintegritet og formålsbegrænsning* ⁽³³⁾ skal personoplysninger være begrænset til de oplysninger, der er relevante for formålene med behandlingen. Derudover skal organisationer, i det omfang det er nødvendigt for behandlingen, træffe passende foranstaltninger for at sikre, at personoplysningerne er pålidelige, nøjagtige, fuldstændige og ajourførte.
- (22) Personoplysninger må desuden alene opbevares i en form, der giver mulighed for at identificere eller gøre en person identificerbar (dvs. i form af personoplysninger) ⁽³⁴⁾, så længe det tjener de(t) formål, hvortil de oprindeligt blev indsamlet eller efterfølgende godkendt i henhold til *princippet om valgfrihed*. Denne pligt forhindrer ikke organisationer i at fortsætte med behandlingen af personoplysninger i længere perioder, men dog kun så længe og i det omfang en sådan behandling med rimelighed tjener et af følgende formål, som kan sammenlignes med undtagelser i henhold til EU's databeskyttelseslovgivning: arkivering i samfundets interesse, journalistik, kunst og litteratur, videnskabelig og historisk forskning samt statistisk analyse ⁽³⁵⁾. Hvis personoplysninger opbevares til et af disse formål, er behandlingen heraf underlagt garantierne i principperne ⁽³⁶⁾.
- (23) Personoplysninger skal endvidere behandles på en måde, der garanterer deres sikkerhed, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse. Med henblik herpå skal de dataansvarlige og databehandlere træffe passende tekniske eller organisatoriske foranstaltninger for at beskytte personoplysninger mod mulige trusler. Disse foranstaltninger skal vurderes under hensyntagen til det aktuelle tekniske niveau og de dermed forbundne omkostninger samt behandlingens karakter, omfang, sammenhæng og formål samt risiciene for den enkeltes rettigheder.

⁽³⁰⁾ Bilag I, afsnit II, punkt 2.c.

⁽³¹⁾ Bilag I, afsnit II, punkt 2.c.

⁽³²⁾ Bilag I, afsnit III, punkt 1.

⁽³³⁾ Bilag I, afsnit II, punkt 5.

⁽³⁴⁾ Jf. bilag I, fodnote 7, hvori det præciseres, at en person anses for at være »identificerbar«, såfremt den pågældende i betragtning af den med rimelighed forventede identifikationsmetode (under hensyntagen til bl.a. omkostningerne og det fornødne tidsforbrug ved identificeringen samt den på behandlingstidspunktet tilgængelige teknologi) med rimelighed kan identificeres af organisationen eller af en tredjemand.

⁽³⁵⁾ Bilag I, afsnit II, punkt 5.b.

⁽³⁶⁾ *Ibid.*

- (24) I henhold til EU-USA-databeskyttelsesrammen sikres dette ved *sikkerhedsprincippet*, som i lighed med artikel 32 i forordning (EU) 2016/679 kræver, at der træffes rimelige og passende sikkerhedsforanstaltninger under hensyntagen til de risici, som behandlingen indebærer, og de pågældende oplysningers karakter ⁽³⁷⁾.

2.2.4 Gennemsigtighed

- (25) De registrerede skal informeres om de vigtigste elementer i behandlingen af deres personoplysninger.
- (26) Dette sikres ved *princippet om oplysningspligt* ⁽³⁸⁾, som i lighed med kravene om gennemsigtighed i forordning (EU) 2016/679 kræver, at organisationer giver oplysninger til registrerede om bl.a. i) organisationens deltagelse i databeskyttelsesrammen, ii) typen af indsamlede oplysninger, iii) formålet med behandlingen, iv) typen eller identiteten af tredjeparter, som personoplysninger kan blive videregivet til, og formålene hermed, v) deres individuelle rettigheder, vi) organisationens kontaktoplysninger og vii) tilgængelige klagemuligheder.
- (27) Meddelelsen herom skal formidles klart og tydeligt, når den enkelte første gang anmodes om at udlevere personoplysninger, eller så hurtigt som muligt derefter, dog under alle omstændigheder inden personoplysningerne anvendes til et væsentligt andet (men kompatibelt) formål end det, hvortil de blev indsamlet, eller inden de videregives til tredjemand ⁽³⁹⁾.
- (28) Derudover skal organisationer offentliggøre deres politikker til beskyttelse af privatlivets fred, der afspejler principperne (eller, hvis der er tale om data vedrørende menneskelige ressourcer, gøre dem let tilgængelige for de berørte personer), og angive links til handelsministeriets websted (med yderligere oplysninger om certificering, de registreredes rettigheder og tilgængelige klagemekanismer), listen over deltagende organisationer i databeskyttelsesrammen og webstedet for en relevant udenretslig tvistbilæggesinstans ⁽⁴⁰⁾.

2.2.5 Individuelle rettigheder

- (29) De registrerede skal have visse rettigheder, som kan håndhæves over for den dataansvarlige eller databehandleren, navnlig retten til indsigt i oplysninger, retten til at gøre indsigelse mod behandlingen og retten til at få oplysninger berigtiget og slettet.
- (30) *Princippet om indsigt* ⁽⁴¹⁾ i EU-USA-databeskyttelsesrammen giver den enkelte sådanne rettigheder. Navnlig har registrerede ret til uden begrundelse at få oplyst, om en organisation behandler personoplysninger om dem, at få oplysningerne udleveret og at få oplysninger om formålet med behandlingen, de kategorier af personoplysninger, der behandles, og de (kategorier af) modtagere, som oplysningerne videregives til ⁽⁴²⁾. Organisationer skal besvare anmodninger om indsigt inden for en rimelig frist ⁽⁴³⁾. En organisation kan fastsætte en passende maksimumsgrænse for det antal gange, anmodninger om indsigt fra en bestemt person inden for en bestemt

⁽³⁷⁾ Bilag I, afsnit II, punkt 4.a. Hvad angår oplysninger om menneskelige ressourcer kræver EU-USA-databeskyttelsesrammen desuden, at arbejdsgiverne respekterer de ansattes ønsker om hemmeligholdelse af personoplysninger ved at give begrænset indsigt i personoplysninger, gøre visse oplysninger anonyme eller anvende koder eller pseudonymer (bilag I, afsnit III, punkt 9.b, nr. iii).

⁽³⁸⁾ Bilag I, afsnit II, punkt 1.

⁽³⁹⁾ Bilag I, afsnit II, punkt 1.b. Supplerende princip 14 (bilag I, afsnit III, punkt 14.b og c) indeholder specifikke bestemmelser om behandling af personoplysninger i forbindelse med sundhedsforskning og kliniske forsøg. Dette princip giver navnlig organisationer mulighed for at behandle oplysninger om kliniske forsøg, selv efter at en person har trukket sig ud af forsøget, hvis dette blev præciseret i den meddelelse, der blev givet, da personen indvilligede i at deltage. Tilsvarende må en organisation under EU-USA-databeskyttelsesrammen, hvis den modtager personoplysninger til sundhedsforskningsformål, kun anvende dem til en ny forskningsaktivitet i overensstemmelse med *principperne om oplysningspligt og valgfrihed*. I så fald skal meddelelsen til den enkelte person i princippet indeholde oplysninger om alle fremtidige specifikke anvendelser af oplysningerne (f.eks. relaterede undersøgelser). Hvis det ikke er muligt at medtage alle fremtidige anvendelser af oplysningerne fra starten af (fordi der kan opstå en ny forskningsanvendelse som følge af ny viden eller medicinsk/forskningsmæssig udvikling), skal der vedlægges en forklaring om, at oplysningerne kan blive anvendt i fremtidige uventede medicinske og farmaceutiske forskningsaktiviteter. Hvis en sådan yderligere anvendelse ikke er i overensstemmelse med de generelle forskningsformål, som dataene blev indsamlet til (dvs. hvis de nye formål er væsentligt anderledes, men stadig forenelige med det oprindelige formål, se betragtning 14-15), skal der indhentes nyt samtykke (dvs. tilvalg). Jf. desuden de specifikke begrænsninger for/undtagelser fra *princippet om oplysningspligt*, der er beskrevet i fodnote 28.

⁽⁴⁰⁾ Bilag I, afsnit III, punkt 6.d.

⁽⁴¹⁾ Jf. ligeledes det supplerende princip »Indsigt« (bilag I, afsnit III, punkt 8).

⁽⁴²⁾ Bilag I, afsnit III, punkt 8.a., nr. i-ii.

⁽⁴³⁾ Bilag I, afsnit III, punkt 8.i.

periode vil blive behandlet, og kan opkræve et gebyr, der ikke er uforholdsmæssigt stort, f.eks. hvis anmodningerne om indsigt er tydeligt overdrevne, navnlig fordi de gentages ⁽⁴⁴⁾.

- (31) Retten til indsigt kan kun begrænses under særlige omstændigheder svarende til dem, der er fastsat i EU's databeskyttelseslovgivning, navnlig hvor det ville medføre en krænkelse af andre personers legitime rettigheder, hvor meradministrationen eller meromkostningerne ved at give indsigt i disse oplysninger ville være uforholdsmæssig store i forhold til risikoen for den pågældende persons privatliv under sagens omstændigheder (selv om meromkostninger og meradministration ikke er afgørende faktorer ved vurderingen af, om det er rimeligt at give indsigt), hvis en videregivelse kan antages at vanskeliggøre beskyttelsen af vigtige altovervejende offentlige interesser, herunder den nationale sikkerhed, den offentlige sikkerhed eller forsvaret), hvis oplysningerne indeholder fortrolige forretningsoplysninger, eller hvis oplysningerne udelukkende behandles med henblik på forskning eller i statistisk øjemed ⁽⁴⁵⁾. Enhver nægtelse eller begrænsning af en rettighed skal være nødvendig og behørigt begrundet, og organisationen skal dokumentere, at disse krav er opfyldt ⁽⁴⁶⁾. I forbindelse med denne vurdering skal organisationen navnlig tage hensyn til den enkeltes interesser ⁽⁴⁷⁾. Hvis det er muligt at adskille oplysningerne fra andre data, der er omfattet af en begrænsning, skal organisationen bortredigere de beskyttede oplysninger og videregive de resterende oplysninger ⁽⁴⁸⁾.
- (32) De registrerede har desuden ret til at få berigtiget eller ændret ukorrekte oplysninger og til at få slettet oplysninger, der er blevet behandlet i strid med principperne ⁽⁴⁹⁾. Som forklaret i betragtning 15 har personer desuden ret til at gøre indsigelse mod/fravælge behandlingen af deres oplysninger til formål, der er væsentligt anderledes end (men forenelige med) dem, hvortil oplysningerne blev indsamlet, og videregivelsen af deres oplysninger til tredjemand. Når personoplysninger anvendes til direkte markedsføring, har personer generelt ret til enhver tid at fravælge behandlingen ⁽⁵⁰⁾.
- (33) Principperne omhandler ikke specifikt spørgsmålet om beslutninger vedrørende en person, der alene er baseret på automatiseret behandling af personoplysninger. I forbindelse med personoplysninger, der er indsamlet i Unionen, vil enhver beslutning baseret på automatiseret behandling imidlertid typisk blive truffet af den dataansvarlige i Unionen (som har en direkte relation til den berørte registrerede), og den vil således være omfattet af forordning (EU) 2016/679 ⁽⁵¹⁾. Dette omfatter overførselsscenarier, hvor behandlingen foretages af en udenlandsk (f. eks. amerikansk) erhvervsdrivende, der handler som mandatar (databehandler) på vegne af den dataansvarlige i Unionen (eller som en underkontraheret databehandler, der handler på vegne af en databehandler i Unionen, som har modtaget oplysningerne fra den indsamlede dataansvarlige i Unionen), og som på dette grundlag således træffer beslutningen.
- (34) Dette blev bekræftet af en undersøgelse bestilt af Kommissionen i 2018 i forbindelse med den anden årlige evaluering af privatlivsskjoldets funktion ⁽⁵²⁾, som konkluderede, at der på daværende tidspunkt ikke var noget, der tydede på, at organisationer i privatlivsskjoldet normalt traf automatiserede beslutninger på grundlag af personoplysninger, som blev overført under privatlivsskjoldet.

⁽⁴⁴⁾ Bilag I, afsnit III, punkt 8.f., nr. i-ii, og g.

⁽⁴⁵⁾ Bilag I, afsnit III, punkt 4, punkt 8.b, c, e, punkt 14.e, f og punkt 15.d.

⁽⁴⁶⁾ Bilag I, afsnit III, punkt 8.e., nr. ii. Organisationens skal underrette den pågældende om årsagerne til nægtelsen/begrænsningen og oplyse, hvor vedkommende kan henvende sig for yderligere oplysninger, afsnit III, punkt 8.a., nr. iii.

⁽⁴⁷⁾ Bilag I, afsnit III, punkt 8.a., nr. ii-iii.

⁽⁴⁸⁾ Bilag I, afsnit III, punkt 8.a., nr. i.

⁽⁴⁹⁾ Bilag I, afsnit II, punkt 6, og afsnit III, punkt 8.a., nr. i.

⁽⁵⁰⁾ Bilag I, afsnit III, punkt 8.12.

⁽⁵¹⁾ I de ekstraordinære tilfælde, hvor den amerikanske organisation har en direkte relation til den registrerede i EU, vil det omvendt typisk være en konsekvens af, at organisationen har rettet sin indsats mod den pågældende person i Unionen ved at tilbyde denne varer eller tjenesteydelser eller ved at overvåge dennes adfærd. I dette scenarie vil den amerikanske organisation selv være omfattet af anvendelsesområdet for forordning (EU) 2016/679 (artikel 3, stk. 2) og skal derfor direkte overholde EU's databeskyttelseslovgivning.

⁽⁵²⁾ SWD(2018) 497 final, afsnit 4.1.5. Undersøgelsen fokuserede på, i) i hvilket omfang organisationer i privatlivsskjoldet i USA træffer beslutninger vedrørende enkeltpersoner på grundlag af automatiseret behandling af personoplysninger, der overføres fra virksomheder i EU under privatlivsskjoldet, og ii) de garantier, som USA's føderale lovgivning yder enkeltpersoner i forbindelse med denne type situationer, og betingelserne for, at disse garantier finder anvendelse.

- (35) Under alle omstændigheder indeholder amerikansk ret på de områder, hvor organisationer ofte anvender automatiseret behandling af personoplysninger til at træffe beslutninger vedrørende en fysisk person (f.eks. långivning, realkreditlån, ansættelse, bolig og forsikring), særlige garantier vedrørende negative beslutninger ⁽⁵³⁾. Disse love indeholder typisk bestemmelser, der giver fysiske personer ret til at blive oplyst om de specifikke årsager til beslutningen (f.eks. afvisning af lån), at bestride ufuldstændige eller unøjagtige oplysninger (samt anvendelsen af uretmæssige forhold) samt til at klage. På forbrugerkreditområdet indeholder Fair Credit Reporting Act (FCRA) og Equal Credit Opportunity Act (ECOA) garantier, der giver forbrugerne en form for ret til en forklaring og ret til at anfægte beslutningen. Disse love er relevante på en lang række områder, herunder långivning, ansættelse, bolig og forsikring. Desuden giver visse love om bekæmpelse af forskelsbehandling, såsom Title VII i Civil Rights Act og Fair Housing Act, personer beskyttelse med hensyn til modeller, der anvendes i automatiserede beslutningsprocesser, som kan føre til forskelsbehandling på grundlag af visse kendetegn, og de giver personer ret til at anfægte sådanne beslutninger, herunder de automatiserede beslutninger. Hvad angår sundhedsrelaterede oplysninger skaber reglen om beskyttelse af privatlivets fred i Health Insurance Portability and Accountability Act (HIPAA) visse rettigheder, der svarer til rettighederne i forordning (EU) 2016/679 med hensyn til adgangen til personlige sundhedsoplysninger. Derudover kræver retningslinjer fra de amerikanske myndigheder, at udbydere af sundhedsydelser modtager oplysninger, der gør det muligt for dem at informere enkeltpersoner om automatiserede beslutningssystemer, der anvendes i sundhedssektoren ⁽⁵⁴⁾.
- (36) Disse regler giver derfor en beskyttelse svarende til den, der er fastsat i EU's databeskyttelseslovgivning, i den usandsynlige situation, hvor organisationen under EU-USA-databeskyttelsesrammen selv træffer automatiserede beslutninger.

2.2.6 Begrænsninger for videreoverførsler

- (37) Beskyttelsesniveauet for personoplysninger, der overføres fra Unionen til organisationer i USA, må ikke undergraves ved videre overførsel af sådanne oplysninger til en modtager i USA eller et andet tredjeland.
- (38) I henhold til *princippet om ansvar for videreoverførsel* ⁽⁵⁵⁾ findes der særlige regler for såkaldte »videreoverførsler«, dvs. overførsler af personoplysninger fra en organisation under EU-USA-databeskyttelsesrammen til tredjemand, som er dataansvarlig eller databehandler, uanset om sidstnævnte befinder sig i USA eller et tredjeland uden for USA (og EU). Videreoverførsel kan alene finde sted i) til begrænsede og bestemte formål, ii) på grundlag af en aftale mellem organisationen under EU-USA-databeskyttelsesrammen og den pågældende tredjepart ⁽⁵⁶⁾ (eller et tilsvarende arrangement i en koncern ⁽⁵⁷⁾) og iii) udelukkende, hvis denne aftale sikrer, at tredjeparten sikrer det samme beskyttelsesniveau som principperne.
- (39) Denne forpligtelse til at sikre det samme beskyttelsesniveau som principperne, sammenholdt med *princippet om dataintegritet og formålsbegrænsning*, betyder navnlig, at tredjemand kun må behandle de personoplysninger, der videregives til vedkommende, til formål, der ikke er uforenelige med de formål, hvortil de blev indsamlet, eller som den registrerede efterfølgende har godkendt (i overensstemmelse med *princippet om valgfrihed*).

⁽⁵³⁾ Jf. f.eks. Equal Credit Opportunity Act (15 U.S.C. 1691 et seq.), Fair Credit Reporting Act (15 USC § 1681 et seq.) eller Fair Housing Act (42 U.S.C. 3601 et seq.). Desuden har USA tilsluttet sig Organisation for Økonomisk Samarbejde og Udviklings principper for kunstig intelligens, som bl.a. omfatter principper om gennemsigtighed, forklarlighed, sikkerhed og ansvarlighed.

⁽⁵⁴⁾ Jf. f.eks. retningslinjerne på 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

⁽⁵⁵⁾ Jf. bilag I, afsnit II, punkt 3, og det supplerende princip »Obligatoriske aftaler om videreoverførsel« (bilag I, afsnit III, punkt 10).

⁽⁵⁶⁾ Som en undtagelse fra dette generelle princip kan en organisation videregive personoplysninger om et lille antal medarbejdere uden at indgå en aftale med modtageren, når der er tale om lejlighedsvis ansættelsesrelaterede operationelle behov, f.eks. i forbindelse med booking af et fly, hotelværelse eller forsikringsdækning. I dette tilfælde skal organisationen dog stadig overholde *principperne om oplysningspligt og valgfrihed* (jf. bilag I, afsnit III, punkt 9.e).

⁽⁵⁷⁾ Jf. det supplerende princip »Obligatoriske aftaler om videreoverførsel« (bilag I, afsnit III, punkt 10.b). Selv om dette princip giver mulighed for overførsler, der også er baseret på ikkekontraktlige instrumenter (f.eks. koncerninterne overholdelses- og kontrolprogrammer), fremgår det klart af teksten, at disse instrumenter altid skal »sikre kontinuitet i beskyttelsen af personoplysninger i henhold til principperne«. Eftersom den certificerede organisation i USA fortsat vil skulle overholde principperne, vil den have et stærkt incitament til at benytte instrumenter, som rent faktisk fungerer godt i praksis.

- (40) Princippet om ansvar for videreoverførsel bør også ses i sammenhæng med princippet om oplysningspligt og, i tilfælde af videreoverførsel til en dataansvarlig tredjepart ⁽⁵⁸⁾, princippet om valgfrihed, ifølge hvilke den registrerede skal oplyses om (bl.a.) typen/identiteten af en eventuel tredjepartsmodtager, formålet med videreoverførslen og valgfriheden og kan vælge at modsætte sig (opt out) eller, i forbindelse med følsomme oplysninger, skal give sit »udtrykkelige samtykke« (opt in) til videreoverførslen.
- (41) Pligten til at yde samme niveau af beskyttelse som krævet i principperne gælder alle tredjeparter, der deltager i behandlingen af overførte oplysninger, uanset hvor de befinder sig (i USA eller et andet tredjeland), også når den oprindelige modtagende tredjepart selv overfører oplysningerne til en anden modtagende tredjepart f.eks. i forbindelse med udlicitering.
- (42) Under alle omstændigheder skal det fastslås i aftalen med den modtagende tredjepart, at denne underretter organisationen under EU-USA-databeskyttelsesrammen, hvis den beslutter, at den ikke længere kan opfylde denne pligt. Når en tredjepart træffer en sådan beslutning, skal denne ophøre med at behandle oplysningerne eller træffe andre rimelige og passende skridt for at rette op på situationen ⁽⁵⁹⁾.
- (43) Der gælder yderligere garantier i tilfælde af videreoverførsel til en tredjepart, der fungerer som mandatar (dvs. en databehandler). I et sådant tilfælde skal den amerikanske organisation sikre, at mandataren kun handler efter dets anvisninger, og træffe rimelige og passende foranstaltninger til i) at sikre, at mandataren behandler de overførte personoplysninger i overensstemmelse med organisationens pligter i henhold til principperne, og ii) at indstille og afhjælpe uautoriseret behandling efter eventuel meddelelse herom ⁽⁶⁰⁾. Organisationen kan af handelsministeriet blive pålagt at forelægge et sammendrag eller en repræsentativ kopi af de relevante bestemmelser om beskyttelse af privatlivets fred i aftalen ⁽⁶¹⁾. I tilfælde af problemer med overholdelsen i udliciterings- eller behandlingskæden skal organisationen, der fungerer som dataansvarlig for personoplysningerne, påtage sig ansvaret, jf. *princippet om klageadgang, håndhævelse og ansvar*, medmindre det beviser, at det ikke er skyld i den begivenhed, der medførte skaden ⁽⁶²⁾.

2.2.7 **Ansvar**

- (44) I henhold til princippet om ansvar skal enheder, der behandler oplysninger, træffe passende tekniske og organisatoriske foranstaltninger med henblik på effektiv overholdelse af deres databeskyttelsesforpligtelser, og de skal være i stand til at dokumentere denne overholdelse, navnlig over for den kompetente tilsynsmyndighed.
- (45) Når en organisation frivilligt har besluttet at foretage certificering ⁽⁶³⁾ under EU-USA-databeskyttelsesrammen, skal det overholde principperne til fulde, og overholdelsen skal håndhæves. I henhold til *princippet om klageadgang, håndhævelse og ansvar* ⁽⁶⁴⁾ skal organisationer under EU-USA-databeskyttelsesrammen iværksætte effektive mekanismer, der sætter dem i stand til at overholde principperne. Organisationer skal desuden træffe foranstaltninger til at kontrollere ⁽⁶⁵⁾, at deres politik til beskyttelse af privatlivets fred er i overensstemmelse med principperne og rent faktisk overholdes. Dette kan enten gøres gennem selvevaluering, som skal inkludere interne procedurer, der sikrer, at de ansatte informeres om implementeringen af organisationens politik til beskyttelse af privatlivets fred, og at overholdelsen kontrolleres regelmæssigt og objektivt, eller gennem ekstern kontrol af overholdelsen, der kan omfatte revision, stikprøvekontrol eller anvendelse af teknologiske værktøjer.

⁽⁵⁸⁾ Registrerede har ikke ret til opt out, hvis personoplysningerne overføres til en tredjepart, der fungerer som mandatar og udfører opgaver på vegne af den amerikanske organisation og i henhold til dens anvisninger. Det kræver dog, at der er indgået en aftale med mandataren, og at den amerikanske organisation bærer ansvaret for at garantere den beskyttelse, der skal ydes i henhold til principperne, ved at udnytte dens anvisningsbeføjelser.

⁽⁵⁹⁾ Omstændighederne varierer, afhængigt af om tredjeparten er en dataansvarlig eller en databehandler (mandatar). I det første tilfælde skal aftalen med tredjeparten fastslå, at sidstnævnte ophører med behandlingen eller træffer andre rimelige eller passende foranstaltninger til at rette op på situationen. I det andet tilfælde er det organisationen under EU-USA-databeskyttelsesrammen — som har ansvaret for behandlingen og giver anvisninger til mandataren — der skal træffe disse foranstaltninger. Jf. bilag I, afsnit II, punkt 3.

⁽⁶⁰⁾ Bilag I, afsnit II, punkt 3.b.

⁽⁶¹⁾ *Ibid.*

⁽⁶²⁾ Bilag I, afsnit II, punkt 7.d.

⁽⁶³⁾ Jf. også det supplerende princip »Selvcertificering« (bilag I, afsnit III, punkt 6).

⁽⁶⁴⁾ Jf. også det supplerende princip »Bilæggelse af tvister og håndhævelse« (bilag I, afsnit III, punkt 11).

⁽⁶⁵⁾ Jf. også det supplerende princip »Kontrol (verifikation)« (bilag I, afsnit III, punkt 7).

- (46) Derudover skal organisationerne føre protokol over implementeringen af deres praksis under EU-USA-databeskyttelsesrammen og på anmodning herom stille disse protokoller til rådighed for et uafhængigt tvistbilæggesorgan eller en kompetent håndhævelsesmyndighed i forbindelse med en undersøgelse eller klage vedrørende manglende overholdelse ⁽⁶⁶⁾.

2.3 Forvaltning, tilsyn og håndhævelse

- (47) EU-USA-databeskyttelsesrammen vil blive forvaltet og overvåget af det amerikanske handelsministerium. Rammen indeholder tilsyns- og håndhævelsesmekanismer til at kontrollere og sikre, at organisationer under EU-USA-databeskyttelsesrammen overholder principperne, og at der tages hånd om eventuel manglende overholdelse. Disse mekanismer er indeholdt i principperne (bilag I) og de tilsagn, der er afgivet af det amerikanske handelsministerium (bilag III), FTC (bilag IV) og det amerikanske transportministerium (bilag V).

2.3.1 (Re)certificering

- (48) Certificering i henhold til EU-USA-databeskyttelsesrammen (eller årlig recertificering) kræver, at organisationerne offentligt erklærer deres tilslutning til principperne, offentliggør deres politik til beskyttelse af privatlivets fred og implementerer den fuldt ud ⁽⁶⁷⁾. Som led i deres ansøgning om (re)certificering skal organisationerne indsende oplysninger til handelsministeriet om bl.a. navnet på den relevante organisation, en beskrivelse af de formål, hvortil organisationen vil behandle personoplysninger, de personoplysninger, der vil være omfattet af certificeringen, samt den valgte kontrolmetode, den relevante uafhængige klageinstans og det lovbestemte organ, der har kompetence til at håndhæve overholdelsen af principperne ⁽⁶⁸⁾.
- (49) Organisationer kan modtage personoplysninger på grundlag af EU-USA-databeskyttelsesrammen fra den dato, hvor handelsministeriet optager dem på listen over deltagende organisationer i databeskyttelsesrammen. Af hensyn til retssikkerheden og for at undgå »falske påstande« er organisationer, der certificeres for første gang, ikke berettiget til offentligt at henvise til deres tilslutning til principperne, før handelsministeriet har fastslået, at organisationens anmeldelse om certificering er fuldstændig, og har tilføjet organisationen til listen over deltagende organisationer ⁽⁶⁹⁾. For fortsat at kunne modtage personoplysninger fra EU inden for EU-USA-databeskyttelsesrammen skal disse organisationer årligt recertificere deres deltagelse. Hvis en organisation af den ene eller anden årsag forlader EU-USA-databeskyttelsesrammen, skal det fjerne alle udtalelser, der lader formode, at organisationen fortsat deltager i databeskyttelsesrammen ⁽⁷⁰⁾.
- (50) Som det fremgår af tilsagnene i bilag III, kontrollerer det amerikanske handelsministerium, om organisationerne opfylder alle certificeringskrav og har indført en (offentlig) politik til beskyttelse af privatlivets fred, som indeholder de oplysninger, der kræves i henhold til *princippet om oplysningspligt* ⁽⁷¹⁾. På grundlag af erfaringerne med (re)certificeringsprocessen under privatlivsskjoldet vil handelsministeriet foretage en række kontroller, herunder for at kontrollere, om organisationernes politikker til beskyttelse af privatlivets fred indeholder et hyperlink til den korrekte klageformular på det relevante tvistbilæggesorgans websted, og — hvis flere af en organisations enheder og datterselskaber er omfattet af en anmeldelse om certificering — om alle disse enheders politikker til beskyttelse af privatlivets fred opfylder certificeringskravene og er let tilgængelige for de registrerede ⁽⁷²⁾. Derudover vil handelsministeriet om nødvendigt foretage krydskontrol sammen med FTC og transportministeriet for at kontrollere, at organisationerne er underlagt det tilsynsorgan, der er identificeret i deres anmeldelse om (re)certificering, og det vil samarbejde med alternative tvistbilæggesorganer for at kontrollere, at organisationerne er registreret hos den uafhængige klageinstans, der er identificeret i deres anmeldelse om (re)certificering ⁽⁷³⁾.

⁽⁶⁶⁾ Bilag I, afsnit III, punkt 7.

⁽⁶⁷⁾ Bilag I, afsnit I, 2.

⁽⁶⁸⁾ Bilag I, afsnit III, punkt 6.b, og bilag III, jf. afsnittet »Kontrol af selvcertificeringskrav«.

⁽⁶⁹⁾ Bilag I, fodnote 12.

⁽⁷⁰⁾ Bilag I, afsnit III, punkt 6.h.

⁽⁷¹⁾ Bilag I, afsnit III, punkt 6.a, og fodnote 12, og bilag III, jf. afsnittet »Kontrol af selvcertificeringskrav«.

⁽⁷²⁾ Bilag III, afsnittet »Kontrol af selvcertificeringskrav«.

⁽⁷³⁾ Tilsvarende vil handelsministeriet samarbejde med den tredjepart, der vil fungere som depotinstitution for de midler, der indsamles via et gebyr til panelet af databeskyttelsesmyndigheder (jf. betragtning 73), for at kontrollere, at organisationer, der vælger databeskyttelsesmyndighederne som deres uafhængige klageinstans, har betalt gebyret for det relevante år. Jf. bilag III, afsnittet »Kontrol af selvcertificeringskrav«.

- (51) Handelsministeriet underretter organisationerne om, at de for at fuldføre (re)certificeringen skal afhjælpe alle de problemer, der blev identificeret under ministeriets revision. Såfremt en organisation ikke svarer inden for en af handelsministeriet fastsat frist (f.eks. forventes det i forbindelse med (re)certificering, at processen afsluttes inden for 45 dage) ⁽⁷⁴⁾ eller på anden måde ikke fuldfører certificeringen, anses anmeldelsen for at være opgivet. I så fald kan der mod en organisation, der afgiver urigtige oplysninger vedrørende dets deltagelse i eller overholdelse af EU-USA-databeskyttelsesrammen, anlægges en håndhævelsessag for FTC eller transportministeriet ⁽⁷⁵⁾.
- (52) For at sikre en korrekt anvendelse af EU-USA-databeskyttelsesrammen skal interesserede parter, f.eks. registrerede, dataeksportører og de nationale databeskyttelsesmyndigheder kunne identificere de organisationer, der har tilsluttet sig principperne. For at sikre en sådan gennemsigtighed på »indgangsstedet« har handelsministeriet påtaget sig at føre og offentliggøre listen over organisationer, der på grundlag af certificering har tilsluttet sig principperne, og som er underlagt mindst en af de håndhævelsesmyndigheder, der er nævnt i bilag IV og V til denne afgørelse ⁽⁷⁶⁾. Handelsministeriet vil ajourføre listen på grundlag af en organisations årlige anmeldelser om recertificering, og når en organisation trækker sig ud af eller udelukkes fra EU-USA-databeskyttelsesrammen. For også at sikre gennemsigtigheden på »udgangsstedet« vil ministeriet ligeledes føre og offentliggøre en fortegnelse over organisationer, der er blevet fjernet fra listen, og i hvert enkelt tilfælde angive årsagen hertil ⁽⁷⁷⁾. Endelig vil ministeriet angive et link FTC's websted vedrørende EU-USA-databeskyttelsesrammen, som indeholder en liste over FTC-håndhævelsessager relateret til databeskyttelsesrammen ⁽⁷⁸⁾.

2.3.2 Overvågning af overholdelsen

- (53) Handelsministeriet vil løbende holde øje med, at organisationerne under EU-USA-databeskyttelsesrammen faktisk overholder principperne ved hjælp af forskellige mekanismer ⁽⁷⁹⁾. Det vil navnlig foretage stikprøvekontrol af tilfældigt udvalgte organisationer samt ad hoc-stikprøvekontrol af specifikke organisationer, når der konstateres potentielle problemer med overholdelsen (som f.eks. er blevet indberettet til handelsministeriet af tredjeparter), for at kontrollere, om i) de kontaktpunkter, der håndterer klager og anmodninger fra registrerede, er tilgængelige og imødekommende, ii) organisationens politik til beskyttelse af privatlivets fred er let tilgængelig, både på dens websted og via et hyperlink på handelsministeriets websted, iii) organisationens politik til beskyttelse af privatlivets fred fortsat er i overensstemmelse med certificeringskravene, og iv) det uafhængige tvistbilæggelsesorgan, som organisationen har valgt, er til rådighed til at behandle klager ⁽⁸⁰⁾.
- (54) Hvis der er troværdig dokumentation for, at en organisation ikke overholder sine forpligtelser i henhold til EU-USA-databeskyttelsesrammen (herunder hvis handelsministeriet modtager klager, eller organisationen ikke svarer tilfredsstillende på dets forespørgsler), vil handelsministeriet kræve, at organisationen udfylder og indsender et detaljeret spørgeskema ⁽⁸¹⁾. en organisation, der ikke besvarer spørgeskemaet rettidigt og på tilfredsstillende vis, vil blive henvist til den relevante myndighed (FTC eller transportministeriet) med henblik på eventuelle håndhævelsesforanstaltninger ⁽⁸²⁾. Som led i sine overvågningsaktiviteter under privatlivsskjoldet gennemførte handelsministeriet

⁽⁷⁴⁾ Bilag III, fodnote 2.

⁽⁷⁵⁾ Jf. bilag III, afsnittet »Kontrol af selvcertificeringskrav«.

⁽⁷⁶⁾ Bilag III (jf. indledningen under »Handelsministeriets forvaltning af og tilsyn med rammeprogrammet for databeskyttelse«) og bilag I (afsnit I, punkt 3, afsnit I, punkt 4, afsnit III, punkt 6.d, og afsnit III, punkt 11.g) indeholder oplysninger om forvaltningen af listen over deltagere i databeskyttelsesrammen.

⁽⁷⁷⁾ Bilag III, jf. indledningen under »Handelsministeriets forvaltning af og tilsyn med rammeprogrammet for databeskyttelse«.

⁽⁷⁸⁾ Jf. bilag III, afsnittet »Skræddersyet websted for databeskyttelsesrammen til bestemte målgrupper«.

⁽⁷⁹⁾ Jf. bilag III, afsnittet »Gennemførelse af regelmæssige ex officio-kontroller og -vurderinger af rammeprogrammet for databeskyttelse«.

⁽⁸⁰⁾ Handelsministeriet kan i sine overvågningsaktiviteter benytte forskellige værktøjer, herunder til at kontrollere, om der er døde links til politikker til beskyttelse af privatlivets fred, eller aktivt holde øje med rapporter i nyhederne, der giver troværdig dokumentation for manglende overholdelse.

⁽⁸¹⁾ Jf. bilag III, afsnittet »Gennemførelse af regelmæssige ex officio-kontroller og -vurderinger af rammeprogrammet for databeskyttelse«.

⁽⁸²⁾ Jf. bilag III, afsnittet »Gennemførelse af regelmæssige ex officio-kontroller og -vurderinger af rammeprogrammet for databeskyttelse«.

regelmæssigt de stikprøvekontroller, der er nævnt i betragtning 53, og overvågede løbende offentlige rapporter, hvilket gjorde det muligt at identificere, tage fat om og løse problemer med overholdelsen ⁽⁸³⁾. Organisationer, der vedvarende overtræder principperne, vil blive fjernet fra listen over deltagere i databeskyttelsesrammen, og de skal tilbagesende eller slette de personoplysninger, de har modtaget i henhold til databeskyttelsesrammen ⁽⁸⁴⁾.

- (55) I andre tilfælde af fjernelse, f.eks. frivillig udtræden eller manglende recertificering, skal organisationen enten slette eller tilbagesende oplysningerne, eller det kan beholde dem, hvis det hvert år bekræfter over for handelsministeriet, at det fortsat vil anvende principperne, eller sikrer en tilstrækkelig beskyttelse af personoplysningerne på anden godkendt vis (f.eks. ved hjælp af en aftale, der fuldt ud afspejler kravene i de relevante standardkontraktbestemmelser, som Kommissionen har godkendt) ⁽⁸⁵⁾. I dette tilfælde skal en organisation desuden udpege et kontaktpunkt i organisationen for alle spørgsmål relateret til EU-USA-databeskyttelsesrammen.

2.3.3 Identificering og håndtering af falske påstande om deltagelse

- (56) Handelsministeriet vil holde øje med falske påstande om deltagelse i EU-USA-databeskyttelsesrammen eller uretmæssig brug af certificeringsmærket for EU-USA-databeskyttelsesrammen, både ex officio og på grundlag af klager (f.eks. fremsendt af databeskyttelsesmyndigheder) ⁽⁸⁶⁾. Handelsministeriet vil navnlig løbende kontrollere, at organisationer, der i) trækker sig ud af EU-USA-databeskyttelsesrammen, ii) ikke foretager den årlige recertificering (dvs. som enten påbegyndte, men ikke afsluttede den årlige recertificeringsproces rettidigt, eller slet ikke påbegyndte den årlige recertificeringsproces), iii) fjernes fra listen over deltagere, navnlig for »vedvarende overtrædelse«, eller iv) ikke foretager den indledende certificering (dvs. som påbegyndte, men ikke afsluttede den første recertificeringsproces rettidigt), fjerner alle henvisninger til EU-USA-databeskyttelsesrammen fra alle relevante offentliggjorte politikker til beskyttelse af privatlivets fred, der lader formode, at organisationen fortsat deltager aktivt i databeskyttelsesrammen ⁽⁸⁷⁾. Handelsministeriet vil endvidere foretage internetsøgninger for at identificere henvisninger til EU-USA-databeskyttelsesrammen, herunder for at identificere falske påstande fremsat af organisationer, som aldrig har deltaget i EU-USA-databeskyttelsesrammen ⁽⁸⁸⁾.
- (57) Hvis ministeriet konstaterer, at henvisninger til EU-USA-databeskyttelsesrammen ikke er blevet fjernet eller bruges uretmæssigt, vil ministeriet underrette organisationen om, at det eventuelt vil henvise sagen til FTC/transportministeriet ⁽⁸⁹⁾. Hvis en organisation ikke reagerer på tilfredsstillende vis, henviser handelsministeriet sagen til den relevante myndighed med henblik på eventuelle håndhævelsesforanstaltninger ⁽⁹⁰⁾. En organisation, der afgiver urigtige oplysninger til offentligheden vedrørende dens tilslutning til principperne i form af vildledende udtalelser eller praksis, kan indbringes for FTC, transportministeriet eller andre relevante håndhævelsesmyndigheder i USA. Afgivelse af urigtige oplysninger til handelsministeriet kan håndhæves i henhold til False Statements Act (18 U.S.C. § 1001).

⁽⁸³⁾ I forbindelse med den anden årlige evaluering af privatlivsskjoldet oplyste handelsministeriet, at det havde foretaget stikprøvekontrol af 100 organisationer og fremsendt spørgeskemaer om overholdelse i 21 tilfælde (hvorefter de konstaterede problemer blev afhjulpet), jf. Kommissionens SWD(2018) 497 final, s. 9. Tilsvarende rapporterede handelsministeriet i forbindelse med den tredje årlige evaluering af privatlivsskjoldet, at det havde identificeret tre hændelser gennem sin overvågning af offentlige rapporter og var begyndt at foretage stikprøvekontrol af 30 virksomheder hver måned, hvilket havde ført til opfølgning med spørgeskemaer om overholdelse i 28 % af tilfældene (hvorefter de konstaterede problemer straks blev afhjulpet eller — i tre tilfælde — blev løst efter en advarselsskrivelse), jf. Kommissionens arbejdsdokument SWD(2019) 495 final, s. 8.

⁽⁸⁴⁾ Bilag I, afsnit III, punkt 11.g. En vedvarende overtrædelse af principperne forekommer navnlig, når en organisation nægter at rette sig efter en endelig afgørelse truffet af en uafhængig selvregulerende tvistbilæggelsesinstans med kompetence inden for beskyttelse af privatlivets fred eller af en håndhævelsesinstans.

⁽⁸⁵⁾ Bilag I, afsnit III, punkt 6.f.

⁽⁸⁶⁾ Bilag III, afsnittet »Søgning efter og håndtering af falske påstande om deltagelse i databeskyttelsesrammen«.

⁽⁸⁷⁾ *Ibid.*

⁽⁸⁸⁾ *Ibid.*

⁽⁸⁹⁾ *Ibid.*

⁽⁹⁰⁾ Under privatlivsskjoldet rapporterede handelsministeriet i forbindelse med den tredje årlige evaluering af rammen, at det havde identificeret 669 tilfælde af falske påstande om deltagelse (mellem oktober 2018 og oktober 2019), hvoraf de fleste blev afhjulpet efter handelsministeriets advarselsskrivelse, mens 143 sager blev henvist til FTC (jf. betragtning 62 nedenfor). Jf. Kommissionens SWD(2019) 495 final, s. 10.

2.3.4 Håndhævelse

- (58) For at garantere, at der også i praksis sikres et tilstrækkeligt niveau for databeskyttelse, skal der oprettes en uafhængig tilsynsmyndighed, der har beføjelser til at overvåge og håndhæve overholdelsen af databeskyttelsesreglerne.
- (59) Organisationer under EU-USA-databeskyttelsesrammen skal være underlagt de kompetente amerikanske myndigheds kompetence (FTC og transportministeriet), som har de nødvendige undersøgelses- og håndhævelsesbeføjelser til effektivt at sikre overholdelse af principperne ⁽⁹¹⁾.
- (60) FTC er en uafhængig myndighed bestående af fem kommissærer, som udnævnes af præsidenten efter råd fra Senatet og med dets samtykke ⁽⁹²⁾. Kommissærerne udnævnes for en syvårig periode og kan kun afsættes af præsidenten på grund af udelighed, tjenesteforsømmelse eller embedsmisbrug. FTC må ikke have mere end tre kommissærer fra samme politiske parti, og kommissærerne må under deres mandat ikke beskæftige sig med andre former for virksomhed, erhverv eller arbejde.
- (61) FTC kan undersøge overholdelsen af principperne samt falske påstande om tilslutning til principperne eller deltagelse i EU-USA-databeskyttelsesrammen fra organisationer, som enten ikke længere er opført på listen over deltagere i databeskyttelsesrammen eller aldrig har foretaget certificering ⁽⁹³⁾. FTC kan håndhæve overholdelsen ved at anmode om administrative eller føderale retsafgørelser (herunder »consent orders« (forligsafgørelser)) ⁽⁹⁴⁾ med henblik på foreløbige eller endelige forbud eller påbud eller andre afhjælpende foranstaltninger og vil systematisk overvåge overholdelsen af disse afgørelser ⁽⁹⁵⁾. Hvis en organisation ikke efterlever afgørelsen, kan FTC søge idømmelse af civilretlige sanktioner eller andre afhjælpende foranstaltninger, herunder for enhver skade som følge af den ulovlige adfærd. Enhver forligsafgørelse, der udstedes til en organisation under EU-USA-databeskyttelsesrammen, vil indeholde bestemmelser om selvrapportering ⁽⁹⁶⁾, og organisationerne vil blive anmodet om at offentliggøre alle afsnit relateret til databeskyttelsesrammen i alle overholdelses- eller vurderingsrapporter forelagt FTC. Endelig vil FTC føre en onlineliste over organisationer omfattet af FTC- eller retsafgørelser i sager om EU-USA-databeskyttelsesrammen ⁽⁹⁷⁾.
- (62) Med hensyn til privatlivsskjoldet traf FTC håndhævelsesforanstaltninger i ca. 22 sager, både i forbindelse med overtrædelser af specifikke krav under rammen (f.eks. manglende bekræftelse over for handelsministeriet af, at organisationen fortsat anvendte beskyttelsen under privatlivsskjoldet, efter at det havde forladt rammen, manglende kontrol — gennem selvevaluering eller eksternt kontrol af overholdelsen — af, at organisationen overholdt rammen) ⁽⁹⁸⁾ og falske påstande om deltagelse i rammen (f.eks. fra organisationer, der ikke fuldførte de nødvendige skridt for at opnå certificering eller lod deres certificering udløbe, men afgav urigtige oplysninger om deres fortsatte deltagelse i rammen) ⁽⁹⁹⁾. Disse håndhævelsesforanstaltninger var bl.a. et resultat af den proaktive brug af administrative pålæg til at indhente materiale fra visse deltagere i privatlivsskjoldet for at kontrollere, om der forelå væsentlige tilsidesættelser af forpligtelserne i privatlivsskjoldet ⁽¹⁰⁰⁾.

⁽⁹¹⁾ En organisation under EU-USA-databeskyttelsesrammen skal offentligt erklære sin tilslutning til principperne, offentliggøre sin politik til beskyttelse af privatlivets fred i overensstemmelse med principperne og fuldt ud implementere den. En overtrædelse af principperne kan retshåndhæves i henhold til Section 5 i FTC Act, der forbyder illoyal eller vildledende handelspraksis (15 U.S.C. § 45) og 49 U.S.C. § 41712, der forbyder transportører eller rejsebureauer at anvende en illoyal eller vildledende praksis i forbindelse med lufttransportydelser eller salg af lufttransportydelser.

⁽⁹²⁾ 15 U.S.C. § 41.

⁽⁹³⁾ Bilag IV.

⁽⁹⁴⁾ FTC er ifølge egne oplysninger ikke bemyndiget til at foretage kontrol på stedet inden for beskyttelse af privatlivets fred. Handelskommissionen har dog kompetence til at tvinge organisationer til at fremsende dokumenter og vidneudsagn (jf. Section 20 i FTC Act) og kan benytte sig af retssystemet til at få håndhævet sådanne afgørelser i tilfælde af manglende overholdelse.

⁽⁹⁵⁾ Jf. bilag IV, afsnittet »Anmodning om og overvågning af afgørelser«.

⁽⁹⁶⁾ Organisationer kan ved FTC- eller retsafgørelser pålægges at iværksætte programmer til beskyttelse af privatlivets fred og regelmæssigt forelægge overholdelsesrapporter eller uafhængige eksterne vurderinger af disse programmer for FTC.

⁽⁹⁷⁾ Bilag IV, afsnittet »Anmodning om og overvågning af afgørelser«.

⁽⁹⁸⁾ Kommissionens SWD(2019) 495 final, s. 11.

⁽⁹⁹⁾ Jf. de sager, der er opført på FTC's websted, på <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>. Jf. også Kommissionens SWD(2017) 344 final, s. 17, Kommissionens SWD(2018) 497 final, s. 12, og Kommissionens SWD(2019) 495 final, s. 11.

⁽¹⁰⁰⁾ Jf. f.eks. Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

- (63) Mere generelt har FTC i de seneste år truffet håndhævelsesforanstaltninger i en række sager vedrørende overholdelse af specifikke databeskyttelseskrav, der også er fastsat i EU-USA-databeskyttelsesrammen, f.eks. med hensyn til principperne om formålsbegrænsning og datalagring ⁽¹⁰¹⁾, dataminimering ⁽¹⁰²⁾, datasikkerhed ⁽¹⁰³⁾ og datanøjagtighed ⁽¹⁰⁴⁾.
- (64) Transportministeriet har enekompetence til at regulere luftfartsselskabernes databeskyttelsespraksis og deler kompetence med FTC for så vidt angår rejsebureauernes databeskyttelsespraksis i forbindelse med salg af lufttransporttydelser. Transportministeriets embedsmænd sigter først og fremmest mod at nå frem til et forlig og kan, hvis dette ikke er muligt, indlede en håndhævelsesprocedure, der omfatter bevishøring for en af ministeriets forvaltningsdommere, som er bemyndiget til at udstede forbud og idømme civile sanktioner ⁽¹⁰⁵⁾. Forvaltningsdommere er omfattet af flere beskyttelsesforanstaltninger i henhold til Administrative Procedure Act (APA) for at sikre deres uafhængighed og upartiskhed. De kan f.eks. kun afsættes med god grund, tildeles sager efter tur, må ikke udføre opgaver, der er uforenelige med deres pligter og ansvar som forvaltningsdommere, er ikke underlagt tilsyn af undersøgelsesholdet hos den myndighed, de er ansat af (i dette tilfælde transportministeriet), og de skal udøve deres dømmende/håndhævende funktion upartisk ⁽¹⁰⁶⁾. Transportministeriet har påtaget sig at overvåge håndhævelsesafgørelser og sikre, at afgørelser, der udstedes i sager om EU-USA-databeskyttelsesrammen, offentliggøres på dets websted ⁽¹⁰⁷⁾.

2.4 Klageadgang

- (65) Med henblik på at sikre tilstrækkelig beskyttelse og navnlig håndhævelse af individuelle rettigheder bør den registrerede have effektive muligheder for administrativ og retslig prøvelse.
- (66) I henhold til *princippet om klageadgang, håndhævelse og ansvar* inden for rammerne af EU-USA-databeskyttelsesrammen skal organisationer give fysiske personer, der er berørt af manglende overholdelse, mulighed for at klage, dvs. give registrerede i EU mulighed for at indgive klager vedrørende organisationer i EU-USA-databeskyttelsesrammens manglende overholdelse og om nødvendigt få disse klager afgjort ved en afgørelse om effektive afhjælpende foranstaltninger ⁽¹⁰⁸⁾. Som led i deres certificering skal organisationer opfylde kravene i dette princip ved at sørge for effektive og let tilgængelige uafhængige klageinstanser, som kan undersøge og finde en hurtig løsning på klager fra fysiske personer eller eventuelle tvister, uden ekstra omkostninger for den pågældende ⁽¹⁰⁹⁾.

⁽¹⁰¹⁾ Se f.eks. FTC's afgørelse i Drizly, LLC., der bl.a. kræver, at virksomheden 1) destruerer personoplysninger, som den har indsamlet, og som ikke er nødvendige for, at den kan levere produkter eller tjenesteydelser til forbrugere, 2), afholder sig fra at indsamle eller lagre personoplysninger, medmindre det er nødvendigt til specifikke formål, der er beskrevet i en opbevaringsplan.

⁽¹⁰²⁾ Se f.eks. FTC's afgørelse i CafePress (24. marts 2022), der bl.a. kræver, at den mængde data, der indsamles, minimeres.

⁽¹⁰³⁾ Se f.eks. FTC's håndhævelsesforanstaltninger i Drizzly, LLC og CafePress, hvor den krævede, at de relevante virksomheder skulle indføre et særligt sikkerhedsprogram eller specifikke sikkerhedsforanstaltninger. For så vidt angår brud på datasikkerheden, se desuden FTC's afgørelse af 27. januar 2023 i Chegg, forliget med Equifax i 2019 (<https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>).

⁽¹⁰⁴⁾ Se f.eks. sagen om RealPage, Inc (16. oktober 2018), hvor FTC traf håndhævelsesforanstaltninger i henhold til FCRA over for en virksomhed, der screener lejere, og som fremlagde baggrundsrapporter om enkeltpersoner til ejendomssejere og ejendomsadministrationsselskaber baseret på oplysninger fra udlejningshistorier, oplysninger fra offentlige registre (herunder tidligere lovovertrædelser og udsættelser) og kreditoplysninger, der blev anvendt som en faktor ved afgørelsen af, om lejer var berettiget til boligen. FTC fandt, at virksomheden ikke havde truffet rimelige foranstaltninger til at sikre nøjagtigheden af de oplysninger, den fremlagde på grundlag af sit automatiske beslutningsværktøj.

⁽¹⁰⁵⁾ Jf. bilag V, afsnittet »Håndhævelsespraksis«.

⁽¹⁰⁶⁾ Jf. 5 U.S.C. § 3105, 7521(a), 554(d) og 556(b)(3).

⁽¹⁰⁷⁾ Bilag V, jf. afsnittet »Overvågning og offentliggørelse af håndhævelsesafgørelser vedrørende overtrædelser af EU-USA-databeskyttelsesrammen«.

⁽¹⁰⁸⁾ Bilag I, afsnit II, punkt 7.

⁽¹⁰⁹⁾ Bilag I, afsnit III, punkt 11.

- (67) Organisationer kan vælge at benytte uafhængige klageinstanser i enten EU eller i USA. Som forklaret nærmere i betragtning 73 omfatter dette også muligheden for frivilligt at forpligte sig til at samarbejde med databeskyttelsesmyndighederne i EU. Når organisationerne behandler oplysninger om menneskelige ressourcer, er det obligatorisk at samarbejde med databeskyttelsesmyndighederne i EU. Andre alternativer er udenretslig tvistbilæggelse eller programmer til beskyttelse af privatlivets fred udviklet i den private sektor, som principperne indarbejdes i. Disse programmer skal omfatte effektive håndhævelsesmekanismer i overensstemmelse med kravene i *princippet om klageadgang, håndhævelse og ansvar*.
- (68) EU-USA-databeskyttelsesrammen giver således de registrerede en række muligheder for at udøve deres rettigheder, indgive klager vedrørende organisationer i EU-USA-databeskyttelsesrammens manglende overholdelse og om nødvendigt at få klagerne afgjort ved en afgørelse om effektive afhjælpende foranstaltninger. Fysiske personer kan indbringe en klage direkte til en organisation, til en uafhængig tvistbilæggesinstans, der er udpeget af organisationen, til de nationale databeskyttelsesmyndigheder, til handelsministeriet eller til FTC. Hvis deres klager ikke afgøres ved hjælp af disse klage- eller håndhævelsesmekanismer, kan fysiske personer indbringe sagen til tvungen voldgift (bilag I til bilag I til denne afgørelse). Med undtagelse af indbringelse for voldgiftspanelet, der kræver, at visse andre retsmidler først skal være udtømt, kan fysiske personer frit vælge at benytte enhver af eller alle disse mekanismer og er ikke forpligtet til at vælge en bestemt mekanisme frem for en anden eller til at følge en bestemt rækkefølge.
- (69) For det første kan registrerede i EU rette klager vedrørende manglende overholdelse af principperne direkte til organisationerne under EU-USA-databeskyttelsesrammen⁽¹¹⁰⁾. Organisationen skal indføre en effektiv klagemekanisme til behandling af disse klager for at fremme en løsning. En organisations politik til beskyttelse af privatlivets fred skal derfor indeholde klare oplysninger til fysiske personer om et kontaktpunkt i eller uden for organisationen, der behandler klagerne (herunder ethvert relevant organ i EU, som kan besvare forespørgsler eller klager), og oplysninger om den udpegede uafhængige tvistbilæggesinstans (jf. betragtning 70). Ved modtagelsen af en klage fra en fysisk person, enten direkte fra personen selv eller via handelsministeriet, som har fået sagen henvist fra en databeskyttelsesmyndighed, skal organisationen fremsende et svar til den registrerede i EU inden for 45 dage⁽¹¹¹⁾. Organisationerne skal ligeledes straks besvare henvendelser og andre anmodninger om oplysninger fra handelsministeriet eller en databeskyttelsesmyndighed⁽¹¹²⁾ (hvis organisationen har forpligtet sig til at samarbejde med databeskyttelsesmyndighederne) vedrørende deres tilslutning til principperne.
- (70) For det andet kan fysiske personer ligeledes indgive klagen direkte til den uafhængige tvistbilæggesinstans (enten i USA eller i EU), der er udpeget af en organisation til at undersøge og afgøre individuelle klager (medmindre klagerne tydeligt er ubegrundede eller useriøse) og sikre fysiske personer passende gratis klageadgang⁽¹¹³⁾. De sanktioner og afhjælpende foranstaltninger, der pålægges af denne instans, skal være af en sådan karakter, at organisationerne tilskyndes til at overholde principperne, og de bør sikre, at organisationen imødegår eller afhjælper følgerne af den manglende overholdelse og, afhængigt af omstændighederne, at den videre behandling af de pågældende personoplysninger indstilles, eller at oplysningerne slettes, og at konstateringerne af manglende overholdelse offentliggøres⁽¹¹⁴⁾. De uafhængige tvistbilæggesinstanser, der udpeges af en organisation, skal angive relevante oplysninger om EU-USA-databeskyttelsesrammen og om de tjenester, de tilbyder i tilknytning hertil, på deres offentlige websteder⁽¹¹⁵⁾. De skal hvert år offentliggøre en årlig rapport med en samlet statistik over disse tjenester⁽¹¹⁶⁾.

⁽¹¹⁰⁾ Bilag I, afsnit III, punkt 11.d., nr. i.

⁽¹¹¹⁾ Bilag I, afsnit III, punkt 11.d., nr. i.

⁽¹¹²⁾ Den myndighed, der er blevet udpeget af panelet af databeskyttelsesmyndigheder til at behandle sagerne, i overensstemmelse med det supplerende princip »Databeskyttelsesmyndighedernes rolle« (bilag I, afsnit III, punkt 5).

⁽¹¹³⁾ Bilag I, afsnit III, punkt 11.d.

⁽¹¹⁴⁾ Bilag I, afsnit II, punkt 7, og afsnit III, punkt 11.e.

⁽¹¹⁵⁾ Bilag I, afsnit III, punkt 11.d., nr. ii.

⁽¹¹⁶⁾ Den årlige rapport skal indeholde oplysninger om: 1) det samlede antal klager relateret til EU-USA-databeskyttelsesrammen modtaget i rapporteringsåret, 2) typen af modtagne klager, 3) kvalitetsmål for tvistbilæggelse såsom klagebehandlingstid og 4) resultaterne af de modtagne klager, navnlig antal og typer af pålagte foranstaltninger eller sanktioner.

- (71) Handelsministeriet kan som led i sin kontrol af overholdelsen ligeledes kontrollere, om organisationer under EU-USA-databeskyttelsesrammen rent faktisk har ladet sig registrere ved den uafhængige klageinstans, som de påstår at have registreret sig ved ⁽¹¹⁷⁾. Både organisationerne og de ansvarlige uafhængige klageinstanser skal straks besvare forespørgsler og anmodninger fra handelsministeriet om oplysninger vedrørende EU-USA-databeskyttelsesrammen. Handelsministeriet vil samarbejde med de uafhængige klageinstanser for at kontrollere, at de lægger oplysninger ud på deres websteder om principperne og de tjenester, de tilbyder i henhold til EU-USA-databeskyttelsesrammen, og at de offentliggør årlige rapporter ⁽¹¹⁸⁾.
- (72) I tilfælde, hvor organisationen ikke følger et tvistbilægelsesorgans eller et selvregulerende organs afgørelse, skal disse indberette den manglende overholdelse til handelsministeriet og FTC (eller en anden amerikansk myndighed med kompetence til at undersøge organisationens manglende overholdelse) eller til en kompetent domstol ⁽¹¹⁹⁾. Hvis en organisation nægter at følge et selvregulerende organs, et uafhængigt tvistbilægelsesorgans eller et statsligt organs endelige afgørelse, eller hvis et sådant organ fastslår, at en organisation regelmæssigt overtræder principperne, kan dette blive betragtet som en vedvarende overtrædelse med det resultat, at handelsministeriet, efter at have givet den pågældende organisation 30 dages varsel og mulighed for at fremsætte bemærkninger, fjerner organisationen fra listen over deltagere i databeskyttelsesrammen ⁽¹²⁰⁾. Hvis organisationen efter at være blevet fjernet fra listen fastholder påstande om deltagelse i EU-USA-databeskyttelsesrammen, henviser ministeriet det til FTC eller en anden retshåndhævende myndighed ⁽¹²¹⁾.
- (73) For det tredje kan enkeltpersoner også indgive deres klager til en national databeskyttelsesmyndighed i Unionen, som kan gøre brug af deres undersøgelsesbeføjelser og afhjælpende beføjelser i henhold til forordning (EU) 2016/679. Organisationer er forpligtede til at samarbejde med databeskyttelsesmyndigheden i forbindelse med undersøgelsen og afgørelsen af klager, enten når det drejer sig om behandling af oplysninger om menneskelige ressourcer, der er indsamlet i forbindelse med ansættelsesforhold, eller når den pågældende organisation frivilligt har underlagt sig databeskyttelsesmyndighedernes tilsyn ⁽¹²²⁾. Organisationerne skal navnlig besvare forespørgsler, rette sig efter databeskyttelsesmyndighedens anbefalinger, herunder om afhjælpende eller kompenserende foranstaltninger, og give databeskyttelsesmyndigheden en skriftlig bekræftelse på, at disse foranstaltninger er truffet ⁽¹²³⁾. I tilfælde af manglende overholdelse af databeskyttelsesmyndighedens rådgivning vil databeskyttelsesmyndigheden henvise sådanne sager til handelsministeriet (som kan fjerne organisationer fra EU-USA-databeskyttelsesrammens liste) eller, med henblik på eventuelle håndhævelsesforanstaltninger, til FTC eller transportministeriet (manglende samarbejde med databeskyttelsesmyndighederne eller overholdelse af principperne kan anfægtes i henhold til amerikansk lovgivning) ⁽¹²⁴⁾.
- (74) For at fremme samarbejdet om effektiv behandling af klager har både handelsministeriet og FTC udpeget et særligt kontaktpunkt, der skal fungere som bindeled direkte til databeskyttelsesmyndighederne ⁽¹²⁵⁾. Disse kontaktpunkter hjælper databeskyttelsesmyndigheden med at besvare forespørgsler om en organisations overholdelse af principperne.
- (75) Databeskyttelsesmyndighedernes anbefalinger ⁽¹²⁶⁾ afgives, når begge parter i sagen har haft passende mulighed for at fremsætte bemærkninger og fremlægge eventuel dokumentation, som de finder relevant. Panelet kan afgive sine anbefalinger så hurtigt som muligt under hensyntagen til kravet om behørig behandling og som hovedregel senest 60 dage efter modtagelse af klagen ⁽¹²⁷⁾. Hvis en organisation ikke har rettet sig efter en anbefaling senest 25 dage efter anbefalingens afgivelse og ikke har givet en tilfredsstillende forklaring på denne forsinkelse, kan panelet meddele, at det agter at indbringe sagen for FTC (eller et andet kompetent amerikansk retshåndhævende organ) eller

⁽¹¹⁷⁾ Bilag I, afsnittet »Kontrol af selvcertificeringskrav«.

⁽¹¹⁸⁾ Jf. bilag III, afsnittet »Lettelse af samarbejdet med alternative tvistbilægelsesorganer, der tilbyder principrelaterede tjenester«. Jf. ligeledes bilag I, afsnit III, punkt 11.d., nr. ii-iii.

⁽¹¹⁹⁾ Jf. bilag I, afsnit III, punkt 11.e.

⁽¹²⁰⁾ Jf. bilag I, afsnit III, punkt 11.g, særlig nr. ii og iii.

⁽¹²¹⁾ Jf. bilag III, afsnittet »Søgning efter og håndtering af falske påstande om deltagelse i databeskyttelsesrammen«.

⁽¹²²⁾ Bilag I, afsnit II, punkt 7.b.

⁽¹²³⁾ Bilag I, afsnit III, punkt 5.

⁽¹²⁴⁾ Bilag I, afsnit III, punkt 5.c., nr. ii.

⁽¹²⁵⁾ Bilag III (jf. afsnittet »Fremme af samarbejdet med databeskyttelsesmyndighederne«) og bilag IV (jf. afsnittet »Prioritering af henviste sager og undersøgelser« og »Håndhævelsessamarbejde med EU's databeskyttelsesmyndigheder«).

⁽¹²⁶⁾ Databeskyttelsesmyndighederne bør fastlægge forretningsordenen for det uformelle panel på grundlag af deres kompetence til at tilrettelægge deres arbejde og samarbejde med hinanden.

⁽¹²⁷⁾ Bilag I, afsnit III, punkt 5.c., nr. i.

at konkludere, at der er sket en væsentlig overtrædelse af samarbejdsaftalen. I det første tilfælde kan det føre til håndhævelsesforanstaltninger i henhold til Section 5 i FTC Act (eller tilsvarende lov) ⁽¹²⁸⁾. I det andet tilfælde vil panelet underrette handelsministeriet, der vil betragte organisationens afslag på at efterkomme panelet af databeskyttelsesmyndighedens anbefalinger som en vedvarende overtrædelse, der indebærer, at organisationen fjernes fra listen over deltagere i databeskyttelsesrammen.

- (76) Hvis den databeskyttelsesmyndighed, som har modtaget en klage, ikke har truffet eller har truffet utilstrækkelige foranstaltninger vedrørende klagen, har den enkelte klager mulighed for at indbringe sagen for de nationale domstole i den pågældende EU-medlemsstat.
- (77) Fysiske personer kan også indgive klager til databeskyttelsesmyndighederne, selv om organisationen ikke har udpeget panelet som tvistbilæggesinstans. I disse tilfælde kan databeskyttelsesmyndigheden henvise klagen til enten handelsministeriet eller FTC. For at fremme og styrke samarbejdet om spørgsmål relateret til individuelle klager og manglende overholdelse fra deltagere i EU-USA-databeskyttelsesrammens side vil handelsministeriet udpege et særligt kontaktpunkt, der skal agere bindeled og hjælpe med at besvare forespørgsler om en organisations overholdelse af principperne ⁽¹²⁹⁾. Tilsvarende har FTC forpligtet sig til at udpege et særligt kontaktpunkt ⁽¹³⁰⁾.
- (78) For det fjerde har handelsministeriet forpligtet sig til at modtage, gennemgå og gøre sit yderste for at behandle klager om en organisations manglende overholdelse af principperne ⁽¹³¹⁾. Handelsministeriet har i den forbindelse indført særlige procedurer, som databeskyttelsesmyndighederne skal følge ved henvisning af klager til et særligt kontaktpunkt, sporing af klagerne og opfølgning over for organisationerne for at fremme en løsning ⁽¹³²⁾. For at fremskynde behandlingen af individuelle klager tager kontaktpunktet direkte kontakt til den pågældende databeskyttelsesmyndighed i tilfælde af problemer med overholdelsen og underretter navnlig myndigheden om status for klagerne senest 90 dage efter henvisningen ⁽¹³³⁾. Dette giver registrerede mulighed for at indgive klager over organisationer under EU-USA-databeskyttelsesrammen, der ikke overholder principperne, direkte til deres nationale databeskyttelsesmyndighed og få dem kanaliseret videre til handelsministeriet, der er den amerikanske myndighed, som forvalter EU-USA-databeskyttelsesrammen.
- (79) Hvis handelsministeriet på grundlag af sin ex officio-kontrol, klager eller andre oplysninger konkluderer, at en organisation vedvarende overtræder principperne, kan det fjerne organisationen fra listen over deltagere i databeskyttelsesrammen ⁽¹³⁴⁾. Hvis en organisation nægter at rette sig efter den endelige afgørelse truffet af en uafhængig selvregulerende tvistbilæggesinstans med kompetence inden for beskyttelse af privatlivets fred eller af en statslig instans, herunder en databeskyttelsesmyndighed, vil det blive betragtet som en vedvarende overtrædelse af principperne ⁽¹³⁵⁾.
- (80) For det femte skal en organisation i EU-USA-databeskyttelsesrammen være underlagt de amerikanske myndigheders, og navnlig FTC's, kompetence ⁽¹³⁶⁾, idet de har de undersøgelses- og håndhævelsesbeføjelser, som er nødvendige for effektivt at sikre overholdelsen af principperne. FTC prioriterer sager om manglende overholdelse af principperne, der henvises fra uafhængige tvistbilæggesorganer eller selvregulerende organer, handelsministeriet og databeskyttelsesmyndighederne (der handler på eget initiativ eller på grundlag af klager) for at bestemme, om Section 5 i FTC Act er blevet overtrådt ⁽¹³⁷⁾. FTC har forpligtet sig til at indføre en standardiseret henvisningsprocedure, til at udpege et kontaktpunkt for henvisninger fra databeskyttelsesmyndighederne og til at udveksle oplysninger om henvisninger. Derudover kan FTC tage imod klager direkte fra fysiske personer og på eget initiativ foretage undersøgelser relateret til EU-USA-databeskyttelsesrammen, navnlig som led i sine mere generelle undersøgelser af forhold vedrørende beskyttelse af privatlivets fred.

⁽¹²⁸⁾ Bilag I, afsnit III, punkt 5.c., nr. ii.

⁽¹²⁹⁾ Jf. bilag III, afsnittet »Fremme af samarbejdet med databeskyttelsesmyndighederne«.

⁽¹³⁰⁾ Jf. bilag IV, afsnittet »Prioritering af henviste sager og undersøgelser« og »Håndhævelsessamarbejde med EU's databeskyttelsesmyndigheder«.

⁽¹³¹⁾ Bilag III, jf. f.eks. afsnittet »Fremme af samarbejdet med databeskyttelsesmyndighederne«.

⁽¹³²⁾ Bilag I, afsnit II, punkt 7.e, og bilag III, afsnittet »Fremme af samarbejdet med databeskyttelsesmyndighederne«.

⁽¹³³⁾ *Ibid.*

⁽¹³⁴⁾ Bilag I, afsnit III, punkt 11.g.

⁽¹³⁵⁾ Bilag I, afsnit III, punkt 11.g.

⁽¹³⁶⁾ En organisation under EU-USA-databeskyttelsesrammen skal offentligt erklære sin tilslutning til principperne, offentliggøre sin politik til beskyttelse af privatlivets fred i overensstemmelse med principperne og fuldt ud implementere den. En overtrædelse af principperne kan retshåndhæves i henhold til Section 5 i FTC Act, der forbyder illoyal eller vildledende handelspraksis.

⁽¹³⁷⁾ Jf. ligeledes de tilsvarende forpligtelser, som transportministeriet har påtaget sig, i bilag V.

- (81) Hvis en klage fra en fysisk person ikke er blevet afgjort på tilfredsstillende vis via de andre tilgængelige klagemuligheder, kan den registrerede i EU for det sjette som en sidste udvej indbringe sagen for »panelet i EU-USA-databeskyttelsesrammen« med henblik på tvungen voldgift ⁽¹³⁸⁾. Organisationer skal informere de registrerede om muligheden for at indbringe sagen til tvungen voldgift, og de er forpligtede til at reagere, når en registreret benytter sig af denne mulighed og retter henvendelse til den berørte organisation ⁽¹³⁹⁾.
- (82) Panelet i EU-USA-databeskyttelsesrammen består af en pulje af mindst ti voldgiftsmænd udpeget af det amerikanske handelsministerium og Kommissionen på grundlag af deres uafhængighed, integritet samt erfaring med USA's og EU's databeskyttelsesregler. I forbindelse med de enkelte tvister skal parterne sammensætte et panel med en eller tre ⁽¹⁴⁰⁾ voldgiftsmænd fra denne pulje.
- (83) Handelsministeriet har udvalgt International Centre for Dispute Resolution (ICDR), den internationale afdeling af American Arbitration Association (AAA), til at forvalte voldgiftssager. Proceduren ved panelet for EU-USA-databeskyttelsesrammen vil være underlagt en række godkendte voldgiftsregler og en adfærdskodeks for de udpegede voldgiftsmænd. ICDR-AAA's websted indeholder klare og kortfattede oplysninger til fysiske personer om voldgiftsordningen og proceduren for indgivelse af voldgiftssager.
- (84) De voldgiftsregler, der er fastlagt af handelsministeriet og Kommissionen, supplerer EU-USA-databeskyttelsesrammen, der indeholder flere elementer, som giver registrerede i EU større mulighed for at anvende denne ordning, bl.a. i) kan den registrerede få hjælp af sin nationale databeskyttelsesmyndighed til at fremsætte en klage for panelet, ii) har den registrerede i EU mulighed for at deltage i voldgiftsbehandlingen, som foregår i USA, via video- eller telekonference uden ekstra omkostninger for den registrerede, iii) vil voldgiftsproceduren som regel foregå på engelsk, men den registrerede vil på begrundet anmodning normalt have adgang til tolkning under voldgiftsbehandlingen og oversættelser uden ekstra omkostninger for den registrerede, iv) og endelig skal hver part afholde egne omkostninger til advokatsalær, hvis parten møder ved advokat for panelet, men handelsministeriet vil etablere en fond finansieret via årlige bidrag fra organisationerne i EU-USA-databeskyttelsesrammen, som skal dække voldgiftsomkostningerne op til maksimumsbeløb, der skal fastlægges af de amerikanske myndigheder i samråd med Kommissionen ⁽¹⁴¹⁾.
- (85) Panelet i EU-USA-databeskyttelsesrammen har beføjelse til at give rimelig individuel ikkepengemæssig oprejsning ⁽¹⁴²⁾ (»individual-specific, non-monetary equitable relief«) for at afhjælpe overtrædelsen af principperne. Selv om panelet tager højde for andre afhjælpende foranstaltninger, der allerede er iværksat gennem andre mekanismer i EU-USA-databeskyttelsesrammen, når det træffer sin afgørelse, kan den enkelte stadig vælge at få sagen afgjort ved voldgift, hvis den pågældende mener, at disse andre retsmidler er utilstrækkelige. Det giver registrerede i EU mulighed for at kræve sagen afgjort ved voldgift, hver gang de tiltag, som organisationerne under EU-USA-databeskyttelsesrammen, de uafhængige klageinstanser eller de kompetente amerikanske myndigheder (f. eks. FTC) har (eller ikke har) iværksat, ikke har ført til en tilfredsstillende afgørelse af deres klager. Der kan ikke stilles krav om voldgift, hvis en databeskyttelsesmyndighed har retligt grundlag for at afgøre den pågældende klage over organisationen under EU-USA-databeskyttelsesrammen, nemlig i de sager, hvor organisationen enten er forpligtet til at samarbejde med og rette sig efter databeskyttelsesmyndighedernes anbefalinger om behandling af personoplysninger om menneskelige ressourcer, der indsamles inden for rammerne af et ansættelsesforhold, eller hvis de frivilligt har forpligtet sig til at gøre dette. Fysiske personer kan få fuldbyrdet voldgiftsavgørelser ved de amerikanske domstole i henhold til Federal Arbitration Act, som således sikrer effektive retsmidler i tilfælde af, at en organisation ikke overholder principperne.

⁽¹³⁸⁾ Jf. bilag I til bilag I, »Voldgiftsmodel«.

⁽¹³⁹⁾ Jf. bilag I, afsnit II, punkt 1.a., nr. xi, og afsnit II, punkt 7.c.

⁽¹⁴⁰⁾ Parterne skal nå til enighed om antallet af voldgiftsmænd i panelet.

⁽¹⁴¹⁾ Bilag I til bilag I, afsnit G.6.

⁽¹⁴²⁾ Registrerede kan ikke kræve erstatning i voldgiftssager, men selv om de kræver voldgift, har de fortsat mulighed for at søge erstatning ved de almindelige amerikanske domstole.

- (86) For det syvende findes der i tilfælde af en organisations manglende overholdelse af principperne og af dens offentliggjorte politik til beskyttelse af privatlivets fred andre muligheder for retslig prøvelse i de enkelte amerikanske staters lovgivning, herunder for at opnå skadeserstatning. Personer kan f.eks. på visse betingelser opnå domstolsprøvelse (herunder skadeserstatning) i henhold til en stats forbrugerlovgivning i tilfælde af svigagtig afgivelse af urigtige oplysninger, illoyal eller vildledende praksis ⁽¹⁴³⁾ og i henhold til erstatningsretten (navnlig i tilfælde af krænkelse af privatlivets fred ⁽¹⁴⁴⁾, tilegnelse af navn eller lignende ⁽¹⁴⁵⁾ og offentliggørelse af private forhold ⁽¹⁴⁶⁾).
- (87) Tilsammen sikrer de forskellige klagemuligheder, der er beskrevet ovenfor, at alle klager over certificerede organisationers manglende overholdelse af EU-USA-databeskyttelsesrammen effektivt vil blive afgjort og afhjulpet.

3. DE AMERIKANSKE MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER OVERFØRT FRA EU

- (88) Kommissionen har også vurderet begrænsningerne og garantierne, herunder tilsynet og de enkelte prøvelsesmekanismer, i amerikansk ret i forbindelse med amerikanske offentlige myndigheders indsamling og efterfølgende anvendelse af personoplysninger, der er blevet overført til dataansvarlige og databehandlere i USA i offentlighedens interesse, navnlig med henblik på strafferetlig håndhævelse og til nationale sikkerhedsformål (myndighedsadgang) ⁽¹⁴⁷⁾. Ved vurderingen af, om de betingelser, hvorunder myndighedsadgangen til oplysninger, der overføres til USA i medfør af denne afgørelse, opfylder »væsentlighedskriteriet« i henhold til artikel 45, stk. 1, i forordning (EU) 2016/679, som fortolket af Domstolen i lyset af chartret om grundlæggende rettigheder, har Kommissionen taget hensyn til flere kriterier.
- (89) Navnlig skal enhver begrænsning af retten til beskyttelse af personoplysninger være fastlagt i lovgivningen, og det retsgrundlag, som tillader et indgreb i disse rettigheder, skal selv definere rækkevidden af begrænsningen af udøvelsen af den pågældende rettighed ⁽¹⁴⁸⁾. For at opfylde kravet om proportionalitet, ifølge hvilket undtagelserne fra og begrænsningerne af beskyttelsen af personoplysninger skal holdes inden for det, der i et demokratisk samfund er strengt nødvendigt for at opfylde specifikke mål af almen interesse svarende til dem, der er anerkendt af Unionen, skal dette retsgrundlag fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning, og som opstiller en række mindstekrav, således at de personer, hvis data er blevet overført, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personoplysninger mod risikoen for misbrug ⁽¹⁴⁹⁾. Desuden skal disse regler og garantier være juridisk bindende og kunne håndhæves af

⁽¹⁴³⁾ Jf. f.eks. statens forbrugerbeskyttelseslovgivning i Californien (Cal. Civ. Code § 1750-1785 (West) Consumers Legal Remedies Act), District of Columbia (D.C. Code § 28-3901), Florida (Fla. Stat. § 501.201-501.213, Deceptive and Unfair Trade Practices Act), Illinois (815 Ill. Comp. Stat. 505/1-505/12, Consumer Fraud and Deceptive Business Practices Act), Pennsylvania (73 Pa. Stat. Ann. § 201-1 — 201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

⁽¹⁴⁴⁾ Dvs. i tilfælde af et forsægtigt indgreb i en persons private sager eller anliggender på en måde, der ville være særdeles krænkende for en fornuftig person (Restatement (2nd) of Torts, § 652(b)).

⁽¹⁴⁵⁾ Almindeligvis i tilfælde af tilegnelse og brug af en persons navn eller lignende til at reklamere for en virksomhed eller et produkt eller til et lignende kommercielt formål (jf. Restatement (2nd) of Torts, § 652C).

⁽¹⁴⁶⁾ Dvs. når oplysninger om en persons privatliv offentliggøres, og dette er særdeles krænkende for en fornuftig person, og oplysningerne ikke er af legitim interesse for offentligheden (Restatement (2nd) of Torts, § 652D).

⁽¹⁴⁷⁾ Dette er også relevant i lyset af bilag I, afsnit I, punkt 5. I henhold til dette afsnit og i lighed med databeskyttelsesforordningen kan overholdelse af databeskyttelseskrav og rettigheder, der er en del af principperne om beskyttelse af privatlivets fred, være underlagt begrænsninger. Sådanne begrænsninger er imidlertid ikke absolutte, men kan kun påberåbes på flere betingelser, f.eks. i det omfang det er nødvendigt for at efterkomme en retskendelse eller opfylde almene hensyn, retshåndhævelse eller nationale sikkerhedskrav. I denne forbindelse og af klarhedshensyn henvises der i dette afsnit også til de betingelser, der er fastsat i EO 14086, og som vurderes i blandt andet betragtning 127-141.

⁽¹⁴⁸⁾ Jf. *Schrems II*, præmis 174-175 og den deri nævnte retspraksis. Jf. ligeledes sag C-623/17, *Privacy International*, ECLI:EU:C:2020:790, præmis 65, for så vidt angår adgang for medlemsstaternes offentlige myndigheder, og forenede sager C-511/18, C-512/18 og C-520/18, *La Quadrature du Net m.fl.*, ECLI:EU:C:2020:791, præmis 175.

⁽¹⁴⁹⁾ Jf. *Schrems II*, præmis 176 og 181 og den deri nævnte retspraksis. Jf. ligeledes *Privacy International*, præmis 68, for så vidt angår adgang for medlemsstaternes offentlige myndigheder, og *La Quadrature du Net m.fl.*, præmis 132.

retssubjekter ⁽¹⁵⁰⁾. De registrerede skal navnlig have mulighed for at anlægge sag ved en uafhængig og upartisk domstol med henblik på at få adgang til deres personoplysninger eller for at få sådanne oplysninger berigtiget eller slettet ⁽¹⁵¹⁾.

3.1 Amerikanske offentlige myndigheders adgang til og anvendelse af oplysninger med henblik på strafferetlig håndhævelse

- (90) Med hensyn til indgreb i personoplysninger overført under EU-USA-databeskyttelsesrammen med henblik på strafferetlig håndhævelse, indfører USA's lovgivning en række begrænsninger i adgangen til og anvendelsen af personoplysninger og indeholder tilsyns- og klagemekanismer, som er i overensstemmelse med de krav, der er omhandlet i betragtning 89 til denne afgørelse. De betingelser, hvorunder en sådan adgang kan finde sted, og de garantier, der gælder for udøvelsen af disse beføjelser, vurderes nærmere i de følgende afsnit. I denne forbindelse har den amerikanske regering (gennem det amerikanske justitsministerium) ligeledes givet sikkerhed for de gældende begrænsninger og garantier (bilag VI til denne afgørelse).

3.1.1 Retsgrundlag, begrænsninger og garantier

3.1.1.1 Begrænsninger og garantier med hensyn til indsamling af personoplysninger med henblik på strafferetlig håndhævelse

- (91) Amerikanske forbundsanklagere og føderale efterforskningsagenter kan få adgang til personoplysninger, der behandles af certificerede amerikanske organisationer, og som er overført fra EU på grundlag af EU-USA-databeskyttelsesrammen, med henblik på strafferetlig håndhævelse i henhold til forskellige procedurer, som forklaret nærmere i betragtning 92-99. Disse procedurer gælder på samme måde, når der indhentes oplysninger fra en hvilken som helst amerikansk organisation, uanset de pågældende registreredes nationalitet eller opholdssted ⁽¹⁵²⁾.
- (92) For det første kan en dommer efter anmodning fra en føderal retshåndhævelsesembedsmand eller en regeringsadvokat udstede en kendelse om ransagnings eller beslaglæggelse (herunder af elektronisk lagrede oplysninger) ⁽¹⁵³⁾. En sådan kendelse kan kun udstedes, hvis der er begrundet mistanke (»probable cause«) ⁽¹⁵⁴⁾ om, at der sandsynligvis kan findes genstande, der kan beslaglægges (»seizable items«) (bevis for en forbrydelse, genstande, som en person er i ulovlig besiddelse af, eller ejendele, der er designet eller beregnet til eller brugt til at begå en forbrydelse), på det sted, der er angivet i kendelsen. I kendelsen skal de ejendele eller genstande, der skal beslaglægges, identificeres, og den dommer, som kendelsen skal tilbageleveres til, skal angives. En person, der er

⁽¹⁵⁰⁾ Jf. *Schrems II*, præmis 181-182.

⁽¹⁵¹⁾ Jf. *Schrems I*, præmis 95, og *Schrems II*, præmis 194. I den forbindelse har EU-Domstolen navnlig understreget, at overholdelsen af artikel 47 i chartret om grundlæggende rettigheder, der garanterer retten til effektive retsmidler ved en uafhængig og upartisk domstol, ligeledes bidrager til »det i Unionen krævede beskyttelsesniveau, som Kommissionen skal fastslå er overholdt, før den vedtager en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til databeskyttelsesforordningens artikel 45, stk. 1« (*Schrems II*, præmis 186).

⁽¹⁵²⁾ Jf. bilag VI. Jf. f.eks. med hensyn til Wiretap Act, Stored Communications Act og Pen Register Act (nævnt mere udførligt i betragtning 95-98), *Suzlon Energy Ltd v. Microsoft Corp.*, 671 F.3d 726, 729 (9th Cir. 2011).

⁽¹⁵³⁾ Federal Rules of Criminal Procedure, 41. I en dom fra 2018 bekræftede Supreme Court, at der også kræves en ransagningskendelse eller en fritagelse herfra for, at de retshåndhævende myndigheder kan få adgang til historiske registreringer af mobiltelefoners lokationer, som giver et samlet overblik over en brugers færden, og at brugeren kan have en rimelig forventning om privatlivets fred med hensyn til sådanne oplysninger (*Timothy Ivory Carpenter v. United States of America*, nr. 16-402, 585 U.S. (2018)). Som følge heraf kan sådanne oplysninger generelt ikke indhentes fra et mobiltelefonselskab på grundlag af en retsafgørelse, som er afsagt, fordi der er rimelig grund til at antage, at oplysningerne er relevante og væsentlige for en igangværende strafferetlig efterforskning, men kræver, at det påvises, at der foreligger en begrundet mistanke, når der anvendes en ransagningskendelse.

⁽¹⁵⁴⁾ Ifølge Supreme Court er »begrundet mistanke« en »praktisk, ikketeknisk« standard, der bygger på »faktuelle og praktiske dagligdags overvejelser, som fornuftige og forsigtige personer handler efter« (*Illinois v. Gates*, 462 U.S. 213, 232 (1983)). Hvad angår ransagningskendelser foreligger der en begrundet mistanke, når der er rimelig sandsynlighed for, at en ransagnings vil føre til, at man finder et bevis for en forbrydelse (id).

udstedt en ransagningskendelse mod, eller hvis ejendele er genstand for en ransagning, kan kræve, at bevismateriale, der er fremskaffet under eller kan henføres til en ulovlig ransagning, slettes, hvis dette bevismateriale føres mod den pågældende under en straffesag ⁽¹⁵⁵⁾. Når en dataindehaver (f.eks. en virksomhed) skal videregive oplysninger i henhold til en kendelse, kan den pågældende navnlig anfægte kravet om videregivelse som værende urimeligt byrdefuldt ⁽¹⁵⁶⁾.

- (93) For det andet kan en anklagejury (grand jury, domstolens efterforskningsgren, som udpeges af en dommer) udstede en stævning i forbindelse med efterforskning af visse alvorlige forbrydelser ⁽¹⁵⁷⁾, normalt på forbundsanklagerens foranledning, for at pålægge en person at tilvejebringe eller udlevere forretningsoplysninger, elektronisk lagrede oplysninger eller andre konkrete ting. Derudover kan der i henhold til forskellige love udstedes administrative pålæg om tilvejebringelse eller udlevering af forretningsoplysninger, elektronisk lagrede oplysninger eller andre konkrete ting i sager, der involverer misbrug af sundhedsydelser, børnemishandling, beskyttelse af efterretningstjenester og kontrollerede stoffer samt i forbindelse med generalinspektørernes undersøgelser ⁽¹⁵⁸⁾. I begge tilfælde skal oplysningerne være relevante for efterforskningen, og pålægget må ikke være urimeligt, dvs. overdrevent, undertrykkende eller byrdefuldt (og kan anfægtes af modtageren af pålægget med henvisning til disse grunde) ⁽¹⁵⁹⁾.
- (94) Der gælder meget lignende betingelser for administrative pålæg, der udstedes for at søge adgang til oplysninger, som virksomheder i USA er i besiddelse af, til civile eller lovgivningsmæssige formål (»offentlig interesse«). Bemyndigelsen af agenturer med civilt og reguleringsmæssigt ansvar til at udstede sådanne administrative pålæg skal fastsættes ved lov. Anvendelsen af et administrativt pålæg er underlagt en »rimelighedstest«, som kræver, at undersøgelsen gennemføres i overensstemmelse med et legitimt formål, at de oplysninger, der anmodes om i henhold til anmodningen, er relevante for dette formål, at agenturet ikke allerede er i besiddelse af de oplysninger, som det søger sammen med anmodningen, og at de nødvendige administrative skridt til at udstede anmodningen er blevet fulgt ⁽¹⁶⁰⁾. Højesteret har også i sin retspraksis præciseret behovet for at afveje betydningen af den offentlige interesse i de oplysninger, der anmodes om, med betydningen af personlige og organisatoriske interesser i privatlivets fred ⁽¹⁶¹⁾. Selv om anvendelsen af et administrativt pålæg ikke er betinget af en forudgående retslig godkendelse, bliver den genstand for domstolsprøvelse i tilfælde af, at modtageren anfægter dette af ovennævnte grunde, eller hvis den udstedende myndighed søger at fuldbyrde stævningen i retten ⁽¹⁶²⁾. Ud over disse generelle overordnede begrænsninger kan specifikke (strengere) krav følge af individuelle love ⁽¹⁶³⁾.

⁽¹⁵⁵⁾ Mapp v. Ohio, 367 U.S. 643 (1961).

⁽¹⁵⁶⁾ Jf. *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (hvori det fastslås, at »en retfærdig rettergang kræver en høring om denne byrde, før et telefonselskab kan tvinges til at yde« bistand i forbindelse med en ransagningskendelse), og *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

⁽¹⁵⁷⁾ Den femte tilføjelse (»amendment«) til den amerikanske forfatning kræver, at en anklagejury rejser tiltale i forbindelse med »forbrydelser, der straffes med døden, og andre infame forbrydelser«. Anklagejuryen består af 16-23 medlemmer og afgør, om der er begrundet mistanke om, at der er begået en forbrydelse. For at nå frem til denne konklusion har anklagejurier undersøgelsesbeføjelser, der giver dem mulighed for at udstede stævninger.

⁽¹⁵⁸⁾ Jf. bilag VI.

⁽¹⁵⁹⁾ Federal Rules of Criminal Procedure, 17.

⁽¹⁶⁰⁾ United States v. Powell, 379 U.S. 48 (1964).

⁽¹⁶¹⁾ Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186 (1946).

⁽¹⁶²⁾ Højesteret har præciseret, at i tilfælde af anfægtelse af et administrativt pålæg skal en domstol tage stilling til, om 1) efterforskningen er lovligt tilladt, 2) den pågældende tilladelse til at udstede pålæg henhører under Kongressens kommandobeføjelse, og 3) de ønskede dokumenter er relevante for undersøgelsen. Domstolen bemærkede også, at en anmodning om et administrativt pålæg skal være »rimelig«, dvs. kræve, at »en specifikation af de dokumenter, der skal fremlægges, er tilstrækkelig, men ikke overdreven, med henblik på den relevante undersøgelse«, herunder »specificitet i forbindelse med beskrivelse af det sted, der skal ransages, og de personer eller ting, der skal beslaglægges«.

⁽¹⁶³⁾ For eksempel giver Right to Financial Privacy Act kun en statslig myndighed beføjelse til at indhente finansielle optegnelser, som en finansiell institution er i besiddelse af i henhold til et administrativt pålæg, hvis 1) der er grund til at antage, at de ønskede optegnelser er relevante for en legitim retshåndhævelsesundersøgelse, og 2) der er blevet givet en kopi af anmodningen eller indkaldelsen til kunden sammen med en meddelelse med rimelig specificitet om undersøgelsens karakter (12 U.S.C. § 3405). Et andet eksempel er Fair Credit Reporting Act, som forbyder forbrugerindberetningsbureauer at offentliggøre forbrugerindberetninger som svar på anmodninger om administrative pålæg (og kun giver dem mulighed for at besvare anmodninger om stævninger udstedt af anklagejurier eller retskendelser, 15 U.S.C. § 1681 ff.). Med hensyn til adgang til kommunikationsoplysninger finder de specifikke krav i Stored Communications Act anvendelse, herunder med hensyn til muligheden for at anvende administrative pålæg (se betragtning 96-97 for en detaljeret oversigt).

- (95) For det tredje findes der flere retsgrundlag, som giver de strafferetlige håndhævelsesmyndigheder mulighed for at få adgang til kommunikationsdata. En domstol kan udstede en afgørelse, der giver tilladelse til indsamling af ikkeindholdsmæssige realtidsoplysninger om opkald, routing, adressering og signalering for et telefonnummer eller en e-mailadresse (ved anvendelse af en pen-register- eller trap and trace-anordning), hvis den finder, at myndigheden har attesteret, at de oplysninger, der forventes opnået, er relevante for en verserende strafferetlig efterforskning ⁽¹⁶⁴⁾. Afgørelsen skal bl.a. angive den mistænkte identitet, hvis den kendes, de væsentligste egenskaber ved den kommunikation, den vedrører, og en angivelse af den lovovertrædelse, som de oplysninger, der skal indsamles, relaterer til. Anvendelsen af en pen-register- eller trap and trace-anordning kan tillades for en periode på højst 60 dage, som kun kan forlænges ved en ny retsafgørelse.
- (96) Desuden kan der med henblik på strafferetlig håndhævelse opnås adgang til internetudbyderes, teleselskabers og andre eksterne tjenesteudbyderes opbevarede abonnentoplysninger, trafikdata og lagrede kommunikationsindhold på grundlag af Stored Communications Act ⁽¹⁶⁵⁾. For at få udleveret lagret elektronisk kommunikationsindhold skal strafferetlige håndhævende myndigheder generelt have udstedt et påbud af en dommer med den begrundelse, at der er begrundet mistanke om, at den pågældende konto indeholder beviser for en forbrydelse ⁽¹⁶⁶⁾. Strafferetlige håndhævende myndigheder kan få udleveret abonnentoplysninger, IP-adresser og tilknyttede tidsstempler samt faktureringsoplysninger på grundlag af et påbud. I forbindelse med de fleste andre lagrede, ikkeindholdsmæssige oplysninger såsom e-mail-hoveder uden emnelinjen skal de strafferetlige håndhævende myndigheder have en retsafgørelse, som udstedes, hvis dommeren mener, at der er rimelig grund til at antage, at de udbedte oplysninger er relevante og væsentlige for en verserende strafferetlig efterforskning.
- (97) Udbydere, der modtager anmodninger i henhold til Stored Communications Act, kan frivilligt underrette en kunde eller abonnent, hvis oplysninger udbedes, medmindre den relevante strafferetlige håndhævende myndighed indhenter en sikrende kendelse, der forbyder sådan underretning ⁽¹⁶⁷⁾. En sådan sikrende kendelse er en retsafgørelse, der pålægger en udbyder af elektroniske kommunikationstjenester eller fjerndatabehandlingstjenester, som en ransagningskendelse, et pålæg eller en retsafgørelse er rettet til, ikke at underrette andre om ransagningskendelsen, pålægget eller retsafgørelsen, så længe retten finder det hensigtsmæssigt. Der afsiges sikrende kendelser, hvis en ret finder, at der er grund til at antage, at en underretning i alvorlig grad ville skade en efterforskning eller forsinke en retssag unødigt, f.eks. fordi det ville bringe en persons liv eller fysiske sikkerhed i fare, medføre flugt for at undgå retsforfølgning, intimidering af potentielle vidner osv. Et memorandum fra vicejustitsministeren (som er bindende for alle advokater og befuldmægtigede) kræver, at anklagerne foretager en detaljeret vurdering af behovet for en sikrende kendelse og begrunder over for retten, hvordan de lovbestemte kriterier for indhentning af en sikrende kendelse er opfyldt i det konkrete tilfælde ⁽¹⁶⁸⁾. Ifølge dette memorandum må anmodninger om sikrende kendelser desuden generelt ikke have til formål at forsinke underretningen i mere end et år. Hvis det under særlige omstændigheder kan være nødvendigt med sikrende kendelser med en længere varighed, kan sådanne kendelser kun indhentes efter skriftlig aftale med en tilsynsmyndighed udpeget af den amerikanske justitsminister eller den relevante assisterende justitsminister. Derudover skal en anklager, når en efterforskning nedlukkes, straks vurdere, om der er grundlag for at opretholde eventuelle udestående sikrende kendelser, og, hvis dette ikke er tilfældet, bringe den sikrende kendelse til ophør og sikre, at tjenesteudbyderen underrettes herom ⁽¹⁶⁹⁾.

⁽¹⁶⁴⁾ 18 U.S.C. § 3123.

⁽¹⁶⁵⁾ 18 U.S.C. § 2701-2713.

⁽¹⁶⁶⁾ 18 U.S.C. § 2701(a)-(b)(1)(A). Hvis den pågældende abonnent eller kunde underrettes herom (enten på forhånd eller under visse omstændigheder ved senere underretning), kan de indholdsoplysninger, der lagres i mere end 180 dage, også indhentes på grundlag af et administrativt pålæg eller en stævning udstedt af anklagejuryen (18 U.S.C. § 2701(b)(1)(B)) eller en retsafgørelse (hvis der er rimelig grund til at antage, at oplysningerne er relevante og væsentlige for en verserende strafferetlig efterforskning (18 U.S.C. § 2701(d))). I overensstemmelse med en afgørelse fra en forbundsappeldomstol får statens efterforskere imidlertid generelt ransagningskendelser fra dommere med henblik på indsamling af indholdet af privat kommunikation eller lagrede oplysninger hos en kommerciel udbyder af kommunikationstjenester. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

⁽¹⁶⁷⁾ 18 U.S.C. § 2705(b).

⁽¹⁶⁸⁾ Jf. memorandum udstedt af vicejustitsminister Rod Rosenstein den 19.10.2017 om en mere restriktiv politik for anmodninger om sikrende kendelser (eller kendelser om beskyttelse af oplysninger), som findes på <https://www.justice.gov/criminal-ccips/page/file/1005791/download>.

⁽¹⁶⁹⁾ Memorandum udstedt af vicejustitsminister Lisa Moncao den 27.5.2022 om en supplerende politik vedrørende anmodninger om sikrende kendelser i henhold til 18 U.S.C. § 2705(b).

- (98) De strafferetlige håndhævende myndigheder kan desuden opfange trådbåren, mundtlig eller elektronisk kommunikation i realtid på grundlag af en retsafgørelse, hvor en dommer bl.a. vurderer, at der er begrundet mistanke om, at aflytningen eller den elektroniske opfangning vil tilvejebringe bevis for en føderal forbrydelse eller for opholdsstedet for en person, der er på flugt for at undgå retsforfølgning ⁽¹⁷⁰⁾.
- (99) Der ydes yderligere beskyttelse gennem justitsministeriets politikker og retningslinjer, herunder justitsministerens retningslinjer for FBI's indenlandske operationer (AGG-DOM), som bl.a. kræver, at Federal Bureau of Investigation (FBI) anvender de mindst indgribende efterforskningsmetoder under hensyntagen til indvirkningen på privatlivets fred og borgerlige frihedsrettigheder ⁽¹⁷¹⁾.
- (100) Ifølge den amerikanske regerings udredninger er der det samme eller et højere beskyttelsesniveau som beskrevet ovenfor i forbindelse med retshåndhævende efterforskninger på delstatsniveau (efterforskninger omfattet af delstatslove) ⁽¹⁷²⁾. Navnlig bekræfter forfatningsmæssige bestemmelser samt love og retspraksis på statsniveau ovennævnte beskyttelse mod urimelige ransagninger og beslaglæggelser ved at kræve udstedelse af en ransagningskendelse ⁽¹⁷³⁾. I lighed med den beskyttelse, der ydes på forbundsplan, kan der kun udstedes ransagningskendelser, hvis der kan påvises begrundet mistanke, og det skal angives, hvor ransagningen skal foretages, og hvilken person eller ting der skal beslaglægges ⁽¹⁷⁴⁾.

⁽¹⁷⁰⁾ 18 U.S.C. § 2510-2522.

⁽¹⁷¹⁾ Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (september 2008), findes på <http://www.justice.gov/archive/opa/docs/guidelines.pdf>. Der er fastlagt yderligere regler og politikker, der begrænser forbundsanklagernes efterforskningsaktiviteter i United States Attorneys' Manual, der er tilgængelig på <http://www.justice.gov/usam/united-states-attorneys-manual>. For at kunne fravige disse retningslinjer skal FBI's direktør, vicedirektør eller assisterende direktør, der er udpeget af direktøren, indhente en forudgående godkendelse, medmindre det ikke er muligt at opnå en sådan godkendelse på grund af den umiddelbart forestående eller alvorlige trussel mod sikkerheden for personer eller ejendom eller mod den nationale sikkerhed (i så fald skal direktøren eller en anden bemyndiget person underrettes så hurtigt, som det er praktisk muligt). Hvis ikke retningslinjerne følges, skal FBI underrette justitsministeriet herom, som derefter underretter justitsministeren og vicejustitsministeren.

⁽¹⁷²⁾ Bilag VI, fodnote 2. Jf. også f.eks. *Arnold v. City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) («Med hensyn til individuelle rettigheder og borgerlige frihedsrettigheder giver den amerikanske forfatning, hvor det er relevant for staterne, en nedre grænse, som statsdomstolsafgørelser ikke må falde under»). *Cooper v. California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) («Vores besiddelse berører naturligvis ikke statens beføjelse til at fastsætte højere standarder for ransagninger og beslaglæggelser end krævet i forbundsforfatningen, hvis den vælger at gøre det»). *Petersen v. City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) («selv om Arizonas forfatning kan fastsætte strengere standarder for ransagninger og beslaglæggelser end den føderale forfatning, kan Arizonas domstole ikke yde mindre beskyttelse end fjerde amendement»).

⁽¹⁷³⁾ De fleste stater har gentaget beskyttelsen i fjerde amendement i deres forfatninger. Jf. Alabamas forfatning, art. I, § 5), Alaskas forfatning, art. I, § 14, 1, Arkansas' forfatning, art. II, § 15, Californiens forfatning, art. I, § 13, Colorados forfatning, art. II, § 7, Connecticut's forfatning, art. I, § 7, Delawares forfatning, art. I, § 6, Floridas forfatning, art. I, § 12, Georgias forfatning, art. I, § 1, para. XIII, Hawais forfatning, art. I, § 7, Idahos forfatning, art. I, § 17, Illinois' forfatning, art. I, § 6, Indianas forfatning, art. I, § 11, Iowas forfatning, art. I, § 8, Kansas' forfatning, Bill of Rights, § 15, Kentuckys forfatning, § 10, Louisianas forfatning, art. I, § 5, Maines forfatning, art. I, § 5, Massachusetts' forfatning, Decl. of Rights art. 14, Michigans forfatning, art. I, § 11, Minnesotas forfatning, art. I, § 10, Mississippis forfatning, art. III, § 23, Missouris forfatning, art. I, § 15, Montanas forfatning, art. II, § 11, Nebraskas forfatning, art. I, § 7, Nevadas forfatning, art. I, § 18, New Hampshires forfatning, pt. 1, art. 19, N.J.'s forfatning, art. II, § 7, New Mexicos forfatning, art. II, § 10, New Yorks forfatning, art. I, § 12, North Dakotas forfatning, art. I, § 8, Ohios forfatning, art. I, § 14, Oklahomas forfatning, art. II, § 30, Oregons forfatning, art. I, § 9, Pennsylvanias forfatning, art. I, § 8, Rhode Islands forfatning, art. I, § 6, South Carolinas forfatning, art. I, § 10, South Dakotas forfatning, art. VI, § 11, Tennessees forfatning, art. I, § 7, Texas' forfatning, art. I, § 9, Utahs forfatning, art. I, § 14, Vermonts forfatning, ch. I, art. 11, West Virginias forfatning, art. III, § 6, Wisconsin's forfatning, art. I, § 11, Wyomings forfatning, art. I, § 4. Andre (f.eks. Maryland, North Carolina og Virginia) har i deres forfatninger indføjet et særligt sprog vedrørende arrestordrer, der er blevet fortolket for at give en beskyttelse, der svarer til eller er højere end fjerde amendement (jf. Maryland. Decl. of Rts. art. 26, North Carolinas forfatning, art. I, § 20, Virginias forfatning, art. I, § 10, og relevant retspraksis, f.eks. *Hamel v. State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008, *State v. Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) og *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). Endelig har Arizona og Washington forfatningsmæssige bestemmelser, der beskytter privatlivets fred mere generelt (Arizonas forfatning, art. 2, § 8, Washingtons forfatning, art. I, § 7), som af domstolene er blevet fortolket som mere beskyttende end fjerde amendement (jf. f.eks. *State v. Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State v. Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), *State v. Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

⁽¹⁷⁴⁾ Jf. f.eks. California Penal Code § 1524,3(b), Rule 3.6-3.13 Alabama Rules of Criminal Procedure, Section 10.79.035; Revised Code of Washington, Section 19.2-59 i Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia.

3.1.1.2 Videre anvendelse af de indsamlede oplysninger

- (101) Hvad angår den videre anvendelse af oplysninger indsamlet af føderale strafferetlige håndhævende myndigheder indeholder forskellige love, retningslinjer og standarder specifikke garantier. Med undtagelse af de specifikke instrumenter, der finder anvendelse på FBI's aktiviteter (AGG-DOM og FBI's interne undersøgelses- og driftsvejledning (Domestic Investigations and Operations Guide)), gælder kravene i dette afsnit generelt for alle føderale myndigheders videre anvendelse af data, herunder data, der tilgås til civile eller lovgivningsmæssige formål. Dette omfatter de krav, der følger af Office of Management and Budget memos/regulations, Federal Information Security Management Modernisation Act, E-Government Act og Federal Records Act.
- (102) I overensstemmelse med den bemyndigelse, der er fastsat i Clinger-Cohen Act (P.L. 104-106, Division E) og Computer Security Act af 1987 (P.L. 100-235), udstedte Office of Management and Budget (OMB) cirkulære nr. A-130 om fastsættelse af generelle bindende retningslinjer, der finder anvendelse på alle forbundsmyndigheder (herunder retshåndhævende myndigheder), når de håndterer personligt identificerbare oplysninger ⁽¹⁷⁵⁾. Cirkulæret kræver navnlig, at alle forbundsorganer »begrænser udarbejdelsen, indsamlingen, anvendelsen, behandlingen, opbevaringen, vedligeholdelsen, udbredelsen og videregivelsen af personligt identificerbare oplysninger til de oplysninger, der er godkendt ved lov, relevante og med rimelighed kan anses for nødvendige for en korrekt udførelse af de autoriserede organers opgaver« ⁽¹⁷⁶⁾. Desuden skal forbundsorganer i det omfang, det med rimelighed er praktisk muligt, sikre, at personligt identificerbare oplysninger er nøjagtige, relevante, rettidige og fuldstændige og reduceret til det minimum, der er nødvendigt for en korrekt udførelse af et organs opgaver. Mere generelt skal forbundsorganer udarbejde et omfattende program til beskyttelse af privatlivets fred for at sikre, at de gældende krav om beskyttelse af privatlivets fred overholdes, udvikle og evaluere politikker til beskyttelse af privatlivets fred og håndtere risici for privatlivets fred, opretholde procedurer til at identificere, dokumentere og indberette tilfælde af manglende respekt for privatlivets fred, udvikle oplysnings- og uddannelsesprogrammer om privatlivets fred for medarbejdere og kontrahenter og indføre politikker og procedurer for at sikre, at personalet holdes ansvarligt for overholdelsen af krav og politikker til beskyttelse af privatlivets fred ⁽¹⁷⁷⁾.
- (103) Derudover kræver E-Government Act ⁽¹⁷⁸⁾, at alle forbundsorganer (herunder strafferetlige håndhævende myndigheder) indfører informationssikkerhedsbeskyttelse, der står i et rimeligt forhold til risikoen for og omfanget af den skade, der ville opstå som følge af uautoriseret adgang, anvendelse, videregivelse, afbrydelse, ændring eller tilintetgørelse, har en informationschef, som sikrer overholdelse af informationssikkerhedskravene og foranlediger en årlig uafhængig evaluering (f.eks. foretaget af en generalinspektør, jf. betragtning 109) af deres program og praksis med hensyn til informationssikkerhed ⁽¹⁷⁹⁾. Tilsvarende kræver Federal Records Act (FRA) ⁽¹⁸⁰⁾ og supplerende bestemmelser ⁽¹⁸¹⁾, at oplysninger, som forbundsorganer er i besiddelse af, er underlagt sikkerhedsforanstaltninger, der sikrer oplysningernes fysiske integritet og beskytter dem mod uautoriseret adgang.
- (104) I henhold til deres føderale lovhjemmel, herunder Federal Information Security Modernisation Act af 2014, har OMB og National Institute of Standards and Technology (NIST) udviklet standarder, som er bindende for forbundsorganer (herunder strafferetlige håndhævende myndigheder), og som yderligere fastsætter de mindstekrav til informations-sikkerhed, der skal indføres, herunder adgangskontrol, oplysning og uddannelse, beredskabsplanlægning, reaktion på hændelser, værktøjer med hensyn til revision og ansvar, sikring af system- og informationsintegriteten, gennemførelse af vurderinger vedrørende privatlivets fred og sikkerhedsrisici osv. ⁽¹⁸²⁾ Derudover skal alle

⁽¹⁷⁵⁾ Dvs. »oplysninger, der kan anvendes til at fastslå eller spore en persons identitet, enten alene eller kombineret med andre oplysninger, der er knyttet til eller kan knyttes til en bestemt person«, jf. OMB-cirkulære nr. A-130, s. 33 (definition af »personligt identificerbare oplysninger«).

⁽¹⁷⁶⁾ OMB-cirkulære nr. A-130, Managing Information as a Strategic Resource, tillæg II, Responsibilities for Managing Personally Identifiable Information, 81 Fed. Reg. 49,689 (28.7.2016), s. 17.

⁽¹⁷⁷⁾ Tillæg II, § 5(a)-(h).

⁽¹⁷⁸⁾ 44 U.S.C. kapitel 36.

⁽¹⁷⁹⁾ 44 U.S.C. § 3544-3545.

⁽¹⁸⁰⁾ FAC, 44 U.S.C. § 3105.

⁽¹⁸¹⁾ 36 C.F.R. § 1228,150 et seq., 1228,228 og tillæg A.

⁽¹⁸²⁾ Jf. f.eks. OMB-cirkulære nr. A-130, NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (10. december 2020) og NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.

forbundsorganer (herunder strafferetlige håndhævende myndigheder) i overensstemmelse med OMB's retningslinjer udarbejde og gennemføre en plan for håndtering af brud på datasikkerheden, herunder reaktion på sådanne brud og vurdering af risikoen for skade ⁽¹⁸³⁾.

- (105) Med hensyn til opbevaring af oplysninger kræver FRA ⁽¹⁸⁴⁾, at amerikanske forbundsorganer (herunder strafferetlige håndhævende myndigheder) fastsætter opbevaringsperioder for deres optegnelser (hvorefter sådanne optegnelser skal bortskaffes), som skal godkendes af National Archives and Record Administration ⁽¹⁸⁵⁾. Varigheden af denne opbevaringsperiode fastsættes ud fra forskellige faktorer, såsom efterforskningstype, om beviserne stadig er relevante for efterforskningen osv. Hvad angår FBI fastsætter AGG-DOM, at FBI skal have en sådan plan for opbevaring af optegnelser og føre et system, der hurtigt kan hente status over og grundlaget for en efterforskning.
- (106) Endelig indeholder OMB-cirkulære nr. A-130 ligeledes visse krav, der skal overholdes ved videregivelse af personligt identificerbare oplysninger. Formidling og videregivelse af personligt identificerbare oplysninger skal i princippet begrænses til, hvad der er retligt tilladt, relevant og anset for rimeligt nødvendigt for en korrekt udførelse af et agenturs opgaver ⁽¹⁸⁶⁾. Når amerikanske forbundsorganer udveksler personligt identificerbare oplysninger med andre statslige enheder, skal de, hvor det er relevant, opstille betingelser (herunder gennemførelse af specifikke kontroller af sikkerheden og respekten for privatlivets fred), der regulerer behandlingen af oplysninger gennem skriftlige aftaler (herunder kontrakter, aftaler om dataanvendelse, aftaler om udveksling af oplysninger og aftalememoranda) ⁽¹⁸⁷⁾. For så vidt angår grundene til, at oplysninger kan udbredes, fastsætter AGG-DOM og FBI Domestic Investigations and Operations Guide ⁽¹⁸⁸⁾ f.eks., at FBI kan være underlagt et retligt krav herom (f.eks. i henhold til en international aftale) eller har tilladelse til at formidle oplysninger under visse omstændigheder, f.eks. til andre amerikanske myndigheder, hvis videregivelsen er forenelig med det formål, som oplysningerne blev indsamlet til, og er relateret til deres ansvar, til kongressen, til udenlandske agenturer, hvis oplysningerne vedrører deres ansvar, og videregivelsen er i overensstemmelse med USA's interesser; videregivelsen er navnlig nødvendig for at beskytte personer eller ejendom eller beskytte mod eller forebygge en forbrydelse eller trussel mod den nationale sikkerhed, og videregivelsen er forenelig med det formål, hvortil oplysningerne blev indsamlet ⁽¹⁸⁹⁾.

3.1.2 Tilsyn

- (107) De føderale strafferetlige håndhævende myndigheder er underlagt forskellige organers tilsyn ⁽¹⁹⁰⁾. Som forklaret i betragtning 92-99 omfatter dette i de fleste tilfælde forudgående tilsyn fra retsvæsenets side, som skal godkende individuelle indsamlingsforanstaltninger, før de kan anvendes. Desuden fører andre organer tilsyn med forskellige faser af de retshåndhævende myndigheders aktiviteter, herunder indsamling og behandling af personoplysninger. Tilsammen sikrer disse retslige og udenretslige organer, at de retshåndhævende myndigheder er underlagt uafhængigt tilsyn.

⁽¹⁸³⁾ Memorandum 17-12, »Preparing for and Responding to a Breach of Personally Identifiable Information«, som findes på https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, og OMB-cirkulære nr. A-130. F.eks. justitsministeriets procedurer for reaktion på brud på datasikkerheden, jf. <https://www.justice.gov/file/4336/download>.

⁽¹⁸⁴⁾ FRA, 44 U.S.C. § 3101 et seq.

⁽¹⁸⁵⁾ National Archives and Record Administration har beføjelse til at vurdere organernes praksis for forvaltning af optegnelser og kan afgøre, om det er berettiget fortsat at opbevare visse optegnelser (44 U.S.C. § 2904(c), 2906).

⁽¹⁸⁶⁾ OMB-cirkulære nr. A-130, Section 5.f.1.(d).

⁽¹⁸⁷⁾ OMB-cirkulære nr. A-130, tillæg I § 3(d).

⁽¹⁸⁸⁾ Jf. også FBI Domestic Investigations and Operations Guide (DIOG), Section 14.

⁽¹⁸⁹⁾ AGG-DOM, Section VI, B og C, FBI Domestic Investigations and Operations Guide (DIOG), Section 14.

⁽¹⁹⁰⁾ De mekanismer, der er nævnt i dette afsnit, finder også anvendelse på forbundsmyndighedernes indsamling og anvendelse af data til civile og lovgivningsmæssige formål. Føderale civile og regulerende organer er underlagt kontrol fra deres respektive Inspectors General (generalinspektører) og tilsyn fra Kongressen, herunder Government Accountability Office, Kongressens revisions- og undersøgelsesorgan. Medmindre agenturet har en udpeget databeskyttelsesansvarlig (Privacy and Civil Liberties Officer) — en stilling, der typisk findes i agenturer som justitsministeriet og Department of Homeland Security (ministeriet for national sikkerhed) på grund af deres ansvar for retshåndhævelse og national sikkerhed — påhviler disse opgaver agenturets øverste embedsmand for privatlivets fred (Senior Agency Official for Privacy — SAOP). Alle føderale myndigheder er retligt forpligtede til at udpege en SAOP, som har ansvaret for at sikre, at agenturet overholder lovgivningen om privatlivets fred, og føre tilsyn med relaterede spørgsmål. Jf. f.eks. OMB M-16-24, Role and Dedesignation of Senior Agency Officials for Privacy (2016).

- (108) For det første findes der databeskyttelsesansvarlige (Privacy and Civil Liberties Officers) i forskellige ministerier med ansvar for strafferetlig håndhævelse ⁽¹⁹¹⁾. Selv om disse databeskyttelsesansvarliges specifikke beføjelser kan variere afhængigt af lovhjemlen, omfatter de typisk tilsynet med procedurer for at sikre, at det pågældende ministerium/organ tager tilstrækkeligt hensyn til beskyttelsen af privatlivets fred og borgerlige frihedsrettigheder, og at der er indført passende procedurer for behandling af klager fra fysiske personer, der mener, at deres privatliv eller borgerlige frihedsrettigheder er blevet krænket. Lederne af de forskellige ministerier eller organer skal sikre, at de databeskyttelsesansvarlige har materiale og ressourcer til at varetage deres mandat, har adgang til alt det materiale og personale, der er nødvendigt for at udføre deres opgaver og underrettes og høres om forslag til politiske ændringer ⁽¹⁹²⁾. De databeskyttelsesansvarlige rapporterer regelmæssigt til den amerikanske Kongres, herunder om antallet og karakteren af de klager, som ministeriet/organet har modtaget, med en oversigt over afgørelserne i disse klagesager, de gennemførte undersøgelser og forespørgsler og resultaterne af deres aktiviteter ⁽¹⁹³⁾.
- (109) For det andet fører en uafhængig generalinspektør (Inspector General) tilsyn med justitsministeriets, herunder FBI's, aktiviteter ⁽¹⁹⁴⁾. Generalinspektører er lovmæssigt uafhængige ⁽¹⁹⁵⁾ og har ansvaret for at foretage uafhængige undersøgelser, revisioner og inspektioner af ministeriets programmer og operationer. De har adgang til alle optegnelser, rapporter, revisioner, evalueringer, dokumenter, papirer, anbefalinger eller andet relevant materiale, om nødvendigt på grundlag af et pålæg, og kan indhente vidneudsagn ⁽¹⁹⁶⁾. Selv om generalinspektørerne fremsætter ikkebindende anbefalinger om korrigerende foranstaltninger, offentliggøres deres rapporter, herunder om opfølgende foranstaltninger (eller mangel herpå) ⁽¹⁹⁷⁾, generelt, og de fremsendes til den amerikanske Kongres, der på dette grundlag kan udøve sin tilsynsfunktion (jf. betragtning 111) ⁽¹⁹⁸⁾.

⁽¹⁹¹⁾ Jf. 42 U.S.C. § 2000ee-1. Dette omfatter f.eks. justitsministeriet, ministeriet for national sikkerhed og FBI. I ministeriet for national sikkerhed er en ledende databeskyttelsesansvarlig (Chief Privacy Officer) desuden ansvarlig for at opretholde og forbedre beskyttelsen af privatlivets fred og fremme gennemsigtigheden i ministeriet (6 U.S.C. 142, Section 222). I ministeriet for national sikkerhed er alle systemer, teknologier, formularer og programmer, der indsamler personoplysninger eller har indvirkning på privatlivets fred, underlagt den ledende databeskyttelsesansvarliges tilsyn, idet denne har adgang til alle optegnelser, rapporter, revisioner, evalueringer, dokumenter, papirer, anbefalinger og andet materiale, som ministeriet har til rådighed, om nødvendigt ved fremsættelse af et pålæg. Den databeskyttelsesansvarlige skal hvert år aflægge rapport til Kongressen om ministeriets aktiviteter, der har indvirkning på privatlivets fred, herunder klager over krænkelser af privatlivets fred.

⁽¹⁹²⁾ 42 U.S.C. § 2000ee-1(d).

⁽¹⁹³⁾ Jf. 42 U.S.C. § 2000ee-1 (f)(1)-(2). Rapporten fra justitsministeriets ledende databeskyttelsesansvarlige og kontoret for databeskyttelse og borgerlige frihedsrettigheder (Office of Privacy and Civil Liberties) for perioden oktober 2020-marts 2021 viser f.eks., at der blev foretaget 389 evalueringer af respekten for privatlivets fred, herunder af informationssystemer og andre programmer (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

⁽¹⁹⁴⁾ Tilsvarende blev der ved Homeland Security Act af 2002 oprettet et generalinspektorat i ministeriet for national sikkerhed.

⁽¹⁹⁵⁾ Generalinspektørerne har et fast embede og kan kun afsættes af præsidenten, der skriftligt skal meddele den amerikanske Kongres årsagerne til denne afsættelse.

⁽¹⁹⁶⁾ Jf. Inspector General Act af 1978, § 6.

⁽¹⁹⁷⁾ Jf. i denne henseende f.eks. oversigten fra justitsministeriets generalinspektorat over de anbefalinger, det har fremsat, og det omfang, hvori de er blevet gennemført ved opfølgende foranstaltninger fra ministeriets eller organets side, <https://oig.justice.gov/sites/default/files/reports/22-043.pdf>.

⁽¹⁹⁸⁾ Jf. Inspector General Act af 1978, § 4(5), 5. Justitsministeriets generalinspektorat offentliggjorde f.eks. for nylig sin halvårige rapport til Kongressen (1.10.2021-31.3.2022, <https://oig.justice.gov/node/23596>), som giver et overblik over dets revisioner, vurderinger, inspektioner, særlige evalueringer og undersøgelser af justitsministeriets programmer og operationer. Disse aktiviteter omfattede en undersøgelse af en tidligere kontrahent vedrørende uretmæssig videregivelse af elektronisk overvågning (aflytning af en person) i en igangværende efterforskning, hvorefter kontrahenten blev dømt. Generalinspektoratet gennemførte ligeledes en undersøgelse af justitsministeriets organers programmer og praksis vedrørende informationssikkerhed, som omfatter kontrol af effektiviteten af informationssikkerhedspolitikker, -procedurer og -praksis i en repræsentativ undergruppe af organernes systemer.

- (110) For det tredje er afdelinger med ansvar for strafferetlig håndhævelse, i det omfang de udfører terrorbekæmpelsesaktiviteter, underlagt tilsyn af rådet for tilsyn med privatlivets fred og borgerlige rettigheder (Privacy and Civil Liberties Oversight Board — PCLOB), et uafhængigt agentur inden for den udøvende magt, der består af et tværpolitisk råd med fem medlemmer, der udpeges af formanden for en fast periode på seks år med senatets godkendelse⁽¹⁹⁹⁾. I henhold til PCLOB's stiftelsesdokument har rådet ansvarsområder relateret til terrorbekæmpelsespolitikker og deres gennemførelse med henblik på at beskytte privatlivets fred og borgerlige frihedsrettigheder. I forbindelse med sin revision kan rådet få adgang til alle tjenesternes relevante optegnelser, rapporter, revisioner, evalueringer, dokumenter, papirer og anbefalinger, herunder klassificerede oplysninger, gennemføre interview og indhente vidneudsagn⁽²⁰⁰⁾. Det modtager rapporter fra databeskyttelsesansvarlige i en række føderale ministerier og organer⁽²⁰¹⁾, det kan udstede anbefalinger til statslige og retshåndhævende myndigheder og rapporterer regelmæssigt til forskellige kongresudvalg og præsidenten⁽²⁰²⁾. Rådets rapporter, herunder dets rapporter til Kongressen, skal i videst muligt omfang gøres offentligt tilgængelige⁽²⁰³⁾.
- (111) Endelig er strafferetlige håndhævelsesaktiviteter underlagt specifikke kongresudvalgs tilsyn (retsudvalgene i Repræsentanternes Hus og Senatet). Retsudvalgene fører regelmæssigt tilsyn på forskellig vis, navnlig ved høringer, undersøgelser, revisioner og rapporter⁽²⁰⁴⁾.

3.1.3 *Klageadgang*

- (112) Som nævnt skal de strafferetlige håndhævende myndigheder i de fleste tilfælde indhente en forudgående retskendelse for at kunne indsamle personoplysninger. Selv om dette ikke er påkrævet i forbindelse med administrative pålæg, er disse begrænset til særlige situationer, og de vil blive underlagt uafhængig domstolsprøvelse, i hvert fald når regeringen anmoder om at få håndhævet pålægget ved domstolene. Modtagere af administrative pålæg kan navnlig anfægte dem ved domstolene med den begrundelse, at de er urimelige, dvs. overdrevne, undertrykkende eller byrdefulde⁽²⁰⁵⁾.
- (113) Enkeltpersoner kan først og fremmest indgive anmodninger eller klager til de retshåndhævende myndigheder på det strafferetlige område vedrørende behandlingen af deres personoplysninger. Dette omfatter muligheden for at anmode om adgang til og berigtigelse af personoplysninger⁽²⁰⁶⁾. For så vidt angår aktiviteter i forbindelse med terrorbekæmpelse kan enkeltpersoner også indgive en klage til databeskyttelsesansvarlige (Privacy and Civil Liberties Officers) (eller andre embedsmænd, der beskæftiger sig med beskyttelse af privatlivets fred) hos retshåndhævende myndigheder⁽²⁰⁷⁾.
- (114) Derudover er der i amerikansk ret fastsat en række klagemuligheder for fysiske personer, så de kan klage over offentlige myndigheder eller en offentlig ansat i tilfælde, hvor disse myndigheder behandler personoplysninger⁽²⁰⁸⁾. Disse muligheder, der navnlig er fastsat i APA, Freedom of Information Act (FOIA) og Electronic Communications Privacy Act (ECPA), er tilgængelige for alle fysiske personer uanset nationalitet under iagttagelse af gældende betingelser.

⁽¹⁹⁹⁾ Rådets medlemmer skal udelukkende udvælges på grundlag af deres faglige kvalifikationer, arbejdspræstationer, offentlige status, ekspertise inden for borgerlige frihedsrettigheder og privatlivets fred samt deres relevante erfaringer, uden at der tages hensyn til deres politiske tilhørsforhold. Rådet kan under ingen omstændigheder have mere end tre medlemmer, som tilhører det samme politiske parti. En person, der udnævnes til rådet, kan ikke i sin mandatperiode være en valgt embedsmand, offentlig ansat eller ansat under den udøvende magt, undtagen i sin egenskab af medlem af rådet. Jf. 42 U.S.C. § 2000ee (h).

⁽²⁰⁰⁾ 42 U.S.C. § 2000ee (g).

⁽²⁰¹⁾ Jf. 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Disse omfatter som minimum justitsministeriet, forsvarsministeriet, ministeriet for national sikkerhed samt andre ministerier, organer eller enheder inden for den udøvende magt, som PCLOB betragter som værende relevante i denne sammenhæng.

⁽²⁰²⁾ 42 U.S.C. § 2000ee, (e).

⁽²⁰³⁾ 42 U.S.C. § 2000ee (f).

⁽²⁰⁴⁾ Udvalgene afholder f.eks. tematiske høringer (jf. f.eks. en nylig høring afholdt af retsudvalget i Repræsentanternes Hus om »digital klapjagt«, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>), samt regelmæssige tilsynshøringer, f.eks. af FBI og justitsministeriet, se <https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation>, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966> og <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899>.

⁽²⁰⁵⁾ Jf. bilag VI.

⁽²⁰⁶⁾ OMB-cirkulære nr. A-130, tillæg II, Section 3(a) og (f), som pålægger forbundsmyndighederne at sikre passende adgang og berigtigelse efter anmodning fra enkeltpersoner og fastlægge procedurer for modtagelse og behandling af klager og anmodninger om beskyttelse af privatlivets fred.

⁽²⁰⁷⁾ Jf. 42 U.S.C. § 2000ee-1 for så vidt angår f.eks. justitsministeriet og ministeriet for national sikkerhed. Jf. også OMB Memorandum M-16-24, *Role and Dedesignation of Senior Agency Officials for Privacy*.

⁽²⁰⁸⁾ De klagemekanismer, der er nævnt i dette afsnit, finder også anvendelse på forbundsmyndighedernes indsamling og anvendelse af data til civile og lovgivningsmæssige formål.

- (115) I bestemmelserne om adgang til retslig prøvelse i APA ⁽²⁰⁹⁾ slås det fast, at »enhver person, mod hvem der er begået juridisk uret på grund af et agents foranstaltninger, eller som er blevet krænkede eller forurettet herved«, kan begære retslig prøvelse ⁽²¹⁰⁾. Det omfatter muligheden for at anmode domstolen om at »erklære agents foranstaltninger, konstateringer og konklusioner for ulovlige og annullere dem, hvis de er vilkårlige, ustadige eller udtryk for magtmisbrug eller på anden vis ikke er i overensstemmelse med loven« ⁽²¹¹⁾.
- (116) Mere specifikt fastsættes der i Title II i ECPA ⁽²¹²⁾ en række lovbestemte rettigheder med hensyn til privatlivets fred, der regulerer retshåndhævende myndigheders adgang til indholdet af trådbåren, mundtlig eller elektronisk kommunikation, der lagres af tredjepartsudbydere ⁽²¹³⁾. Herved kriminaliseres den ulovlige adgang (dvs. den adgang, der ikke er godkendt af en domstol eller i øvrigt tilladt) til sådan kommunikation, og den pågældende person får mulighed for at anlægge et civil søgsmål ved en amerikansk forbundsdomstol mod en embedsmand, der forsætligt har begået sådanne ulovlige handlinger, eller mod USA for at få tilkendt direkte og pønalt begrundet erstatning eller for at søge oprejsning og anerkendelse.
- (117) Derudover giver adskillige andre bestemmelser de registrerede ret til at anlægge sag mod en amerikansk offentlig myndighed eller offentlig ansat for behandling af deres personoplysninger, herunder Wiretap Act ⁽²¹⁴⁾, Computer Fraud and Abuse Act ⁽²¹⁵⁾, Federal Torts Claim Act ⁽²¹⁶⁾, Right to Financial Privacy Act ⁽²¹⁷⁾ og Fair Credit Reporting Act ⁽²¹⁸⁾.

⁽²⁰⁹⁾ 5 U.S.C. § 702.

⁽²¹⁰⁾ Generelt er det kun agents »endelige« — og ikke »foreløbige, proceduremæssige eller mellemliggende« — foranstaltninger, der er genstand for retslig prøvelse. Jf. 5 U.S.C. § 704.

⁽²¹¹⁾ 5 U.S.C. § 706(2)(A).

⁽²¹²⁾ 18 U.S.C. § 2701-2712.

⁽²¹³⁾ ECPA beskytter kommunikation, som to definerede kategorier af netværksudbydere ligger inde med, nemlig udbydere af: i) elektroniske kommunikationstjenester, f.eks. telefoni eller e-mail, og ii) fjerndatabasebehandlingstjenester såsom datalagrings- eller databasebehandlingstjenester.

⁽²¹⁴⁾ 18 U.S.C. § 2510 et seq. Ifølge Wiretap Act (18 U.S.C. § 2520) kan en person, hvis trådbårne, mundtlige eller elektroniske kommunikation er blevet opfanget, offentliggjort eller forsætligt anvendt, anlægge et privat søgsmål for overtrædelse af Wiretap Act, herunder, under visse omstændigheder, mod en individuel embedsmand eller USA. Hvad angår indsamling af ikkeindholdsmæssige oplysninger (f.eks. IP-adresse, e-mails afsender- og modtageradresse), se også kapitlet om pen-register- og trap and trace-anordninger i Title 18 (18 U.S.C. § 3121-3127, og vedrørende private søgsmål § 2707).

⁽²¹⁵⁾ 18 U.S.C. § 1030. Ifølge Computer Fraud and Abuse Act kan en person anlægge sag mod en anden person for bevidst uautoriseret adgang (eller adgang ud over autoriseret adgang) for at indhente oplysninger fra en finansiell institution, den amerikanske regerings computersystemer eller en anden specificeret computer, herunder, under visse omstændigheder, mod en individuel embedsmand.

⁽²¹⁶⁾ 28 U.S.C. § 2671 et seq. Ifølge Federal Tort Claims Act kan en person, under visse omstændigheder, anlægge sag mod USA for »en embedsmands uagtsomme eller ulovlige handling eller udeladelse i forbindelse med udførelsen af vedkommendes embede«.

⁽²¹⁷⁾ 12 U.S.C. § 3401 et seq. Ifølge Right to Financial Privacy Act kan en person, under visse omstændigheder, anlægge sag mod USA vedrørende adgang til eller offentliggørelse af beskyttede finansielle oplysninger, der udgør en lovovertrædelse. Statslig adgang til beskyttede finansielle oplysninger er generelt forbudt, medmindre regeringen gør anmodningen til genstand for et retsligt pålæg eller en ransagningskendelse, eller, i begrænsede tilfælde, en formel skriftlig anmodning, hvilket den pågældende person, hvis oplysninger udbedes, underrettes om.

⁽²¹⁸⁾ 15 U.S.C. § 1681-1681x. Ifølge Fair Credit Reporting Act kan en person anlægge sag mod enhver person, som ikke overholder betingelserne (herunder især kravet om lovlig tilladelse) for indsamling, videregivelse og anvendelse af forbrugerkreditrapporter eller, under visse omstændigheder, mod et statsligt organ.

- (118) I henhold til FOIA ⁽²¹⁹⁾, 5 U.S.C., § 552, har enhver person ret til at få adgang til registre fra forbundsagenturet, herunder hvis disse indeholder personens personoplysninger. Når de administrative retsmidler er udtømt, kan en person påberåbe sig en sådan ret til aktindsigt i retten, medmindre disse registre er beskyttet mod offentliggørelse ved en undtagelse eller en særlig udelukkelse fra retshåndhævelse ⁽²²⁰⁾. I dette tilfælde vil retten vurdere, om en undtagelse finder anvendelse eller lovligt er blevet påberåbt af den relevante offentlige myndighed.

3.2 De amerikanske offentlige myndigheders adgang til og brug af personoplysninger til nationale sikkerhedsformål

- (119) Amerikansk ret indeholder forskellige begrænsninger og garantier med hensyn til adgangen til og brugen af personoplysninger til nationale sikkerhedsformål samt tilsyns- og klagemekanismer, der er i overensstemmelse med de krav, der er omhandlet i betragtning 89 til denne afgørelse. De betingelser, hvorunder en sådan adgang kan finde sted, og de garantier, der gælder for udøvelsen af disse beføjelser, vurderes nærmere i de følgende afsnit.

3.2.1 Retsgrundlag, begrænsninger og garantier

3.2.1.1 Relevante retsregler

- (120) De amerikanske myndigheder kan indsamle personoplysninger, der overføres fra Unionen til organisationer under EU-USA-databeskyttelsesrammen, til nationale sikkerhedsformål på grundlag af forskellige retlige instrumenter. Denne indsamling er dog underlagt specifikke betingelser og garantier.
- (121) Når organisationer i USA har modtaget personoplysninger, kan amerikanske efterretningstjenester kun søge adgang til sådanne oplysninger af hensyn til den nationale sikkerhed i henhold til loven, nærmere bestemt i henhold til Foreign Intelligence Surveillance Act (FISA) eller lovbestemmelser, der giver adgang via nationale sikkerhedsbreve (NSL) ⁽²²¹⁾. Der er en række retsgrundlag i FISA, som kan anvendes til at indsamle (og efterfølgende behandle) personoplysninger for registrerede i EU overført under EU-USA-databeskyttelsesrammen (Section 105 i FISA ⁽²²²⁾, Section 302 i FISA ⁽²²³⁾, Section 402 i FISA ⁽²²⁴⁾, Section 501 i FISA ⁽²²⁵⁾ og Section 702 i FISA ⁽²²⁶⁾), som nærmere beskrevet i betragtning 142-152.

⁽²¹⁹⁾ 5 U.S.C. § 552.

⁽²²⁰⁾ Disse undtagelser er dog begrænsede. F.eks. er rettigheder i henhold til FOIA, 5 U.S.C. § 552 (b)(7), udelukket for »optegnelser eller oplysninger, der er indsamlet til retshåndhævelsesformål, men kun i det omfang, at fremlæggelsen af sådanne retshåndhævelsesoptegnelser eller -oplysninger A) med rimelighed kan antages at hindre retshåndhævende foranstaltninger, B) vil fratage en person retten til en retfærdig rettergang eller en uvildig pådømmelse, C) med rimelighed kan antages at udgøre en uberettiget krænkelse af privatlivets fred, D) med rimelighed kan forventes at afsløre identiteten på en hemmelig kilde (herunder en stat, en inden- eller udenlandsk tjeneste eller myndighed eller enhver privat institution, som har tilvejebragt oplysninger på et fortroligt grundlag, og — i tilfælde af en optegnelse eller oplysning indsamlet af en strafferetlig håndhævende myndighed i forbindelse med en strafferetlig efterforskning eller af en tjeneste, som foretager en lovlig national sikkerhedsefterretningsundersøgelse — oplysninger tilvejebragt af en hemmelig kilde), E) vil offentliggøre teknikker og procedurer brugt i de retshåndhævende myndigheders efterforskninger eller retsforfølgelser eller offentliggøre retningslinjer for de retshåndhævende myndigheders efterforskninger eller retsforfølgelse, hvis en sådan offentliggørelse med rimelighed kan antages at medføre en omgåelse af retten, eller F) med rimelighed kan antages at bringe en persons liv eller fysiske sikkerhed i fare«. Dertil kommer, at »når der indgives en anmodning om indsigt i optegnelser, hvis fremlæggelse med rimelighed kan antages at hindre retshåndhævende foranstaltninger, og A) undersøgelsen eller proceduren vedrører en mulig overtrædelse af strafferetten, og B) der er grund til at tro, at i) genstanden for undersøgelsen eller proceduren ikke har kendskab hertil, og ii) offentliggørelse af optegnelsernes eksistens med rimelighed kan antages at hindre retshåndhævende foranstaltninger, kan agenturet, udelukkende i den periode omstændighederne varer ved, behandle optegnelserne, som om de ikke var underlagt betingelserne i dette stykke« (5 U.S.C. § 552 (c)(1)).

⁽²²¹⁾ 12 U.S.C. § 3414, 15 U.S.C. § 1681u-1681v og 18 U.S.C. § 2709. Jf. betragtning 153.

⁽²²²⁾ 50 U.S.C. § 1804, som vedrører individualiseret elektronisk overvågning.

⁽²²³⁾ 50 U.S.C. § 1822, som vedrører fysiske ransagninger til udenlandske efterretningsformål.

⁽²²⁴⁾ 50 U.S.C. § 1842, sammenholdt med § 1841(2) og Section 3127 i Title 18, som vedrører installation af pen-register- eller trap and trace-anordninger.

⁽²²⁵⁾ 50 U.S.C. § 1861, hvorefter FBI kan indgive »en anmodning om en afgørelse, som tillader en transportvirksomhed, en offentlig indkvarteringsfacilitet, en fysisk lagerfacilitet eller en biludlejningsfacilitet at frigive optegnelser, der er i dens besiddelse, til en efterforskning med henblik på at indsamle udenlandske efterretningsoplysninger eller en efterforskning vedrørende international terrorisme«.

⁽²²⁶⁾ 50 U.S.C. § 1881a, hvorefter amerikanske efterretningsenheder kan søge indsigt i oplysninger, herunder i indholdet af internetkommunikation, fra amerikanske virksomheder, som vedrører visse ikkeamerikanske personer uden for USA, med retsligt påbudt bistand fra udbydere af elektronisk kommunikation.

- (122) Amerikanske efterretningstjenester har endvidere mulighed for at indsamle personoplysninger uden for USA, hvilket kan omfatte personoplysninger i transit mellem Unionen og USA. Indsamlingen af personoplysninger uden for USA er baseret på præsidentielt dekret 12333 (EO 12333) ⁽²²⁷⁾, udstedt af præsidenten ⁽²²⁸⁾.
- (123) Indsamlingen af signalefterretninger er den form for indsamling af efterretninger, der er mest relevant for den foreliggende konstatering af et tilstrækkeligt beskyttelsesniveau, da den vedrører indsamling af elektronisk kommunikation og data fra informationssystemer. En sådan indsamling kan foretages af amerikanske efterretnings-tjenester i USA (på grundlag af FISA), og mens oplysningerne er i transit til USA (på grundlag af EO 12333).
- (124) Den 7. oktober 2022 udstedte den amerikanske præsident EO 14086 med titlen Enhancing Safeguards for United States Signals Intelligence, der fastsætter begrænsninger og garantier for alle amerikanske signalefterretningsaktiviteter. Dette præsidentielle dekret erstatter i vid udstrækning præsidentielt direktiv PPD 28 ⁽²²⁹⁾, styrker de betingelser, begrænsninger og garantier, der gælder for alle signalefterretningsaktiviteter (dvs. på grundlag af FISA og EO 12333), uanset hvor de finder sted ⁽²³⁰⁾, og indfører en ny klagemekanisme, hvorigennem disse garantier kan påberåbes og håndhæves af fysiske personer ⁽²³¹⁾ (jf. betragtning 176-194 for yderligere oplysninger). Derved gennemfører det resultatet af de drøftelser, der fandt sted mellem EU og USA efter Domstolens ugyldiggørelse af Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet vedrørende privatlivsskjoldet, i amerikansk ret (jf. betragtning 6). Det er derfor et særdeles vigtigt element i den retlige ramme, der vurderes i denne afgørelse.
- (125) De begrænsninger og garantier, der blev indført ved EO 14086, supplerer de begrænsninger og garantier, der er fastsat i Section 702 i FISA og EO 12333. Efterretningstjenesterne skal anvende de krav, der er beskrevet nedenfor (i afsnit 3.2.1.2 og 3.2.1.3), når de deltager i signalefterretningsaktiviteter i henhold til Section 702 i FISA og EO 12333, f.eks. ved udvælgelse/identifikation af kategorier af udenlandske efterretningsoplysninger, der skal indhentes i henhold til Section 702 i FISA, indsamle udenlandske efterretninger eller kontrafterretninger i henhold til EO 12333 og træffe individuelle afgørelser om målretning i henhold til Section 702 i FISA og EO 12333.
- (126) Kravene i dette præsidentielle dekret er bindende for hele efterretningssamfundet. De skal gennemføres yderligere ved efterretningstjenesternes politikker og procedurer, der omsætter dem til konkrete retningslinjer for de daglige operationer. I den forbindelse giver EO 14086 de amerikanske efterretningstjenester en frist på højst et år til at ajourføre deres eksisterende politikker og procedurer (dvs. senest den 7.10.2023) og bringe dem i overensstemmelse med kravene i det præsidentielle dekret. Sådanne ajourførte politikker og procedurer skal udarbejdes i samråd med den amerikanske justitsminister, den ansvarlige for beskyttelse af borgerlige frihedsrettigheder (Civil Liberties Protection Officer) under direktøren for den nationale efterretningstjeneste (ODNI CLPO) og PCLOB — et uafhængigt tilsynsorgan, der er bemyndiget til at gennemgå den udøvende magts politikker og gennemførelsen heraf med henblik på at beskytte privatlivets fred og de borgerlige frihedsrettigheder (jf. betragtning 110 for så vidt angår PCLOB's rolle og status) — og gøres offentligt tilgængelige ⁽²³²⁾. Når de ajourførte
-
- ⁽²²⁷⁾ EO 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (af 8.12.1981, som ændret den 30.7.2008). EO 12333 definerer mere overordnet den amerikanske efterretningsindsats' formål, retning, opgaver og ansvarsområder (herunder de forskellige efterretningsenheders rolle) og fastlægger de generelle parametre for udøvelsen af efterretningsaktiviteter.
- ⁽²²⁸⁾ 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.
- ⁽²²⁹⁾ EO 14086 erstatter et tidligere præsidentielt direktiv, PPD 28, med undtagelse af Section 3 og et supplerende bilag (som kræver, at efterretningstjenester hvert år reviderer deres signalefterretningsprioriteter og -krav under hensyntagen til fordelene ved signalefterretningsaktiviteter for USA's nationale interesser samt den risiko, som disse aktiviteter indebærer) og Section 6 (som indeholder generelle bestemmelser), jf. National Security Memorandum on Partial Revocation of Presidential Policy Directive 28, som findes på <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/>.
- ⁽²³⁰⁾ Jf. Section 5(f) i EO 14086, hvor det forklares, at det præsidentielle dekret har samme anvendelsesområde som PPD 28, der i henhold til direktivets fodnote 3 fandt anvendelse på signalefterretningsaktiviteter, der blev udført med henblik på at indsamle kommunikation eller oplysninger om kommunikation, bortset fra signalefterretningsaktiviteter, der blev udført for at teste eller udvikle signalefterretningskapacitet.
- ⁽²³¹⁾ Jf. i denne forbindelse f.eks. Section 5(h) i EO 14086, hvori det præciseres, at dekretets garantier skaber en juridisk rettighed og kan håndhæves af fysiske personer gennem klagemekanismen.
- ⁽²³²⁾ Jf. Section 2(c)(iv)(C) i EO 14086.

politikker og procedurer er på plads, foretager PCLOB desuden en gennemgang for at sikre, at de er i overensstemmelse med det præsidentielle dekret. Senest 180 dage efter, at PCLOB har afsluttet denne gennemgang, skal de enkelte efterretningstjenester nøje overveje og gennemføre eller på anden måde forholde sig til alle PCLOB's anbefalinger. Den 3. juli 2023 offentliggjorde den amerikanske regering sådanne ajourførte politikker og procedurer ⁽²³³⁾.

3.2.1.2 Begrænsninger og garantier med hensyn til indsamling af personoplysninger til nationale sikkerhedsformål

- (127) EO 14086 fastsætter en række vidtgående krav, som gælder for alle signalefterretningsaktiviteter (indsamling, anvendelse, videregivelse osv. af personoplysninger).
- (128) For det første skal sådanne aktiviteter være hjemlet ved lov eller præsidentiel bemyndigelse og udføres i overensstemmelse med amerikansk lovgivning, herunder forfatningen ⁽²³⁴⁾.
- (129) For det andet skal der være indført passende garantier for at sikre, at hensynet til privatlivets fred og borgerlige frihedsrettigheder integreres i planlægningen af sådanne aktiviteter ⁽²³⁵⁾.
- (130) Navnlig må enhver signalefterretningsaktivitet kun udføres, »efter at det på grundlag af en rimelig vurdering af alle relevante faktorer er fastslået, at aktiviteterne er nødvendige for at fremme en valideret efterretningsprioritet« (jf. betragtning 135, hvad angår begrebet »valideret efterretningsprioritet«) ⁽²³⁶⁾.
- (131) Derudover kan sådanne aktiviteter kun udføres »i et omfang og på en måde, der står i et rimeligt forhold til den validerede efterretningsprioritet, som de er godkendt til« ⁽²³⁷⁾. Med andre ord skal der findes en passende balance »mellem betydningen af den efterretningsprioritet, der forfølges, og indvirkningen på privatlivets fred og de berørte personers borgerlige frihedsrettigheder, uanset deres nationalitet og opholdssted« ⁽²³⁸⁾.
- (132) For at sikre overholdelsen af disse generelle krav — som afspejler principperne om lovlighed, nødvendighed og proportionalitet — er signalefterretningsaktiviteter underlagt tilsyn (se nærmere i afsnit 3.2.2) ⁽²³⁹⁾.
- (133) Disse overordnede krav underbygges yderligere med hensyn til indsamling af signalefterretninger af en række betingelser og begrænsninger, der sikrer, at indgrebet i fysiske personers rettigheder begrænses til, hvad der er nødvendigt og forholdsmæssigt for at fremme et legitimt mål.
- (134) For det første begrænser det præsidentielle dekret de forhold, der kan ligge til grund for dataindsamling som led i signalefterretningsaktiviteter, på to måder. På den ene side fastlægger det præsidentielle dekret de legitime mål, der kan forfølges ved indsamling af signalefterretninger, f.eks. at forstå eller vurdere udenlandske organisationers, herunder internationale terrororganisationers, kapaciteter, hensigter eller aktiviteter, der udgør en aktuel eller potentiell trussel mod USA's nationale sikkerhed, at beskytte landet mod udenlandsk militærs kapaciteter og aktiviteter, at forstå eller vurdere tværnationale trusler, der påvirker den globale sikkerhed, såsom klimaændringer og andre miljøændringer, risici for folkesundheden og humanitære trusler ⁽²⁴⁰⁾. På den anden side opregner det præsidentielle dekret visse mål, som aldrig må forfølges med signalefterretningsaktiviteter, f.eks. at undertrykke

⁽²³³⁾ <https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086>.

⁽²³⁴⁾ Section 2(a)(i) i EO 14086.

⁽²³⁵⁾ Section 2(a)(ii) i EO 14086.

⁽²³⁶⁾ Section 2(a)(ii)(A) i EO 14086. Dette kræver ikke altid, at signalefterretninger er det eneste middel til at fremme aspekter af en valideret efterretningsprioritet. Indsamlingen af signalefterretninger kan f.eks. anvendes til at sikre alternative veje til validering (f.eks. til at bekræfte oplysninger modtaget fra andre efterretningskilder) eller til at opretholde pålidelig adgang til de samme oplysninger (Section 2(c)(i)(A) i EO 14086).

⁽²³⁷⁾ Section 2(a)(ii)(B) i EO 14086.

⁽²³⁸⁾ Section 2(a)(ii)(B) i EO 14086.

⁽²³⁹⁾ Section 2(a)(iii), sammenholdt med Section 2(d) i EO 14086.

⁽²⁴⁰⁾ Section 2(b)(i) i EO 14086. På grund af den afgrænsede liste over legitime mål i det præsidentielle dekret, som ikke omfatter eventuelle fremtidige trusler, giver det præsidentielle dekret præsidenten mulighed for at ajourføre denne liste, hvis der opstår nye trusler mod den nationale sikkerhed. Sådanne ajourføringer skal i princippet offentliggøres, medmindre præsidenten fastslår, at dette i sig selv ville udgøre en risiko for USA's nationale sikkerhed (Section 2(b)(i)(B) i EO 14086).

kritik, uenighed eller fysiske personers eller pressens frie tilkendegivelse af meninger eller politiske holdninger, at forskelsbehandle mennesker på grund af etnisk oprindelse, race, køn, kønsidentitet, seksuel orientering eller religion, eller at give amerikanske virksomheder en konkurrencefordel ⁽²⁴¹⁾.

- (135) Desuden kan efterretningstjenesterne ikke alene påberåbe sig de legitime mål, der er fastsat i EO 14086, som en begrundelse for indsamling af signalefterretninger, idet disse mål i operationelt øjemed skal omsættes til mere konkrete prioriteter, til hvilke der kan indsamles signalefterretninger. Med andre ord kan egentlig indsamling kun finde sted for at fremme en mere specifik prioritet. Sådanne prioriteter fastlægges gennem en særlig proces, der har til formål at sikre, at de gældende retlige krav overholdes, herunder dem, der vedrører privatlivets fred og borgerlige frihedsrettigheder. Efterretningsprioriteterne opstilles nærmere bestemt først af direktøren for den nationale efterretningstjeneste (gennem den såkaldte National Intelligence Priorities Framework), hvorefter de forelægges præsidenten til godkendelse ⁽²⁴²⁾. Inden direktøren forelægger præsidenten sådanne efterretningsprioriteter, skal direktøren i overensstemmelse med EO 14086 indhente en vurdering fra ODNI CLPO for hver prioritet med hensyn til, om den 1) fremmer et eller flere af de legitime mål i det præsidentielle dekret, 2) hverken er udformet til eller forventes at resultere i indsamling af signalefterretninger med henblik på et af de forbudte formål i det præsidentielle dekret, og 3) er fastlagt, efter at der er taget behørigt hensyn til privatlivets fred og de borgerlige frihedsrettigheder for alle personer, uanset deres nationalitet og opholdssted ⁽²⁴³⁾. Såfremt direktøren er uenig i CLPO's vurdering, skal begge synspunkter forelægges præsidenten ⁽²⁴⁴⁾.
- (136) Denne proces sikrer dermed navnlig, at der tages hensyn til privatlivets fred allerede i den indledende fase, hvor efterretningsprioriteterne opstilles.
- (137) For det andet gælder det, at når en efterretningsprioritet er blevet fastlagt, er der en række krav, der bestemmer, om og i hvilket omfang der kan indsamles signalefterretninger for at fremme en sådan prioritet. Disse krav operationaliserer de overordnede nødvendigheds- og proportionalitetsstandarder, der er fastsat i Section 2(a) i EO.
- (138) Navnlig må der kun indsamles signalefterretninger, »når det på grundlag af en rimelig vurdering af alle relevante faktorer er fastslået, at indsamlingen er nødvendig for at fremme en specifik efterretningsprioritet« ⁽²⁴⁵⁾. Ved afgørelsen af, om en bestemt indsamling af signalefterretninger er nødvendig for at fremme en valideret efterretningsprioritet, skal de amerikanske efterretningstjenester overveje, om andre mindre indgribende kilder og metoder, herunder diplomatiske og offentlige kilder, er tilgængelige, anvendelige og hensigtsmæssige ⁽²⁴⁶⁾. Sådanne alternative, mindre indgribende kilder og metoder skal prioriteres, når de er tilgængelige ⁽²⁴⁷⁾.
- (139) Når indsamling af signalefterretninger anses for nødvendig ved anvendelsen af disse kriterier, skal den være så »målrettet som muligt« og må ikke i uforholdsmæssig grad påvirke privatlivets fred og de borgerlige frihedsrettigheder ⁽²⁴⁸⁾. For at sikre, at privatlivets fred og de borgerlige frihedsrettigheder ikke påvirkes uforholdsmæssigt — dvs. for at finde en passende balance mellem nationale sikkerhedsbehov og beskyttelsen af privatlivets fred og de borgerlige frihedsrettigheder — skal der tages behørigt hensyn til alle relevante faktorer, såsom arten af det forfulgte mål, indsamlingens indgribende karakter, herunder dens varighed, indsamlingens sandsynlige bidrag til opnåelsen af det forfulgte mål, de konsekvenser for fysiske personer, der med rimelighed kan forudses, og arten og følsomheden af de oplysninger, der skal indsamles ⁽²⁴⁹⁾.

⁽²⁴¹⁾ Section 2(b)(ii) i EO 14086.

⁽²⁴²⁾ Section 102A i National Security Act og Section 2(b)(iii) i EO 14086.

⁽²⁴³⁾ I særlige tilfælde (navnlig når en sådan proces ikke kan gennemføres på grund af et behov for at imødekomme et nyt efterretningsbehov eller et behov under udvikling) kan sådanne prioriteter fastsættes direkte af præsidenten eller af chefen for en af efterretningsenhederne, som i princippet skal anvende de samme kriterier som dem, der er beskrevet i Section 2(b)(iii)(A)(1)-(3), jf. Section 4(n) i EO 14086.

⁽²⁴⁴⁾ Section 2(b)(iii)(C) i EO 14086.

⁽²⁴⁵⁾ Section 2(b) og (c)(i)(A) i EO 14086.

⁽²⁴⁶⁾ Section 2(c)(i)(A) i EO 14086.

⁽²⁴⁷⁾ Section 2(c)(i)(A) i EO 14086.

⁽²⁴⁸⁾ Section 2(c)(i)(B) i EO 14086.

⁽²⁴⁹⁾ Section 2(c)(i)(B) i EO 14086.

(140) Hvad angår formen for indsamling af signalefterretninger skal indsamlingen af oplysninger i USA, som er mest relevant for den nuværende konstatering af et tilstrækkeligt beskyttelsesniveau, da den vedrører oplysninger, der er blevet overført til organisationer i USA, altid være målrettet, som forklaret nærmere i betragtning 142-153.

(141) »Masseindsamling«⁽²⁵⁰⁾ må kun gennemføres uden for USA på grundlag af EO 12333. Også i dette tilfælde skal målrettet indsamling prioriteres i henhold til EO 14086⁽²⁵¹⁾. Omvendt er masseindsamling kun tilladt, hvis de oplysninger, der er nødvendige for at fremme en valideret efterretningsprioritet, ikke med rimelighed kan opnås gennem målrettet indsamling⁽²⁵²⁾. Når det er nødvendigt at foretage masseindsamling af oplysninger uden for USA, gælder der særlige garantier i henhold til EO 14086⁽²⁵³⁾. For det første skal der anvendes metoder og tekniske foranstaltninger for at begrænse de indsamlede oplysninger til det, der er nødvendigt for at fremme en valideret efterretningsprioritet, samtidig med at indsamlingen af ikkerekvante oplysninger mindskes⁽²⁵⁴⁾. For det andet begrænser det præsidentielle dekret anvendelsen af masseindsamlede oplysninger (herunder søgninger) til seks specifikke mål, herunder beskyttelse mod terrorisme, gidseltagning og tilbageholdelse af personer, der holdes fanget af eller på vegne af en udenlandsk regering, en udenlandsk organisation eller en udlænding, beskyttelse mod udenlandsk spionage, sabotage eller mord, beskyttelse mod trusler som følge af udvikling, besiddelse eller spredning af masseødelæggelsesvåben eller relaterede teknologier og trusler osv.⁽²⁵⁵⁾ Endelig må enhver søgning i masseindsamlede signalefterretninger kun finde sted, når det er nødvendigt for at fremme en valideret efterretningsprioritet, med henblik på at nå disse seks mål og i overensstemmelse med politikker og procedurer, der tager behørigt hensyn til søgningernes indvirkning på privatlivets fred og de borgerlige frihedsrettigheder for alle personer, uanset deres nationalitet og opholdssted⁽²⁵⁶⁾.

(142) Ud over kravene i EO 14086 er signalefterretningsindsamling af oplysninger, der er blevet overført til en organisation i USA, underlagt specifikke begrænsninger og garantier i henhold til Section 702 i FISA⁽²⁵⁷⁾. Section 702 i FISA gør det muligt at indsamle udenlandske efterretningsoplysninger ved at foretage målrettet overvågning af ikkeamerikanske personer, der med rimelighed kan formodes at befinde sig uden for USA, med påbudt bistand fra amerikanske udbydere af elektroniske kommunikationstjenester⁽²⁵⁸⁾. Med henblik på at indsamle udenlandske efterretningsoplysninger i henhold til Section 702 i FISA indsender den amerikanske justitsminister og direktøren for den nationale efterretningstjeneste årlige certificeringer til den amerikanske domstol for overvågning

⁽²⁵⁰⁾ Dvs. indsamling af store mængder signalefterretninger, der på grund af tekniske eller operationelle forhold foretages uden brug af diskriminanter (f.eks. uden brug af specifikke identifikatorer eller selektorer), jf. Section 4(b) i EO 14086. I henhold til EO 14086 og som nærmere forklaret i betragtning 141 finder masseindsamling i henhold til EO 12333 kun sted, når det er nødvendigt for at fremme specifikke validerede efterretningsprioriteter, og den er underlagt en række begrænsninger og garantier, der skal sikre, at der ikke gives adgang til oplysninger på et vilkårligt grundlag. Masseindsamling skal derfor holdes adskilt fra indsamling, der finder sted på et generelt og vilkårligt grundlag (»masseovervågning«) uden begrænsninger og garantier.

⁽²⁵¹⁾ Section 2(c)(ii)(A) i EO 14086.

⁽²⁵²⁾ Section 2(c)(ii)(A) i EO 14086.

⁽²⁵³⁾ De specifikke regler for masseindsamling i EO 14086 finder også anvendelse på en målrettet indsamling af signalefterretninger, som midlertidigt anvender data, der er indsamlet uden forskelsbehandling (f.eks. specifikke selektorer eller identifikatorer), dvs. masseindsamling (hvilket kun er muligt uden for USA's område). Dette er ikke tilfældet, når sådanne data kun anvendes til at understøtte den indledende tekniske fase af den målrettede indsamling af signalefterretninger, kun opbevares i en kort periode, der er nødvendig for at afslutte denne fase, og slettes umiddelbart derefter (Section 2(c)(ii)(D) EO 14086). I dette tilfælde er det eneste formål med den første indsamling uden forskelsbehandling at muliggøre en målrettet indsamling af oplysninger ved at anvende en specifik identifikator eller selektor. I et sådant scenarie indlæses kun oplysninger, der reagerer ved anvendelse af en bestemt diskriminant, i statslige databaser, mens de resterende oplysninger destrueres. En sådan målrettet indsamling er derfor fortsat underlagt de generelle regler, der gælder for indsamling af signalefterretninger, herunder Section 2(a) og 2(c)(i) i EO 14086.

⁽²⁵⁴⁾ Section 2(c)(ii)(A) i EO 14086.

⁽²⁵⁵⁾ Section 2(c)(ii)(B) i EO 14086. Hvis der opstår nye trusler mod den nationale sikkerhed, kan præsidenten ajourføre denne liste. Sådanne ajourføringer skal i princippet offentliggøres, medmindre præsidenten fastslår, at dette i sig selv ville udgøre en risiko for USA's nationale sikkerhed (Section 2(c)(ii)(C) EO 14086). Hvad angår søgninger i masseindsamlede oplysninger, jf. Section 2(c)(iii)(D) i EO 14086.

⁽²⁵⁶⁾ Section 2(a)(ii)(A), sammenholdt med Section 2(c)(iii)(D) i EO 14086. Jf. også bilag VII.

⁽²⁵⁷⁾ 50 U.S.C. § 1881.

⁽²⁵⁸⁾ 50 U.S.C. § 1881a (a). Som påpeget af PCLOB er overvågning i henhold til Section 702 navnlig »udelukkende rettet mod specifikke [ikkeamerikanske] personer, som er blevet individuelt identificeret« (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 in the Foreign Intelligence Surveillance Act, 2.7.2014, Section 702 Report, s. 111). Jf. ligeledes NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.4.2014. Udtrykket »udbydere af elektroniske kommunikationstjenester« er defineret i 50 U.S.C. § 1881 (a)(4).

af efterretningsvirksomhed i udlandet (Foreign Intelligence Surveillance Court (FISC)), som identificerer kategorier af udenlandske efterretningsoplysninger, der skal indhentes ⁽²⁵⁹⁾. Certificeringerne skal ledsages af målretnings-, minimerings- og søgningsprocedurer, som også godkendes af domstolen og er juridisk bindende for amerikanske efterretningstjenester.

- (143) FISC er en uafhængig domstol ⁽²⁶⁰⁾ oprettet ved føderal lov, hvis afgørelser kan indbringes for appeldomstolen for overvågning af efterretningsvirksomhed i udlandet (Foreign Intelligence Court of Review (FISCR)) ⁽²⁶¹⁾ og i sidste ende for De Forenede Staters højesteret (Supreme Court of the United States) ⁽²⁶²⁾. FISC (og FISCR) understøttes af et fast panel bestående af fem advokater og fem tekniske eksperter i national sikkerhed og borgerlige frihedsrettigheder ⁽²⁶³⁾. Domstolen udnævner en person fra denne gruppe til at optræde som *amicus curiae* og bistå ved behandlingen af en anmodning om en kendelse eller prøvelse, der efter domstolens opfattelse udgør en ny eller væsentlig fortolkning af lovbestemmelser, medmindre domstolen finder, at en sådan udnævnelse ikke er hensigtsmæssig ⁽²⁶⁴⁾. Dette sikrer navnlig, at hensynet til privatlivets fred afspejles behørigt i domstolens vurdering. Domstolen kan ligeledes udpege en person eller en organisation til at optræde som *amicus curiae*, herunder til at bistå med teknisk ekspertise, når den finder det hensigtsmæssigt, eller på begæring tillade personer eller organisationer at indgive *amicus curiae*-indlæg ⁽²⁶⁵⁾.

- (144) FISC gennemgår certificeringerne og de dermed forbundne procedurer (navnlig målretnings- og minimeringsprocedurer) for overholdelse af kravene i FISA. Hvis domstolen mener, at kravene ikke er opfyldt, kan den helt eller delvist afvise certificeringen og anmode om, at procedurerne ændres ⁽²⁶⁶⁾. I denne forbindelse har FISC gentagne gange bekræftet, at dets gennemgang af målretnings- og minimeringsprocedurer i henhold til Section 702 ikke er begrænset til de nedskrevne procedurer, men også omfatter regeringens gennemførelse af procedurerne ⁽²⁶⁷⁾.

- (145) Individuelle afgørelser om målrettet overvågning træffes af National Security Agency (NSA, den efterretningstjeneste, der er ansvarlig for målretning i henhold til Section 702 i FISA) i overensstemmelse med FISC-godkendte målretningsprocedurer, som kræver, at NSA på grundlag af samtlige omstændigheder vurderer, at det er sandsynligt, at målretning mod en bestemt person vil udmønte sig i modtagelse af en kategori af udenlandske efterretningsoplysninger, der er identificeret i en certificering ⁽²⁶⁸⁾. Denne vurdering skal være specifik, baseret på kendsgerninger

⁽²⁵⁹⁾ 50 U.S.C. § 1881a (g).

⁽²⁶⁰⁾ FISC består af dommere udnævnt af USA's højesteretspræsident blandt siddende amerikanske distriktsdommere, der er blevet udnævnt af præsidenten og godkendt af Senatet. Dommerne er ansat i livstidsstillinger og kan kun afsættes med god grund, og de sidder ved FISC i forskudte syvårige embedsperioder. I henhold til FISA skal dommerne hentes fra mindst syv forskellige amerikanske retskredse. Jf. 50 U.S.C. § 1803 (a). Dommerne bistås af erfarne dommerfuldmægtige, der udgør domstolens retspersonale og udarbejder juridiske analyser af anmodninger om indsamling. Jf. brev fra Reggie B. Walton, retspræsident for U.S. Foreign Intelligence Surveillance Court, til Patrick J. Leahy, formand for retsudvalget i det amerikanske Senat (29.7.2013) (Walton-brevet), s. 2, findes på <https://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

⁽²⁶¹⁾ FISCR består af dommere udnævnt af USA's højesteretspræsident og hentet fra amerikanske distriktsdomstole eller appeldomstole, og de sidder i en forskudt syvårig embedsperiode. Jf. 50 U.S.C. § 1803 (b).

⁽²⁶²⁾ Jf. 50 U.S.C. § 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

⁽²⁶³⁾ 50 U.S.C. § 1803 (i)(1),(3)(A).

⁽²⁶⁴⁾ 50 U.S.C. § 1803 (i)(2)(A).

⁽²⁶⁵⁾ 50 U.S.C. § 1803 (i)(2)(B).

⁽²⁶⁶⁾ Jf. f.eks. FISC's udtalelse af 18. oktober 2018, som findes på https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, som bekræftet af Foreign Intelligence Court of Reviews udtalelse af 12. juli 2019, som findes på https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

⁽²⁶⁷⁾ Jf. f.eks. FISC, Memorandum Opinion and Order, s. 35 (18.11.2020) (offentlig frigivelse tilladt den 26.4.2021), (bilag D).

⁽²⁶⁸⁾ 50 U.S.C. § 1881a(a), Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, of March 2018 (NSA's målretningsprocedurer), findes på: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, s. 1-4, nærmere forklaret i PCLOB-rapporten, s. 41-42.

og udfærdiget på grundlag af en analytisk vurdering, analytikerens specialuddannelse og erfaring samt arten af de udenlandske efterretningsoplysninger, der skal indhentes ⁽²⁶⁹⁾. Måltreningen foretages ved at fastlægge såkaldte selektorer, der identificerer specifikke kommunikationsfaciliteter, såsom målets e-mailadresse eller telefonnummer, men aldrig nøgleord eller navne på enkeltpersoner ⁽²⁷⁰⁾.

- (146) NSA-analytikere vil først identificere ikkeamerikanske personer uden for USA, hvor en overvågning ifølge analytikernes vurdering vil resultere i indsamling af relevante udenlandske efterretningsoplysninger som præciseret i certificeringen ⁽²⁷¹⁾. Som det fremgår af NSA's målretningsprocedurer, kan NSA kun overvåge et mål, når det ved noget om målet ⁽²⁷²⁾. Denne viden kan følge af oplysninger fra forskellige kilder, f.eks. menneskelige efterretninger. Gennem disse andre kilder skal analytikeren også indhente viden om en specifik selektor (dvs. kommunikationskonto), der anvendes af det potentielle mål. Når disse individualiserede personer er blevet identificeret og den målrettede overvågning godkendt på grundlag af en omfattende evalueringsmekanisme i NSA ⁽²⁷³⁾, vil de selektorer, der identificerer de kommunikationsfaciliteter (f.eks. e-mailadresser), som anvendes af målene, derefter blive aktiveret (dvs. udviklet og anvendt) ⁽²⁷⁴⁾.

- (147) NSA skal dokumentere det faktuelle grundlag for udvælgelsen af målet ⁽²⁷⁵⁾ og med jævne mellemrum efter den første målrettede overvågning bekræfte, at målretningsstandarden fortsat er opfyldt ⁽²⁷⁶⁾. Så snart målretningsstandarden ikke længere er opfyldt, skal indsamlingen indstilles ⁽²⁷⁷⁾. NSA's udvælgelse af hvert enkelt mål og dets optegnelser over hver enkelt registreret målsætningsvurdering og -begrundelse gennemgås hver anden måned hvad angår overholdelsen af målretningsprocedurerne af embedsmænd i justitsministeriets efterretningstilsynsmyndigheder, som er forpligtet til at indberette enhver overtrædelse til FISC og Kongressen ⁽²⁷⁸⁾. NSA's skriftlige dokumentation gør det lettere for FISC at føre tilsyn med, om specifikke personer er velegnede mål i henhold til Section 702 i FISA, i overensstemmelse med de tilsynsbeføjelser, der er beskrevet i betragtning 173-174 ⁽²⁷⁹⁾. Endelig skal direktøren for den nationale efterretningstjeneste (DNI) også hvert år indberette det samlede antal mål i henhold til Section 702 i FISA i offentlige årlige statistiske rapporter om gennemsigtighed. Virksomheder, der modtager direktiver i henhold til Section 702 i FISA, kan offentliggøre aggregerede data (via gennemsigtighedsrapporter) om de anmodninger, de modtager ⁽²⁸⁰⁾.

⁽²⁶⁹⁾ NSA's målretningsprocedurer, s. 4.

⁽²⁷⁰⁾ Jf. PCLOB, Section 702 Report, s. 32-33 og 45 med yderligere henvisninger. Jf. ligeledes Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, s. 41 (oktober 2018), findes på https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

⁽²⁷¹⁾ PCLOB, Section 702 Report, s. 42-43.

⁽²⁷²⁾ NSA's målretningsprocedurer, s. 2.

⁽²⁷³⁾ PCLOB, Section 702 Report, s. 46. NSA skal f.eks. kontrollere, at der er en forbindelse mellem målet og selektoren, og dokumentere de udenlandske efterretningsoplysninger, som forventes at blive indhentet, og disse oplysninger skal gennemgås og godkendes af to ledende analytikere i NSA, og ODNI og det amerikanske justitsministerium vil spore hele processen ved efterfølgende kontrol af overholdelsen. Jf. NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.4.2014.

⁽²⁷⁴⁾ 50 U.S.C. § 1881a (h).

⁽²⁷⁵⁾ NSA's målretningsprocedurer, s. 8. Jf. også PCLOB, Section 702 Report, s. 46. Manglende skriftlig begrundelse udgør et tilfælde af manglende dokumentation, der skal indberettes til FISC og Kongressen. Jf. Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, s. 41 (oktober 2018), DoJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017, s. A-6, findes på https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

⁽²⁷⁶⁾ Jf. den amerikanske regerings indlæg til den amerikanske domstol for overvågning af efterretningsvirksomhed i udlandet, 2015 Summary of Notable Section 702 Requirements, s. 2-3 (15.7.2015), og oplysningerne i bilag VII.

⁽²⁷⁷⁾ Jf. den amerikanske regerings indlæg til den amerikanske domstol for overvågning af efterretningsvirksomhed i udlandet, 2015 Summary of Notable Section 702 Requirements, s. 2-3 (15.7.2015), hvori det hedder, at »hvis regeringen senere vurderer, at den fortsatte aktivering af et måls selektor ikke forventes at resultere i indhentning af udenlandske efterretningsoplysninger, skal selektoren omgående deaktiveres, og enhver forsinkelse kan medføre et indberetningspligtigt tilfælde af manglende overholdelse«. Jf. ligeledes oplysningerne i bilag VII.

⁽²⁷⁸⁾ PCLOB, Section 702 Report, s. 70-72, Regel 13(b) i procedurereglerne for den amerikanske domstol for overvågning af efterretningsvirksomhed i udlandet, som findes på <https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

⁽²⁷⁹⁾ Jf. endvidere DoJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017, s. A-6.

⁽²⁸⁰⁾ 50 U.S.C. § 1874.

- (148) Hvad angår de andre retsgrundlag for indsamling af personoplysninger, der overføres til organisationer i USA, gælder der forskellige begrænsninger og garantier. Generelt er masseindsamling af oplysninger og anvendelse af NSL specifikt forbudt i henhold til Section 402 i FISA (pen-register- og trap and trace-tilladelse), idet der i stedet anvendes specifikke »selektorer«⁽²⁸¹⁾.
- (149) For at udføre traditionel individualiseret elektronisk overvågning (i henhold til Section 105 i FISA) skal efterretnings-tjenesterne indgive en anmodning til FISC med en erklæring om de faktiske forhold og omstændigheder, der gøres gældende som begrundelse for den antagelse, at der er begrundet mistanke om, at faciliteten anvendes eller snart vil blive anvendt af en fremmed magt eller en agent fra en fremmed magt⁽²⁸²⁾. FISC vil bl.a. vurdere, om der på grundlag af de forelagte faktiske forhold er begrundet mistanke om, at dette reelt er tilfældet⁽²⁸³⁾.
- (150) For at foretage ransagning af lokaler eller ejendom, der skal føre til inspektion, beslaglæggelse m.v. af oplysninger, materiale eller ejendom (f.eks. computerudstyr) på grundlag af Section 301 i FISA, kræves der en anmodning om et pålæg fra FISC⁽²⁸⁴⁾. En sådan anmodning skal bl.a. påvise, at der er en begrundet mistanke om, at målet for ransagningen er en fremmed magt eller en agent for en fremmed magt, at det lokale eller den ejendom, der skal ransages, indeholder udenlandske efterretningsoplysninger, og at det lokale, der skal ransages, ejes eller bruges af eller er i transit til eller fra en (agent fra en) fremmed magt eller er i dennes besiddelse⁽²⁸⁵⁾.
- (151) Tilsvarende kræver installation af pen-register- eller trap and trace-anordninger (i henhold til Section 402 i FISA), at der indgives en anmodning til FISC (eller en amerikansk undersøgelsesdommer) om en afgørelse, og at der anvendes en specifik selektor, dvs. en term, der specifikt identificerer en person, konto osv., og som anvendes til at begrænse mængden af indhentede oplysninger i muligt og rimeligt omfang⁽²⁸⁶⁾. Denne tilladelse vedrører ikke kommunikationens indhold, men derimod oplysninger om den kunde eller abonnent, der anvender en tjeneste (såsom navn, adresse, abonnentnummer, den modtagne tjenestes længde/type, betalingskilde/-mekanisme).
- (152) I henhold til Section 501 i FISA⁽²⁸⁷⁾, som giver mulighed for indsamling af forretningsoplysninger fra en transportvirksomhed (dvs. enhver person eller enhed, der transporterer personer eller ejendom med bil, tog, skib eller fly mod vederlag), offentlig indkvarteringsfacilitet (f.eks. hotel, motel eller kro), biludlejningsfacilitet eller fysisk lagerfacilitet (dvs. som udbyder plads til eller tjenesteydelser i forbindelse med oplagring af varer og materialer)⁽²⁸⁸⁾, skal der også indgives en anmodning til FISC eller en undersøgelsesdommer. Denne anmodning skal indeholde oplysninger om de ønskede optegnelser og de specifikke og præcise faktiske forhold, der giver grund til at antage, at den person, som optegnelserne vedrører, er en fremmed magt eller en agent for en fremmed magt⁽²⁸⁹⁾.
- (153) Endelig er NSL tilladt i henhold til forskellige lovbestemmelser og giver efterforskningsorganer mulighed for at indhente visse oplysninger (bortset fra indholdet af kommunikation) fra visse enheder (f.eks. finansielle institutioner, kreditoplysningsbureauer, udbydere af elektronisk kommunikation), der er indeholdt i kreditoplysninger, finansielle oplysninger og elektroniske abonnent- og transaktionsoplysninger⁽²⁹⁰⁾. Loven om NSL, der tillader indsigt i elektronisk kommunikation, må kun anvendes af FBI og kræver, at anmodninger anvender en term, der specifikt identificerer en person, en enhed, et telefonnummer eller en konto og attesterer, at oplysningerne er af relevans for en godkendt national sikkerhedsundersøgelse med henblik på beskyttelse mod international terrorisme eller hemmelige efterretningsaktiviteter⁽²⁹¹⁾. Modtagere af et NSL kan anfægte det ved domstolene⁽²⁹²⁾.

⁽²⁸¹⁾ 50 U.S.C. § 1842(c)(3), og 12 U.S.C. § 3414(a)(2) for så vidt angår NSL, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v(a) og 18 U.S.C. § 2709(a).

⁽²⁸²⁾ »En agent fra en fremmed magt« kan omfatte ikkeamerikanske personer involveret i international terrorisme eller international spredning af masseødelæggelsesvåben (herunder forberedende foranstaltninger) (50 U.S.C. § 1801 (b)(1)).

⁽²⁸³⁾ 50 U.S.C. § 1804. Jf. ligeledes § 1841(4) hvad angår valget af selektorer.

⁽²⁸⁴⁾ 50 U.S.C. § 1821(5).

⁽²⁸⁵⁾ 50 U.S.C. § 1823(a).

⁽²⁸⁶⁾ 50 U.S.C. § 1842, sammenholdt med § 1841(2) og Section 3127 i Title 18.

⁽²⁸⁷⁾ 50 U.S.C. § 1862.

⁽²⁸⁸⁾ 50 U.S.C. § 1861-1862.

⁽²⁸⁹⁾ 50 U.S.C. § 1862(b).

⁽²⁹⁰⁾ 12 U.S.C. § 3414, 15 U.S.C. § 1681u-1681v og 18 U.S.C. § 2709.

⁽²⁹¹⁾ 18 U.S.C. § 2709(b).

⁽²⁹²⁾ F.eks. 18 U.S.C. § 2709(d).

3.2.1.3 Videre anvendelse af de indsamlede oplysninger

- (154) Behandlingen af personoplysninger, som amerikanske efterretningstjenester indsamler gennem signalefterretninger, er underlagt en række sikkerhedsforanstaltninger.
- (155) For det første skal de enkelte efterretningstjenester sørge for passende datasikkerhed og forhindre uautoriserede personer i at få adgang til personoplysninger indsamlet gennem signalefterretninger. I denne forbindelse præciserer forskellige instrumenter, herunder lovbestemmelser, retningslinjer og standarder, de mindstekrav til informations-sikkerhed, der skal indføres (f.eks. multifaktorgodkendelse, kryptering osv.) ⁽²⁹³⁾. Indsigt i indsamlede oplysninger skal begrænses til autoriseret, uddannet personale, der har brug for oplysningerne for at varetage deres opgaver ⁽²⁹⁴⁾. Mere generelt skal efterretningstjenesterne sørge for passende uddannelse af deres ansatte, herunder i procedurer for indberetning og håndtering af lovovertrædelser (herunder EO 14086) ⁽²⁹⁵⁾.
- (156) For det andet skal efterretningstjenesterne overholde efterretningssamfundets standarder for nøjagtighed og objektivitet, navnlig med hensyn til at sikre oplysningernes kvalitet og pålidelighed, hensyntagen til alternative informationskilder og objektivitet ved udførelsen af analyser ⁽²⁹⁶⁾.
- (157) For det tredje præciseres det i EO 14086 for så vidt angår opbevaring af data, at personoplysninger om ikkeamerikanske personer er omfattet af de samme opbevaringsperioder som dem, der gælder for oplysninger om amerikanere ⁽²⁹⁷⁾. Efterretningstjenester skal definere specifikke opbevaringsperioder og/eller de faktorer, der skal tages i betragtning ved fastsættelsen af længden af de gældende opbevaringsperioder (f.eks. om oplysningerne er bevis for en forbrydelse, om oplysningerne udgør udenlandske efterretningsoplysninger, om oplysningerne er nødvendige for at beskytte sikkerheden for personer eller organisationer, herunder ofre for eller mål for international terrorisme), som er fastsat i forskellige retlige instrumenter ⁽²⁹⁸⁾.
- (158) For det fjerde gælder der særlige regler for videregivelse af personoplysninger indsamlet gennem signalefterretninger. Som et generelt krav må personoplysninger om ikkeamerikanske personer kun videregives, hvis de omfatter samme type oplysninger som dem, der må videregives om amerikanere, f.eks. oplysninger, der er nødvendige for at beskytte en persons eller en organisations sikkerhed (f.eks. internationale terrororganisationers mål, ofre eller gidsler) ⁽²⁹⁹⁾. Derudover må personoplysninger ikke videregives alene på grund af en persons nationalitet eller opholdssted eller med det formål at omgå kravene i EO 14086 ⁽³⁰⁰⁾. Videregivelse inden for den amerikanske regering må kun finde sted, hvis en autoriseret og uddannet person har rimelig grund til at antage, at modtageren har behov for at kende

⁽²⁹³⁾ Section 2(c)(iii)(B)(1) i EO 14086. Jf. også Title VIII i National Security Act (med nærmere oplysninger om de krav, der skal være opfyldt for at få indsigt i klassificerede oplysninger), EO 12333 Section 1.5 (som kræver, at lederne af efterretningstjenesterne skal følge retningslinjerne for informationsudveksling og -sikkerhed, beskyttelse af privatlivets fred med hensyn til oplysninger og andre retlige krav), nationalt sikkerhedsdirektiv 42, »National Policy for the Security of National Security Telecommunications and Information Systems« (der pålægger udvalget for nationale sikkerhedssystemer at vejlede administrative afdelinger og agenturer i systemsikkerhed for nationale sikkerhedssystemer) og nationalt sikkerhedsmemorandum 8, »Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems« (som fastsætter tidsfrister og retningslinjer for, hvordan cybersikkerhedskrav implementeres for nationale sikkerhedssystemer, herunder multifaktorgodkendelse, kryptering, cloudteknologier og endpointdetektionstjenester).

⁽²⁹⁴⁾ Section 2(c)(iii)(B)(2) i EO 14086. Derudover må personoplysninger, for hvilke der ikke er truffet en endelig afgørelse om opbevaring, kun tilgås for at træffe eller understøtte en sådan afgørelse eller for at udføre autoriserede administrative funktioner eller test-, udviklings-, sikkerheds- eller tilsynsfunktioner (Section 2(c)(iii)(B)(3) i EO 14086).

⁽²⁹⁵⁾ Section 2(d)(ii) i EO 14086.

⁽²⁹⁶⁾ Section 2(c)(iii)(C) i EO 14086.

⁽²⁹⁷⁾ Section 2(c)(iii)(A)(2)(a)-(c) i EO 14086. Mere generelt skal hver tjeneste indføre politikker og procedurer, der har til formål at minimere videregivelsen og opbevaringen af personoplysninger indsamlet gennem signalefterretninger (Section 2(c)(iii)(A) i EO 14086).

⁽²⁹⁸⁾ Jf. f.eks. Section 309 i Intelligence Authorization Act for Fiscal Year 2015, minimeringsprocedurer, der er vedtaget af de enkelte efterretningstjenester i henhold til Section 702 i FISA og godkendt af FISC, procedurer godkendt af den amerikanske justitsminister og FRA (krav om, at amerikanske føderale myndigheder, herunder nationale sikkerhedsagenturer, skal fastsætte opbevaringsperioder for deres registre, som skal godkendes af National Archives and Record Administration).

⁽²⁹⁹⁾ Section 2(c)(iii)(A)(1)(a) og 5(d) i EO 14086, sammenholdt med Section 2.3 i EO 12333.

⁽³⁰⁰⁾ Section 2(c)(iii)(A)(1)(b) og (e) i EO 14086.

oplysningerne ⁽³⁰¹⁾ og vil beskytte dem på passende vis ⁽³⁰²⁾. For at afgøre, om personoplysninger kan videregives til modtagere uden for den amerikanske regering (herunder en udenlandsk regering eller international organisation), skal der tages hensyn til formålet med videregivelsen, arten og omfanget af de oplysninger, der videregives, og den potentielle skadelige indvirkning på den eller de berørte personer ⁽³⁰³⁾.

- (159) Endelig skal de enkelte efterretningstjenester, herunder for at lette tilsynet med overholdelsen af de gældende retlige krav og sikre effektiv klageadgang, i henhold til EO 14086 opbevare passende dokumentation om indsamlingen af signalefterretninger. Dokumentationskravene omfatter elementer såsom det faktuelle grundlag for den vurdering, hvorefter en specifik indsamlingsaktivitet er nødvendig for at fremme en valideret efterretningsprioritet ⁽³⁰⁴⁾.
- (160) Ud over ovennævnte garantier i EO 14086 for anvendelse af oplysninger indsamlet gennem signalefterretninger er alle amerikanske efterretningstjenester underlagt mere generelle krav om formålsbegrænsning, dataminimering, nøjagtighed, sikkerhed, opbevaring og formidling, navnlig i henhold til OMB-cirkulære nr. A-130, E-Government Act, Federal Records Act (se betragtning 101-106) og retningslinjer fra udvalget for nationale sikkerhedssystemer (CNSS) ⁽³⁰⁵⁾.

3.2.2 Tilsyn

- (161) De amerikanske efterretningstjenesters aktiviteter er underlagt forskellige organers tilsyn.
- (162) For det første kræver EO 14086, at de enkelte efterretningstjenester har ledende juridiske samt tilsyns- og kontrolansvarlige embedsmænd, som sikrer, at gældende amerikansk lovgivning overholdes ⁽³⁰⁶⁾. De skal navnlig føre regelmæssigt tilsyn med signalefterretningsaktiviteter og sikre, at enhver manglende overholdelse afhjælpes. Efterretningstjenesterne skal give sådanne embedsmænd adgang til alle relevante oplysninger, så de kan udføre deres tilsynsfunktioner, og må ikke træffe foranstaltninger for at hindre eller påvirke deres tilsynsaktiviteter uretmæssigt ⁽³⁰⁷⁾. Endvidere skal alle væsentlige tilfælde af manglende overholdelse ⁽³⁰⁸⁾, som en tilsynsembedsmand eller en anden medarbejder konstaterer, straks indberettes til lederen af efterretningstjenesten og direktøren for den nationale efterretningstjeneste, som skal sikre, at alle nødvendige foranstaltninger træffes for at afhjælpe og forhindre en gentagelse af det væsentlige tilfælde af manglende overholdelse ⁽³⁰⁹⁾.
- (163) Denne tilsynsfunktion varetages af embedsmænd, der er udpeget til at varetage en kontrollfunktion, samt af databeskyttelsesansvarlige og generalinspektører ⁽³¹⁰⁾.
-
- ⁽³⁰¹⁾ Se f.eks. AGG-DOM, hvori det fastlægges, at FBI kun må formidle oplysninger, hvis modtageren har behov for at kende dem, for at modtageren kan udføre sin opgave eller beskytte offentligheden.
- ⁽³⁰²⁾ Section 2(c)(iii)(A)(1)(c) i EO 14086. Efterretningsagenturer kan f.eks. formidle oplysninger under omstændigheder, der er relevante for en strafferetlig efterforskning, eller som vedrører en forbrydelse, f.eks. ved at udsende advarsler om trusler om drab, alvorlig legemsbeskadigelse eller kidnapning, formidling af oplysninger om cybertrusler, cyberhændelser eller reaktioner på indtrængen og underretning af ofre eller varsling af potentielle ofre for kriminalitet.
- ⁽³⁰³⁾ Section 2(c)(iii)(A)(1)(d) i EO 14086.
- ⁽³⁰⁴⁾ Section 2(c)(iii)(E) i EO 14086.
- ⁽³⁰⁵⁾ Se CNSS Policy No. 22, Cybersecurity Risk Management Policy og CNSS Instruction 1253, som indeholder detaljerede retningslinjer for sikkerhedsforanstaltninger, der skal indføres for nationale sikkerhedssystemer.
- ⁽³⁰⁶⁾ Section 2(d)(i)(A)-(B) i EO 14086.
- ⁽³⁰⁷⁾ Section 2(d)(i)(B)-(C) i EO 14086.
- ⁽³⁰⁸⁾ Dvs. en systemisk eller forsætlig tilsidesættelse af gældende amerikansk lovgivning, der kan så tvivl om en efterretningsenheds omdømme eller integritet eller på anden vis rejse tvivl om sømmeligheden af en af efterretningstjenestens aktiviteter, herunder i lyset af enhver væsentlig indvirkning på den eller de berørte personers interesser med hensyn til privatlivets fred og borgerlige frihedsrettigheder, jf. Section 5(l) i EO 14086.
- ⁽³⁰⁹⁾ Section 2(d)(iii) i EO 14086.
- ⁽³¹⁰⁾ Section 2(d)(i)(B) i EO 14086.

- (164) Som det er tilfældet med de strafferetlige håndhævende myndigheder, findes der databeskyttelsesansvarlige i alle efterretningstjenester ⁽³¹¹⁾. Disse embedsmænds beføjelser omfatter typisk tilsynet med procedurer for at sikre, at det pågældende ministerium/organ tager tilstrækkeligt hensyn til beskyttelsen af privatlivets fred og borgerlige frihedsrettigheder, og at der er indført passende procedurer for behandling af klager fra fysiske personer, der mener, at deres privatliv eller borgerlige frihedsrettigheder er blevet krænkede (og i nogle tilfælde har de selv beføjelse til at undersøge klager, f.eks. direktøren for den nationale efterretningstjeneste (ODNI) ⁽³¹²⁾). Lederne af efterretningstjenesterne skal sikre, at de databeskyttelsesansvarlige har ressourcer til at varetage deres mandat, at de får adgang til alt materiale og personale, der er nødvendigt for at udføre deres opgaver, og at de informeres og høres om foreslåede politiske ændringer ⁽³¹³⁾. De databeskyttelsesansvarlige rapporterer regelmæssigt til den amerikanske Kongres og til PCLOB, herunder om antallet og karakteren af de klager, som ministeriet/organet har modtaget, med en oversigt over afgørelserne i disse klagesager, de gennemførte undersøgelser og forespørgsler og resultaterne af deres aktiviteter ⁽³¹⁴⁾.
- (165) For det andet har hver efterretningstjeneste en uafhængig generalinspektør med ansvar for bl.a. tilsyn med udenlandske efterretningsaktiviteter. Dette omfatter inden for ODNI et generalinspektorat for efterretnings-samfundet (Office of the Inspector General of the Intelligence Community), som har brede beføjelser til at føre tilsyn med hele den amerikanske efterretningstjeneste og til at undersøge klager eller oplysninger om påstande om ulovlig praksis eller magtmisbrug i forbindelse med ODNI's og/eller efterretningstjenestens programmer og aktiviteter ⁽³¹⁵⁾. Som det er tilfældet med de strafferetlige håndhævende myndigheder (jf. betragtning 109), er sådanne generalinspektører lovmæssigt uafhængige ⁽³¹⁶⁾ og har ansvar for revisioner og undersøgelser af de programmer og operationer, den pågældende tjeneste gennemfører til nationale efterretningsformål, herunder af misbrug og lovovertrædelser ⁽³¹⁷⁾. De har adgang til alle optegnelser, rapporter, revisioner, evalueringer, dokumenter,
-
- ⁽³¹¹⁾ Jf. 42 U.S.C. § 2000ee-1. Herunder udenrigsministeriet (Department of State), justitsministeriet, ministeriet for national sikkerhed, forsvarsministeriet (Department of Defense), NSA, Central Intelligence Agency (CIA), FBI og ODNI.
- ⁽³¹²⁾ Jf. Section 3(c) i EO 14086.
- ⁽³¹³⁾ 42 U.S.C. § 2000ee-1(d).
- ⁽³¹⁴⁾ Jf. 42 U.S.C. § 2000ee-1 (f)(1),(2). Det fremgår f.eks. af rapporten fra NSA's kontor for borgerlige frihedsrettigheder, privatlivets fred og gennemsigtighed (Civil Liberties, Privacy and Transparency Office), der dækker januar 2021-juni 2021, at det gennemførte 591 undersøgelser af de borgerlige frihedsrettigheder og privatlivets fred i forskellige sammenhænge, f.eks. med hensyn til indsamlingsaktiviteter, informationsudvekslingsordninger og -afgørelser, afgørelser om opbevaring af data osv., idet der blev taget hensyn til forskellige faktorer såsom mængden og typen af oplysninger, der var knyttet til aktiviteten, de involverede personer, formålet med og den forventede anvendelse af oplysningerne, de eksisterende sikkerhedsforanstaltninger til afhjælpning af potentielle risici for privatlivets fred osv. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%20CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Tilsvarende indeholder rapporterne fra CIA's kontor for privatlivets fred og borgerlige frihedsrettigheder (Office of Privacy and Civil Liberties) for januar-juni 2019 oplysninger om kontorets tilsynsaktiviteter, f.eks. en undersøgelse af overholdelsen af justitsministerens retningslinjer under EO 12333 med hensyn til opbevaring og videregivelse af oplysninger, vejledning om gennemførelsen af PPD 28 og krav med henblik på at identificere og håndtere brud på datasikkerheden samt undersøgelser af anvendelsen og håndteringen af personoplysninger (<https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf>).
- ⁽³¹⁵⁾ Denne generalinspektør udnævnes af præsidenten med Senatets godkendelse og kan kun afsættes af præsidenten.
- ⁽³¹⁶⁾ Generalinspektørerne har et fast embede og kan kun afsættes af præsidenten, der skriftligt skal meddele den amerikanske Kongres årsagerne til denne afsættelse. Det betyder ikke nødvendigvis, at de slet ikke er underlagt instrukser. I nogle tilfælde kan lederen af ministeriet forbyde generalinspektøren at indlede, gennemføre eller afslutte en revision eller efterforskning, hvis det anses for nødvendigt for at beskytte vigtige nationale (sikkerheds)interesser. Kongressen skal imidlertid orienteres om udøvelse af denne myndighed og kan på dette grundlag holde den pågældende leder ansvarlig. Jf. f.eks. Inspector General Act af 1978, § 8 (for forsvarsministeriet), § 8E (for justitsministeriet), § 8G (d)(2)(A),(B) (for NSA), 50. U.S.C. § 403q (b) (for CIA), Intelligence Authorization Act For Fiscal Year 2010, Sec. 405(f) (for efterretningssamfundet).
- ⁽³¹⁷⁾ Inspector General Act af 1978, som ændret, Pub. L. 117-108 af 8.4.2022. Som forklaret i de halvårige rapporter til Kongressen for perioden 1.4.2021-31.3.2022 udførte NSA's generalinspektør f.eks. evalueringer af håndteringen af amerikanske personoplysninger indsamlet i henhold til EO 12333, processen med at slette signalefterretningsoplysninger, et automatiseret målretningsværktøj, som anvendes af NSA, og overholdelsen af dokumentations- og søgeregler i forbindelse med indsamling i henhold til Section 702 i FISA og fremsatte i denne forbindelse en række anbefalinger (jf. <https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d>, s. 5-8, og <https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907>, s. 10-13). Jf. også den amerikanske efterretningstjenestes generalinspektørs seneste revisioner og undersøgelser vedrørende informationsikkerhed og uautoriseret videregivelse af klassificerede nationale sikkerhedsoplysninger (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, s. 8 og 11, og https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, s. 19-20).

papirer, anbefalinger eller andet relevant materiale, om nødvendigt på grundlag af et pålæg, og kan indhente vidneudsagn⁽³¹⁸⁾. Generalinspektørerne henviser sager om formodede strafferetlige overtrædelser til retsforfølgning og fremsætter anbefalinger om korrigerende foranstaltninger for tjenesternes ledere⁽³¹⁹⁾. Selv om deres anbefalinger ikke er bindende, offentliggøres deres rapporter, herunder om opfølgende foranstaltninger (eller mangel herpå)⁽³²⁰⁾, og de fremsendes til den amerikanske Kongres, der på dette grundlag kan udøve sin tilsynsfunktion (jf. betragtning 168-169)⁽³²¹⁾.

(166) For det tredje fører Intelligence Oversight Board (IOB), som er nedsat under President's Intelligence Advisory Board (PIAB), tilsyn med de amerikanske efterretningsmyndigheders overholdelse af forfatningen og alle gældende bestemmelser⁽³²²⁾. PIAB er et rådgivende organ i præsidentens kabinet, der består af 16 medlemmer udpeget af præsidenten, som ikke er med i den amerikanske regering. IOB består af højst fem medlemmer, som er udpeget af præsidenten blandt PIAB's medlemmer. Ifølge EO 12333⁽³²³⁾ skal lederne af alle efterretningstjenester indberette enhver efterretningsaktivitet, for hvilken der er grund til at tro, at den kan være ulovlig eller i strid med et præsidentielt dekret eller direktiv, til IOB. For at sikre, at IOB har adgang til de oplysninger, der er nødvendige for, at det kan udføre sine opgaver, pålægger EO 13462 direktøren for den nationale efterretningstjeneste og lederne af efterretningstjenesterne at fremlægge alle de oplysninger og yde den bistand, som IOB finder nødvendig for at udføre sine opgaver, i det omfang det er tilladt ved lov⁽³²⁴⁾. IOB skal til gengæld underrette præsidenten om efterretningsaktiviteter, som det mener kan være i strid med amerikansk ret (herunder præsidentielle dekreter), og som ikke behandles hensigtsmæssigt af justitsministeren, direktøren for den nationale efterretningstjeneste eller lederen af en efterretningstjeneste⁽³²⁵⁾. Derudover skal IOB underrette justitsministeren om mulige overtrædelser af straffelovgivningen.

(167) For det fjerde er efterretningstjenester underlagt PCLOB's tilsyn. I henhold til PCLOB's stiftelsesdokument har rådet ansvarsområder relateret til terrorbekæmpelsespolitikker og deres gennemførelse med henblik på at beskytte privatlivets fred og borgerlige frihedsrettigheder. I forbindelse med sin revision af efterretningstjenesternes handlinger kan rådet få adgang til alle tjenesternes relevante optegnelser, rapporter, revisioner, evalueringer, dokumenter, papirer og anbefalinger, herunder klassificerede oplysninger, gennemføre interview og indhente vidneudsagn⁽³²⁶⁾. Det modtager rapporter fra databeskyttelsesansvarlige i en række føderale ministerier og organer⁽³²⁷⁾, det kan udstede anbefalinger til statslige agenturer og efterretningstjenester og rapporterer regelmæssigt til forskellige kongresudvalg og præsidenten⁽³²⁸⁾. Rådets rapporter, herunder dets rapporter til Kongressen, skal i videst muligt omfang gøres offentligt tilgængelige⁽³²⁹⁾. PCLOB har udstedt flere tilsyns- og opfølgingsrapporter, herunder en analyse af de programmer, der gennemføres på grundlag af Section 702 i FISA, og beskyttelsen af privatlivets fred i denne sammenhæng, samt om gennemførelsen af PPD 28 og EO 12333⁽³³⁰⁾.

⁽³¹⁸⁾ Jf. Inspector General Act af 1978, § 6.

⁽³¹⁹⁾ Jf. *ibid.* § 4, 6-5.

⁽³²⁰⁾ For så vidt angår opfølgningen på generalinspektørernes rapporter og anbefalinger se f.eks. svaret på en rapport fra generalinspektøren for justitsministeriet, hvori det blev konstateret, at FBI ikke havde udvist tilstrækkelig gennemsigtighed over for FISC i anmodninger fra 2014-2019, hvilket førte til reformer for at forbedre kontrollen, tilsynet og ansvaret hos FBI (f.eks. anordnede FBI's direktør mere end 40 korrigerende foranstaltninger, herunder 12, der var specifikke for FISA-proceduren vedrørende dokumentation, overvågning, filvedligeholdelse, uddannelse og revision) (jf. <https://www.justice.gov/opa/pr/departments-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance> og <https://oig.justice.gov/reports/2019/o20012.pdf>). Jf. f.eks. generalinspektøren for justitsministeriets revision af FBI's chefjurists rolle og ansvar i forbindelse med tilsynet med overholdelsen af gældende love, politikker og procedurer vedrørende FBI's nationale sikkerhedsaktiviteter og tillæg 2, som indeholder et brev fra FBI, som godkender alle anbefalinger. I den forbindelse giver tillæg 3 et overblik over den opfølgning og de oplysninger, som generalinspektøren anmodede FBI om for at kunne afslutte sine anbefalinger (<https://oig.justice.gov/sites/default/files/reports/22-116.pdf>).

⁽³²¹⁾ Jf. Inspector General Act af 1978, § 4(5), 5.

⁽³²²⁾ Jf. EO 13462.

⁽³²³⁾ Section 1.6(c) i EO 12333.

⁽³²⁴⁾ Section 8(a) i EO 13462.

⁽³²⁵⁾ Section 6(b) i EO 13462.

⁽³²⁶⁾ 42 U.S.C. § 2000ee (g).

⁽³²⁷⁾ Jf. 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Disse omfatter som minimum justitsministeriet, forsvarsministeriet, ministeriet for national sikkerhed, direktøren for den nationale efterretningstjeneste og direktøren for CIA (Central Intelligence Agency) samt andre ministerier, organer eller enheder inden for den udøvende magt, som PCLOB betragter som værende relevante i denne sammenhæng.

⁽³²⁸⁾ 42 U.S.C. § 2000ee (e).

⁽³²⁹⁾ 42 U.S.C. § 2000ee (f).

⁽³³⁰⁾ Findes på <https://www.pclob.gov/Oversight>.

PCLOB varetager endvidere specifikke tilsynsfunktioner i forbindelse med gennemførelsen af EO 14086, navnlig ved at undersøge, om organernes procedurer er i overensstemmelse med det præsidentielle dekret (jf. betragtning 126), og evaluere, om klagemekanismen fungerer korrekt (jf. betragtning 194).

- (168) For det femte fører særlige udvalg i den amerikanske Kongres (efterretnings- og retsudvalgene i Repræsentanternes Hus og Senatet), ud over tilsynsmekanismerne under den udøvende magt, tilsyn med alle amerikanske udenlandske efterretningsaktiviteter. Udvalgsmedlemmerne har både adgang til klassificerede oplysninger og til efterretningsmetoder og -programmer ⁽³³¹⁾. Udvalgene udøver deres tilsynsfunktioner på forskellig vis, navnlig gennem høringer, undersøgelser, evalueringer og rapporter ⁽³³²⁾.
- (169) Kongresudvalgene modtager regelmæssige rapporter om efterretningsaktiviteter, herunder fra justitsministeren, direktøren for den nationale efterretningstjeneste, efterretningstjenesterne og andre tilsynsorganer (f.eks. generalinspektørerne), jf. betragtning 164-165. I henhold til National Security Act »sikrer præsidenten, at Kongressens efterretningsudvalg orienteres fuldt ud og løbende om amerikanske efterretningsaktiviteter, herunder om betydelige forventede efterretningsaktiviteter som krævet i dette afsnit« ⁽³³³⁾. Det er ligeledes anført, at »præsidenten sikrer, at enhver ulovlig efterretningsaktivitet og enhver gennemført eller planlagt korrigerende foranstaltning over for denne ulovlige aktivitet straks indberettes til Kongressens efterretningsudvalg« ⁽³³⁴⁾.
- (170) Specifikke love indeholder yderligere rapporteringskrav. I henhold til FISA skal den amerikanske justitsminister navnlig »orientere« Repræsentanternes Hus' og Senatets efterretnings- og retsudvalg »fuldt ud« om regeringens aktiviteter i henhold til bestemte paragraffer i FISA ⁽³³⁵⁾. Der stilles ligeledes krav om, at regeringen giver kongresudvalgene kopier af alle afgørelser, kendelser eller udtalelser fra FISC eller FISCR, som indeholder en »væsentlig forståelse eller fortolkning« af FISA-bestemmelser. Med hensyn til overvågning i henhold til Section 702 i FISA udøves det parlamentariske tilsyn gennem lovpligtige rapporter til efterretnings- og retsudvalgene og gennem hyppige briefinger og høringer. Disse omfatter en halvårlig rapport udarbejdet af den amerikanske justitsminister om anvendelsen af Section 702 i FISA med tilhørende dokumenter, herunder justitsministeriets og ODNI's overholdelsesrapporter og en redegørelse for eventuelle tilfælde af manglende overholdelse ⁽³³⁶⁾, og en særskilt halvårlig vurdering fra den amerikanske justitsminister og DNI, der dokumenterer overholdelsen af målretnings- og minimeringsprocedurerne ⁽³³⁷⁾.

⁽³³¹⁾ 50 U.S.C. § 3091.

⁽³³²⁾ Udvalgene afholder f.eks. tematiske høringer (jf. f.eks. en nylig høring afholdt af retsudvalget i Repræsentanternes Hus om »digital klapjagt«, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>, og en høring i efterretningsudvalget i Repræsentanternes Hus om efterretningsgrundlagets brug af AI, <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263>), samt regelmæssige tilsynshøringer, f.eks. af FBI's og justitsministeriets afdeling for national sikkerhed, jf. <https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation>, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966> og <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899>. Som eksempel på en undersøgelse henvises til Senatets efterretningsudvalgs undersøgelse af russisk indblanding i det amerikanske valg i 2016, jf. <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>. For så vidt angår rapportering, jf. f.eks. oversigten over udvalgets (tilsyns)aktiviteter i rapporten fra Senatets efterretningsudvalg for perioden 4.1.2019-3.1.2021 til Senatet, <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4>.

⁽³³³⁾ Jf. 50 U.S.C. § 3091(a)(1). Denne bestemmelse indeholder generelle krav vedrørende Kongressens tilsyn med nationale sikkerhedsanliggender.

⁽³³⁴⁾ Jf. 50 U.S.C. § 3091(b).

⁽³³⁵⁾ Jf. 50 U.S.C. § 1808, 1846, 1862, 1871, 1881f.

⁽³³⁶⁾ Jf. 50 U.S.C. § 1881f.

⁽³³⁷⁾ Jf. 50 U.S.C. § 1881a(l)(1).

- (171) I henhold til FISA skal den amerikanske regering desuden hvert år bl.a. oplyse Kongressen (og offentligheden) om det antal FISA-kendelser, der er anmodet om og udstedt, og om det skønnede antal overvågede amerikanske og ikkeamerikanske personer ⁽³³⁸⁾. I loven stilles der ligeledes yderligere krav om offentliggørelse af antallet af udstedte NSL'er, også her vedrørende både amerikanske og ikkeamerikanske personer (og modtagerne af FISA-kendelser og -certificeringer og NSL-anmodninger får mulighed for at udarbejde gennemsigthedsrapporter på visse betingelser) ⁽³³⁹⁾.
- (172) Mere generelt bestræber det amerikanske efterretningssamfund sig på forskellig vis på at skabe gennemsigthed omkring dets (udenlandske) efterretningsaktiviteter. I 2015 vedtog ODNI f.eks. principperne for gennemsigthed i efterretningsoplysninger og en plan for gennemførelse af gennemsigthed og pålagde de enkelte efterretnings-tjenester at udpege en ansvarlig for gennemsigthed i efterretningsoplysninger for at fremme gennemsigtheden og gennemføre gennemsigthedsinitiativer ⁽³⁴⁰⁾. Som led i disse bestræbelser har efterretningssamfundet offentliggjort — og fortsætter med at offentliggøre — afklassificerede dele af politikker, procedurer, tilsynsrapporter, rapporter om aktiviteter i henhold til Section 702 i FISA og EO 12333, FISC-afgørelser og andet materiale, bl.a. på et særligt websted »IC on the Record«, der forvaltes af ODNI ⁽³⁴¹⁾.
- (173) Endelig er indsamlingen af personoplysninger i henhold til Section 702 i FISA ud over tilsynsorganernes tilsyn, som omhandlet i betragtning 162-168, underlagt FISC's tilsyn ⁽³⁴²⁾. I henhold til regel 13 i FISC's procedureregler skal kontrolansvarlige i de amerikanske efterretnings tjenester indberette enhver overtrædelse af målretnings-, minimerings- og søgningsprocedurer i henhold til Section 702 i FISA til justitsministeriet og ODNI, som så indberetter dem til FISC. Derudover indsender justitsministeriet og ODNI fælles halvårslige tilsynsvurderings-rapporter til FISC, i hvilke der identificeres tendenser med hensyn til overholdelsen af målretningsprocedurerne, afgives statistiske oplysninger, beskrives kategorier af tilfælde af manglende overholdelse, gives en detaljeret beskrivelse af årsagerne til, at visse tilfælde af manglende overholdelse af målretningsprocedurerne er opstået, og i hvilke de foranstaltninger, som efterretningstjenesterne har truffet for at undgå gentagelse, skitseres ⁽³⁴³⁾.
- (174) Domstolen kan om nødvendigt (f.eks. hvis der konstateres overtrædelser af målretningsprocedurerne) pålægge den relevante efterretningstjeneste at træffe afhjælpende foranstaltninger ⁽³⁴⁴⁾. De pågældende afhjælpende foranstaltninger kan spænde fra individuelle til strukturelle foranstaltninger, f.eks. fra ophør med indsamlingen af oplysninger og sletning af ulovligt indhentede oplysninger til en ændring i indsamlingspraksis, herunder med hensyn til vejledning og uddannelse af personale ⁽³⁴⁵⁾. Desuden tager FISC i forbindelse med sin årlige evaluering af

⁽³³⁸⁾ 50 U.S.C. § 1873(b). I henhold til Section 402 skal »direktøren for den nationale efterretningstjeneste i samråd med den amerikanske justitsminister foretage en afklassificeringsgennemgang af enhver afgørelse, kendelse eller udtalelse udstedt af Foreign Intelligence Surveillance Court eller Foreign Intelligence Surveillance Court of Review (som defineret i Section 601(e)), som indeholder en væsentlig forståelse eller fortolkning af lovbestemmelser, herunder en ny eller væsentlig forståelse eller fortolkning af den specifikke selektor (»specific selection term«), og i overensstemmelse med denne gennemgang i videst muligt omfang offentliggøre sådanne afgørelser, kendelser eller udtalelser«.

⁽³³⁹⁾ 50 U.S.C. § 1873(b)(7) og 1874.

⁽³⁴⁰⁾ <https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic>.

⁽³⁴¹⁾ Jf. »IC on the Record«, som findes på <https://icontherecord.tumblr.com/>.

⁽³⁴²⁾ FISC har tidligere konkluderet, at »det er klart for domstolen, at gennemførelsesorganerne samt ODNI og justitsministeriets afdeling for national sikkerhed afsætter betydelige ressourcer til deres kontrol- og tilsynsopgaver i henhold til Section 702. Generelt identificeres tilfælde af manglende overholdelse omgående, og der træffes passende afhjælpende foranstaltninger, herunder sletning af oplysninger, der er indhentet uretmæssigt eller på anden måde er omfattet af destruktionskrav i henhold til gældende procedurer«. FISA-domstolen, Memorandum Opinion and Order [overskrift redigeret] (2014), findes på <https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

⁽³⁴³⁾ Jf. f.eks. DoJ/ODNI FISA 702 Compliance Report to FISC for June 2018 – Nov. 2018, s. 21-65.

⁽³⁴⁴⁾ 50 U.S.C. § 1803(h). Jf. ligeledes PCLOB, Section 702 Report, s. 76. Jf. desuden FISC Memorandum Opinion and Order af 3.10.2011 som et eksempel på en utilstrækkelighedskendelse, hvori regeringen blev pålagt at afhjælpe de konstaterede mangler inden for 30 dage. Findes på <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>. Jf. Walton-brevet, afsnit 4, s. 10-11. Jf. ligeledes FISC's udtalelse af 18.10.2018, som findes på https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, som bekræftet af FISC i dens udtalelse af 12.7.2019, som findes på https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_12Jul19.pdf, hvori FISC bl.a. pålagde regeringen at overholde visse underretnings-, dokumentations- og rapporteringskrav over for FISC.

⁽³⁴⁵⁾ Jf. f.eks. FISC, Memorandum Opinion and Order, s. 76 (6.12.2019) (offentlig frigivelse tilladt den 4.9.2020), hvori FISC pålagde regeringen at forelægge en skriftlig rapport senest den 28.2.2020 om de skridt, som regeringen tog for at forbedre procedurerne for identifikation og fjernelse af rapporter udledt af FISA 702-oplysninger, der blev tilbagekaldt af overholdelseshensyn, samt om andre emner. Jf. også bilag VII.

Section 702-certificeringerne hensyn til tilfældene af manglende overholdelse for at afgøre, om de indsendte certificeringer opfylder FISA's krav. Tilsvarende kan FISC, hvis den finder, at regeringens certificeringer ikke var tilstrækkelige, bl.a. på grund af særlige tilfælde af manglende overholdelse, udstede en såkaldt »utilstrækkelighedskendelse«, der pålægger regeringen at afhjælpe overtrædelsen inden for 30 dage eller kræver, at regeringen indstiller eller undlader at påbegynde gennemførelsen af Section 702-certificeringen. Endelig vurderer FISC tendenser, som den observerer med hensyn til overholdelsesproblemer, og kan kræve ændringer af procedurer eller yderligere tilsyn og rapportering for at tage højde for overholdelsestendenser ⁽³⁴⁶⁾.

3.2.3 Klageadgang

- (175) Som forklaret nærmere i dette afsnit giver amerikansk ret de registrerede i EU en række muligheder for at anlægge sag ved en uafhængig og upartisk domstol med bindende beføjelser. Tilsammen giver de registrerede mulighed for at få indsigt i deres personoplysninger, få kontrolleret lovligheden af statslige organers adgang til deres oplysninger og, hvis det konstateres, at der er sket en overtrædelse, få en sådan overtrædelse afhjulpet, herunder ved at få berigtiget eller slettet deres personoplysninger.
- (176) For det første oprettes der i henhold til EO 14086 en særlig klagemekanisme, som suppleres af justitsministerens forordning om oprettelse af Data Protection Review Court (DPRC), der skal sikre, at klager fra fysiske personer vedrørende amerikanske signalefterretningsaktiviteter behandles og løses. Enhver person i EU har ret til at indgive en klage til klagemekanismen vedrørende en påstået overtrædelse af amerikansk ret om signalefterretningsaktiviteter (f.eks. EO 14086, Section 702 i FISA, EO 12333), der er til skade for den pågældendes interesser med hensyn til privatlivets fred og borgerlige frihedsrettigheder ⁽³⁴⁷⁾. Denne klagemekanisme er tilgængelig for fysiske personer i lande eller regionale organisationer for økonomisk integration, der af den amerikanske justitsminister er udpeget som »kvalificerede stater« ⁽³⁴⁸⁾. Den 30. juni 2023 blev Den Europæiske Union og de tre lande i Den Europæiske Frihandelskommunitet, der tilsammen udgør Det Europæiske Økonomiske Samarbejdsområde, udpeget af Attorney General i henhold til section 3 (f) EO 14086 som en »kvalificeret stat« ⁽³⁴⁹⁾. Denne udpegelse berører ikke artikel 4, stk. 2, i traktaten om Den Europæiske Union.
- (177) En registreret i Unionen, der ønsker at indgive en sådan klage, skal indgive den til en tilsynsmyndighed i en EU-medlemsstat, der har kompetence til at føre tilsyn med offentlige myndigheders behandling af personoplysninger (en databeskyttelsesmyndighed) ⁽³⁵⁰⁾. Dette sikrer let adgang til klagemekanismen, idet personer kan henvende sig til en »lokal« myndighed, som de kan kommunikere med på deres eget sprog. Når kravene til indgivelse af en klage, jf. betragtning 178, er blevet kontrolleret, vil den kompetente databeskyttelsesmyndighed via Det Europæiske Databeskyttelsesråds sekretariat kanalisere klagen videre til klagemekanismen.
- (178) Fysiske personer skal kun opfylde få krav for at kunne indgive en klage til klagemekanismen, og de behøver f.eks. ikke at påvise, at deres oplysninger faktisk har været genstand for amerikanske signalefterretningsaktiviteter ⁽³⁵¹⁾. Samtidig skal der som et udgangspunkt for klagemekanismens behandling af klagen afgives visse grundlæggende oplysninger, f.eks. vedrørende de personoplysninger, der med rimelighed kan antages at være blevet overført til USA, og de midler, hvormed de menes at være blevet overført, identiteten af de statslige enheder i USA, der menes at være involveret i den påståede overtrædelse (hvis de er kendt), grundlaget for påstanden om, at der er sket en overtrædelse af amerikansk ret (selv om dette igen ikke kræver, at det påvises, at personoplysninger rent faktisk er blevet indsamlet af amerikanske efterretnings tjenester), og arten af den ønskede afhjælpning.

⁽³⁴⁶⁾ Jf. bilag VII.

⁽³⁴⁷⁾ Jf. Section 4(k)(iv) i EO 14086, hvori det fastsættes, at klager til klagemekanismen skal indgives af en klager, der handler på egne vegne (dvs. ikke som repræsentant for en regering eller en ikkestatslig eller mellemstatslig organisation). Begrebet »påvirkes negativt« kræver ikke, at klageren opfylder en vis tærskel for at få adgang til klagemekanismen (se betragtning 178 i denne henseende). Den præciserer snarere, at ODNI CLPO og DPRC har beføjelse til at afhjælpe overtrædelser af amerikansk lovgivning om signalefterretningsaktiviteter, der har en negativ indvirkning på en klagers individuelle interesser vedrørende privatlivets fred og borgerlige frihedsrettigheder. Omvendt ville overtrædelser af krav i henhold til gældende amerikansk lovgivning, der ikke har til formål at beskytte enkeltpersoner (f.eks. budgetkrav), falde uden for ODNI CLPO's og DPRC's jurisdiktion.

⁽³⁴⁸⁾ Section 3(f) i EO 14086.

⁽³⁴⁹⁾ <https://www.justice.gov/opcl/executive-order-14086>.

⁽³⁵⁰⁾ Section 4(d)(v) i EO 14086.

⁽³⁵¹⁾ Jf. Section 4(k)(i)-(iv) i EO 14086.

- (179) Den indledende undersøgelse af klager, der er indgivet til denne klagemekanisme, foretages af ODNI CLPO, hvis eksisterende lovbestemte rolle og beføjelser er blevet udvidet til også at omfatte de specifikke foranstaltninger, der skal træffes i henhold til EO 14086 ⁽³⁵²⁾. Inden for efterretningssamfundet er CLPO bl.a. ansvarlig for at sikre, at beskyttelsen af borgerlige frihedsrettigheder og privatlivets fred på passende vis indarbejdes i ODNI's og efterretningstjenesternes politikker og procedurer, for at føre tilsyn med, at ODNI overholder de gældende krav vedrørende borgerlige frihedsrettigheder og privatlivets fred, og for at foretage analyser af konsekvenserne for privatlivets fred ⁽³⁵³⁾. ODNI CLPO kan kun afsættes af direktøren for den nationale efterretningstjeneste i tilfælde af tjenesteforseelse, embedsmisbrug, brud på sikkerheden, tjenesteforsømmelse eller uarbejdsdygtighed ⁽³⁵⁴⁾.
- (180) ODNI CLPO har i forbindelse med sin behandling adgang til oplysningerne for at kunne foretage sin vurdering og kan regne med påbudt bistand fra de databeskyttelsesansvarlige i de forskellige efterretningstjenester ⁽³⁵⁵⁾. Efterretningstjenesterne må ikke hindre eller uretmæssigt påvirke ODNI CLPO's behandling. Dette omfatter direktøren for den nationale efterretningstjeneste, som ikke må blande sig i behandlingen ⁽³⁵⁶⁾. Ved behandlingen af en klage skal ODNI CLPO »anvende loven upartisk« under hensyntagen til både de nationale sikkerhedsinteresser inden for signalefterretningsaktiviteterne og beskyttelsen af privatlivets fred ⁽³⁵⁷⁾.
- (181) Som led i behandlingen afgør ODNI CLPO, om der er sket en overtrædelse af gældende amerikansk ret, og træffer i givet fald afgørelse om en passende afhjælpning ⁽³⁵⁸⁾. Sidstnævnte henviser til foranstaltninger, der fuldt ud afhjælper en konstateret overtrædelse, såsom ophør med ulovlig indsamling af oplysninger, sletning af ulovligt indsamlede oplysninger, sletning af resultaterne af ubehørigt foretagne søgninger i ellers lovligt indsamlede oplysninger, begrænsning af adgangen til lovligt indsamlede oplysninger til behørigt uddannet personale eller tilbagekaldelse af efterretningsrapporter, som indeholder oplysninger, der er indhentet uden lovlig tilladelse, eller som er blevet ulovligt videregivet ⁽³⁵⁹⁾. ODNI CLPO's afgørelser om individuelle klager (herunder om afhjælpning) er bindende for de berørte efterretningstjenester ⁽³⁶⁰⁾.
- (182) ODNI CLPO skal kunne dokumentere sin vurdering og fremlægge en klassificeret afgørelse, der forklarer grundlaget for dens faktuelle konklusioner, beslutningen om, hvorvidt der har fundet en overtrædelse sted, og beslutningen om passende afhjælpning ⁽³⁶¹⁾. Såfremt ODNI CLPO's behandling afslører en overtrædelse begået af en myndighed, der er underlagt FISC's tilsyn, skal CLPO desuden forelægge en klassificeret rapport for den assisterende justitsminister for national sikkerhed (Assistant Attorney General for National Security), som igen er forpligtet til at indberette den manglende overholdelse til FISC, som kan træffe yderligere håndhævelsesforanstaltninger (i overensstemmelse med den procedure, der er beskrevet i betragtning 173-174) ⁽³⁶²⁾.
- (183) Når behandlingen er afsluttet, underretter ODNI CLPO via den nationale myndighed klageren om, at »behandlingen enten ikke identificerede nogen overtrædelse, eller at ODNI CLPO udstedte en beslutning om passende afhjælpning« ⁽³⁶³⁾. Dermed beskyttes fortroligheden af aktiviteter, der gennemføres for at beskytte den nationale sikkerhed, samtidig med at de omhandlede personer får en afgørelse, der bekræfter, at deres klage er blevet behørigt behandlet og afgjort. Denne afgørelse kan i øvrigt anfægtes af den omhandlede person. Med henblik herpå vil han eller hun blive underrettet om muligheden for at få CLPO's beslutninger prøvet ved DPRC (jf. betragtning 184 ff.), og at der, hvis sagen indbringes for domstolen, vil blive udpeget en særlig advokat til at forsvare klagerens interesser ⁽³⁶⁴⁾.

⁽³⁵²⁾ Section 3(c)(iv) i EO 14086. Jf. endvidere National Security Act 1947, 50 U.S.C. § 403-3d, Section 103D, vedrørende CLPO's rolle i ODNI.

⁽³⁵³⁾ 50 U.S.C § 3029 (b).

⁽³⁵⁴⁾ Section 3(c)(iv) i EO 14086.

⁽³⁵⁵⁾ Section 3(c)(iii) i EO 14086.

⁽³⁵⁶⁾ Section 3(c)(iv) i EO 14086.

⁽³⁵⁷⁾ Section 3(c)(i)(B)(i) og (iii) i EO 14086.

⁽³⁵⁸⁾ Section 3(c)(i) i EO 14086.

⁽³⁵⁹⁾ Section 4(a) i EO 14086.

⁽³⁶⁰⁾ Section 3(c)(d) i EO 14086.

⁽³⁶¹⁾ Section 3(c)(i)(F)-(G) i EO 14086.

⁽³⁶²⁾ Jf. endvidere Section 3(c)(i)(D) i EO 14086.

⁽³⁶³⁾ Section 3(c)(i)(E)(1) i EO 14086.

⁽³⁶⁴⁾ Section 3(c)(i)(E)(2)-(3) i EO 14086.

- (184) Enhver klager og enhver enhed i efterretningstjenesten kan anmode om at få ODNI CLPO's afgørelse prøvet ved Data Protection Review Court. Sådanne anmodninger om prøvelse skal indgives senest 60 dage efter modtagelsen af meddelelsen fra ODNI CLPO om, at dens behandling er afsluttet, og indeholde alle de oplysninger, som den pågældende ønsker at forelægge DPRC (f.eks. argumenter om retlige spørgsmål eller lovens anvendelse på sagens faktiske omstændigheder) ⁽³⁶⁵⁾. Registrerede i Unionen kan igen indgive deres ansøgning til den kompetente databeskyttelsesmyndighed (se betragtning 177).
- (185) DPRC er en uafhængig domstol, der er oprettet af justitsministeren på grundlag af EO 14086 ⁽³⁶⁶⁾. Den består af mindst seks dommere, der udnævnes af justitsministeren i samråd med PCLOB, handelsministeren og direktøren for den nationale efterretningstjeneste for en periode på fire år, der kan forlænges ⁽³⁶⁷⁾. Justitsministerens udnævnelse af dommere sker på grundlag af de kriterier, som den udøvende magt anvender ved vurderingen af kandidater til den føderale dommerstand, idet der lægges vægt på tidligere erfaring fra retsvæsenet ⁽³⁶⁸⁾. Desuden skal dommerne være aktører inden for retsvæsenet (dvs. være aktive medlemmer, der har et godt omdømme og har behørig tilladelse til at arbejde som advokat) og have relevant erfaring med lovgivningen om privatlivets fred og national sikkerhed. Justitsministeren skal bestræbe sig på at sikre, at mindst halvdelen af dommerne til enhver tid har tidligere erfaring fra retsvæsenet, og alle dommere skal være i besiddelse af sikkerhedsgodkendelser, så de kan få adgang til klassificerede nationale sikkerhedsoplysninger ⁽³⁶⁹⁾.
- (186) Kun personer, der har de kvalifikationer, der er nævnt i betragtning 185, og som ikke er eller har været ansat under den udøvende magt på tidspunktet for deres udnævnelse eller i de foregående to år, kan udnævnes til DPRC. Tilsvarende må dommerne under deres embedsperiode i DPRC ikke have andre officielle pligter eller være ansat i andre statslige organer end DPRC ⁽³⁷⁰⁾.
- (187) Beslutningsprocessens uafhængighed sikres gennem en række garantier. Navnlig er den udøvende magt (justitsministeren og efterretningstjenesterne) afskåret fra at blande sig i eller på utilbørlig vis påvirke DPRC's arbejde ⁽³⁷¹⁾. DPRC er selv forpligtet til at træffe upartiske afgørelser i sager ⁽³⁷²⁾ og fungerer i henhold til sine egne procedureregler (vedtaget med flertal). Desuden kan DPRC's dommere kun afsættes af justitsministeren og kun i tilfælde af tjenesteforseelse (dvs. embedsmisbrug, brud på sikkerheden, tjenesteforsømmelse eller uarbejdsdygtighed), efter at der er taget behørigt hensyn til de standarder, der gælder for forbundsdommere, og som er fastsat i reglerne for sager om retsvæsenets aktørers adfærd og handicap (Rules for Judicial-Conduct and Judicial-Disability Proceedings) ⁽³⁷³⁾.
-
- ⁽³⁶⁵⁾ Section 201.6(a)-(b) i justitsministerens forordning.
- ⁽³⁶⁶⁾ Section 3(d)(i) og justitsministerens forordning. USA's højesteret har anerkendt muligheden for, at justitsministeren kan oprette uafhængige organer med beslutningskompetence, herunder til at træffe afgørelse i individuelle sager, jf. navnlig *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954) og *United States v. Nixon*, 418 U.S. 683, 695 (1974). Overholdelsen af de forskellige krav i EO 14086, f.eks. kriterierne og proceduren for udnævnelse og afskedigelse af DPRC-dommere, er navnlig underlagt tilsyn af justitsministeriets generalinspektør (se også betragtning 109 om generalinspektørernes lovbestemte myndighed).
- ⁽³⁶⁷⁾ Section 3(d)(i)(A) i EO 14086 og Section 201.3(a) i justitsministerens forordning.
- ⁽³⁶⁸⁾ Section 201.3(b) i justitsministerens forordning.
- ⁽³⁶⁹⁾ Section 3(d)(i)(B) i EO 14086.
- ⁽³⁷⁰⁾ Section 3(d)(i)(A) i EO 14086 og Section 201.3(a) og (c) i justitsministerens forordning. Personer, der udnævnes til DPRC, kan deltage i udenretslige aktiviteter, herunder forretningsaktiviteter, finansielle aktiviteter, nonprofit fundraising- og formueforvaltningsaktiviteter samt udøvelse af advokatvirksomhed, så længe sådanne aktiviteter ikke griber ind i den upartiske udførelse af deres opgaver eller DPRC's effektivitet eller uafhængighed (Section 201.7(c) i justitsministerens forordning).
- ⁽³⁷¹⁾ Section 3(d)(iii)-(iv) i EO 14086 og Section 201.7(d) i justitsministerens forordning.
- ⁽³⁷²⁾ Section 3(d)(i)(D) i EO 14086 og Section 201.9 i justitsministerens forordning.
- ⁽³⁷³⁾ Section 3(d)(iv) i EO 14086 og Section 201.7(d) i justitsministerens forordning. Jf. også *Bumap v. USA*, 252 U.S. 512, 515 (1920), som bekræftede det mangeårige princip i amerikansk ret om, at afsættelsesbeføjelsen hænger sammen med beføjelsen til at udpege (som også påpeget af justitsministeriets kontor for juridisk rådgivning i *The Constitutional Separation of Powers Between the President and Congress*, 20, Op. O.L.C. 124, 166 (1996)).

- (188) Anmodninger indgivet til DPRC behandles af paneler bestående af tre dommere, herunder en retsformand, som skal handle i overensstemmelse med adfærdskodeksen for amerikanske dommere (Code of Conduct for United States Judges) ⁽³⁷⁴⁾. Hvert panel består af en særlig advokat ⁽³⁷⁵⁾, der har adgang til alle oplysninger vedrørende sagen, herunder klassificerede oplysninger ⁽³⁷⁶⁾. Den særlige advokats rolle er at sikre, at klagerens interesser er repræsenteret, og at DPRC-panelet er velinformeret om alle relevante retlige og faktiske spørgsmål ⁽³⁷⁷⁾. For yderligere at underbygge sin holdning til en anmodning om prøvelse, som en person indgiver til DPRC, kan den særlige advokat indhente oplysninger fra klageren gennem skriftlige forespørgsler ⁽³⁷⁸⁾.
- (189) DPRC gennemgår ODNI CLPO's beslutninger (både om der er sket en overtrædelse af gældende amerikansk ret og med hensyn til passende afhjælpning), hvilket som minimum sker på baggrund af optegnelserne over ODNI CLPO's undersøgelse samt alle oplysninger og indlæg fra klageren, den særlige advokat eller en efterretningstjeneste ⁽³⁷⁹⁾. Et DPRC-panel har adgang til alle de oplysninger, der er nødvendige for at foretage denne behandling, og det kan indhente disse oplysninger gennem ODNI CLPO (panelet kan f.eks. anmode CLPO om at supplere sine optegnelser med yderligere oplysninger eller faktuelle konklusioner, hvis det er nødvendigt for behandlingen) ⁽³⁸⁰⁾.
- (190) Ved behandlingens afslutning kan DPRC 1) beslutte, at der ikke er noget bevis for, at der er udført signalefterretningsaktiviteter, som involverer klagerens personoplysninger, 2) beslutte, at ODNI CLPO's beslutninger var juridisk korrekte og underbygget af væsentlige beviser, eller 3) hvis DPRC er uenig i ODNI CLPO's beslutninger (med hensyn til om der er sket en overtrædelse af gældende amerikansk ret eller med hensyn til passende afhjælpning), udstede sine egne beslutninger ⁽³⁸¹⁾.

⁽³⁷⁴⁾ Section 3(d)(i)(B) i EO 14086 og Section 201.7(a)-(c) i justitsministerens forordning. Justitsministeriets kontor for privatlivets fred og borgerlige frihedsrettigheder (Office of Privacy and Civil Liberties, OPCL), som har ansvaret for at yde administrativ støtte til DPRC og de særlige advokater (jf. Section 201.5 i justitsministerens forordning), udvælger et panel med tre personer, som udskiftes efter tur, idet det sikres, at der i hvert panel sidder mindst én dommer med tidligere erfaring fra retsvæsenet (hvis ingen af dommerne i panelet har en sådan erfaring, er retsformanden den første dommer, der udvælges af OPCL).

⁽³⁷⁵⁾ Section 201.4 i justitsministerens forordning. Der udpeges mindst to særlige advokater af justitsministeren i samråd med handelsministeren, direktøren for den nationale efterretningstjeneste og PCLOB for to perioder, der kan forlænges. De særlige advokater skal have relevant erfaring inden for lovgivningen om privatlivets fred og national sikkerhed, være erfarne advokater, være aktive medlemmer af advokatstanden, have et godt omdømme og have behørig tilladelse til at arbejde som advokat. Desuden må de på tidspunktet for deres første udnævnelse ikke have været ansat under den udøvende magt i de foregående to år. I forbindelse med hver behandling af en anmodning vælger retsformanden en særlig advokat, der skal bistå panelet, jf. Section 201.8(a) i justitsministerens forordning.

⁽³⁷⁶⁾ Section 201.8(c) og 201.11 i justitsministerens forordning.

⁽³⁷⁷⁾ Section 3(d)(i)(C) i EO 14086 og Section 201.8(e) i justitsministerens forordning. Den særlige advokat handler ikke som repræsentant for og har ikke et advokat-klient-forhold til klageren.

⁽³⁷⁸⁾ Jf. Section 201.8(d)(e) i justitsministerens forordning. Sådanne forespørgsler gennemgås først af OPCL i samråd med den relevante enhed i efterretningstjenesten med henblik på at identificere og udelukke klassificerede eller privilegerede eller beskyttede oplysninger, inden de videregives til klageren. Yderligere oplysninger, som den særlige advokat modtager som svar på sådanne forespørgsler, indføres i den særlige advokats indlæg for DPRC.

⁽³⁷⁹⁾ Section 3(d)(i)(D) i EO 14086.

⁽³⁸⁰⁾ Section 3(d)(iii) i EO 14086 og Section 201.9(b) i justitsministerens forordning.

⁽³⁸¹⁾ Section 3(d)(i)(E) i EO 14086 og Section 201.9(c)-(e) i justitsministerens forordning. I henhold til definitionen af »passende afhjælpning« i Section 4(a) EO 14086 skal DPRC tage hensyn til »de måder, hvorpå en overtrædelse af den art, der er konstateret, sædvanligvis er blevet håndteret«, når den træffer afgørelse om en afhjælpende foranstaltning for fuldt ud at afhjælpe en overtrædelse, dvs. DPRC vil bl.a. overveje, hvordan lignende overholdelsesproblemer tidligere er blevet afhjulpet for at sikre, at retsmidlet er effektivt og hensigtsmæssigt.

- (191) DPRC vedtager i alle sager en skriftlig afgørelse ved flertalsafstemning. Hvis behandlingen påviser en overtrædelse af de gældende regler, vil afgørelsen præcisere en passende afhjælpning, herunder sletning af ulovligt indsamlede oplysninger, sletning af resultaterne af ubehørigt foretagne søgninger, begrænsning af adgangen til lovligt indsamlede oplysninger til behørigt uddannet personale eller tilbagekaldelse af efterretningsrapporter, som indeholder oplysninger, der er indhentet uden lovlig tilladelse, eller som er blevet ulovligt videregivet ⁽³⁸²⁾. DPRC's afgørelse er bindende for så vidt angår den klage, der er indbragt for den ⁽³⁸³⁾. Såfremt behandlingen afslører en overtrædelse begået af en myndighed, der er underlagt FISC's tilsyn, skal DPRC desuden forelægge en klassificeret rapport for den assisterende justitsminister for national sikkerhed, som igen er forpligtet til at indberette den manglende overholdelse til FISC, som kan træffe yderligere håndhævelsesforanstaltninger (i overensstemmelse med den procedure, der er beskrevet i betragtning 173-174) ⁽³⁸⁴⁾.
- (192) Alle DPRC-panelernes afgørelser fremsendes til ODNI CLPO ⁽³⁸⁵⁾. I sager, hvor DPRC's undersøgelse kan henføres til en anmodning fra klageren, underrettes klageren via den nationale myndighed om, at DPRC har afsluttet behandlingen, og at »behandlingen enten ikke identificerede nogen overtrædelse, eller at DPRC udstedte en beslutning om passende afhjælpning« ⁽³⁸⁶⁾. Justitsministeriets kontor for privatlivets fred og borgerlige frihedsrettigheder fører optegnelser over alle de oplysninger, som DPRC har gennemgået, og alle de trufne afgørelser, som stilles til rådighed som ikkebindende præcedens for fremtidig DPRC-paneler ⁽³⁸⁷⁾.
- (193) Handelsministeriet skal også føre optegnelser over alle de klagere, der har indgivet en klage ⁽³⁸⁸⁾. For at øge gennemsigtigheden skal handelsministeriet mindst hvert femte år kontakte de relevante efterretningstjenester for at kontrollere, om oplysninger vedrørende sager ved DPRC er blevet afklassificeret ⁽³⁸⁹⁾. Hvis det er tilfældet, vil den berørte person blive underrettet om, at disse oplysninger kan være tilgængelige i henhold til gældende ret (dvs. at vedkommende kan anmode om indsigt i oplysningerne i henhold til Freedom of Information Act, jf. betragtning 199).
- (194) Endelig vil der blive foretaget en regelmæssig og uafhængig evaluering af, om denne klagemekanisme fungerer korrekt. I henhold til EO 14086 skal PCLOB, som er et uafhængigt organ, nærmere bestemt hvert år foretage en evaluering af klagemekanismens korrekte funktion (jf. betragtning 110) ⁽³⁹⁰⁾. Som led i denne evaluering vil PCLOB bl.a. vurdere, om ODNI CLPO og DPRC har behandlet klagerne rettidigt, om de har fået fuld indsigt i de nødvendige oplysninger, om de materielle garantier i EO 14086 er blevet taget behørigt i betragtning under evalueringen, og om efterretningstjenesten fuldt ud har efterlevet ODNI CLPO's og DPRC's beslutninger. PCLOB vil forelægge en rapport om resultatet af sin evaluering for præsidenten, justitsministeren, direktøren for den nationale efterretningstjeneste, lederne af efterretningstjenesterne, ODNI CLPO og Kongressens efterretningsudvalg, som også vil blive offentliggjort i en uklassificeret udgave — og som derefter vil indgå i Kommissionens regelmæssige evaluering af, hvorvidt denne afgørelse fungerer. Justitsministeren, direktøren for den nationale efterretningstjeneste, ODNI CLPO og lederne af efterretningstjenesterne skal gennemføre eller på anden måde forholde sig til alle de anbefalinger, der fremsættes i sådanne rapporter. Desuden vil PCLOB hvert år foretage en offentlig certificering af, hvorvidt klager indgivet til klagemekanismen behandles i overensstemmelse med kravene i EO 14086.

⁽³⁸²⁾ Section 4(a) i EO 14086.

⁽³⁸³⁾ Section 3(d)(ii) i EO 14086 og Section 201.9(g) i justitsministerens forordning. Da DPRC's afgørelse er endelig og bindende, kan ingen andre udøvende eller administrative institutioner/organer (herunder USA's præsident) tilsidesætte DPRC's afgørelse. Dette blev også bekræftet i højesterets retspraksis, hvori det blev præciseret, at den amerikanske justitsminister ved at delegere sin unikke beføjelse inden for den udøvende magt til at udstede bindende afgørelser til et uafhængigt organ nægter sig selv muligheden for at diktere dette organs afgørelse på nogen måde (jf. *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954)).

⁽³⁸⁴⁾ Section 3(d)(i)(F) i EO 14086 og Section 201.9(i) i justitsministerens forordning.

⁽³⁸⁵⁾ Section 201.9(h) i justitsministerens forordning.

⁽³⁸⁶⁾ Section 3(d)(i)(H) i EO 14086 og Section 201.9(h) i justitsministerens forordning. Hvad angår arten af notifikationen, henvises til Section 201.9(h)(3) i justitsministerens forordning.

⁽³⁸⁷⁾ Section 201.9(j) i justitsministerens forordning.

⁽³⁸⁸⁾ Section 3(d)(v)(A) i EO 14086.

⁽³⁸⁹⁾ Section 3(d)(v) i EO 14086.

⁽³⁹⁰⁾ Section 3(e) i EO 14086. Jf. endvidere [https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf).

- (195) Ud over den særlige klagemekanisme, der er oprettet i henhold til EO 14086, har alle enkeltpersoner (uanset nationalitet eller opholdssted) adgang til retsmidler ved de almindelige amerikanske domstole ⁽³⁹¹⁾.
- (196) FISA og en tilknyttet lov giver navnlig personer mulighed for at anlægge et civilt erstatningssøgsmål mod USA, når oplysninger om dem er blevet ulovligt og forsætligt anvendt eller videregivet ⁽³⁹²⁾, at sagsøge amerikanske regeringsembedsmænd personligt for økonomisk erstatning ⁽³⁹³⁾ og at gøre indsigelse mod lovligheden af overvågning (og anmode om at få oplysningerne fjernet), hvis den amerikanske regering agter at bruge eller videregive oplysninger indhentet gennem eller udledt af elektronisk overvågning mod den pågældende i forbindelse med retslige eller administrative procedurer i USA ⁽³⁹⁴⁾. Mere generelt gælder det, at hvis regeringen agter at bruge oplysninger, der er indhentet i forbindelse med efterretningsoperationer, mod en mistænkt i en straffesag, pålægger forfatnings- og lovkrav ⁽³⁹⁵⁾ forpligtelser til at videregive visse oplysninger, således at den sagsøgte kan anfægte lovligheden af regeringens indsamling og anvendelse af bevismaterialet.
- (197) Derudover er der flere specifikke muligheder for at anlægge sag mod embedsmænd for ulovlig statslig adgang til eller brug af personoplysninger, herunder til påståede nationale sikkerhedsformål (Computer Fraud and Abuse Act ⁽³⁹⁶⁾, Electronic Communications Privacy Act ⁽³⁹⁷⁾ og Right to Financial Privacy Act ⁽³⁹⁸⁾). Alle disse muligheder for at anlægge sag vedrører specifikke oplysninger, mål og/eller typer af adgang (f.eks. fjernadgang fra en computer via internettet) og kan anvendes i visse tilfælde (f.eks. forsætlig adfærd, handlinger, der ligger uden for udførelsen af et hverv, lidt skade).
- (198) En mere generel klagemulighed findes i APA ⁽³⁹⁹⁾, ifølge hvilken »enhver person, mod hvem der er begået juridisk uret på grund af et agents foranstaltninger, eller som er blevet krænket eller forurettet herved« kan begære retslig prøvelse ⁽⁴⁰⁰⁾. Det omfatter muligheden for at anmode domstolen om at »erklære agents foranstaltninger, konstateringer og konklusioner for ulovlige og annullere dem, hvis de er vilkårlige, ustadige eller udtryk for magtmisbrug eller på anden vis ikke er i overensstemmelse med loven« ⁽⁴⁰¹⁾. F.eks. traf en forbundsappeldomstol i 2015 afgørelse om en APA-påstand om, at den amerikanske regerings masseindsamling af telefonmetadata ikke var tilladt i henhold til Section 501 i FISA ⁽⁴⁰²⁾.
-
- ⁽³⁹¹⁾ Adgangen til disse retsmidler kræver, at den berørte person kan dokumentere sin søgsmålskompetence. Denne standard, som gælder for enhver person uanset nationalitet, udspringer af kravet om retstvist (»case or controversy«) i artikel III i den amerikanske forfatning. Ifølge den amerikanske højesteret kræver dette, at 1) personen har lidt en »faktisk skade« (dvs. at en retligt beskyttet interesse er blevet påført konkret og specifik, aktuel eller nært forestående skade), 2) der er en årsagssammenhæng mellem skaden og den adfærd, der anfægtes ved retten, og 3) det er sandsynligt og ikke ren spekulation, at en positiv afgørelse fra domstolen vil afhjælpe skaden (jf. *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)).
- ⁽³⁹²⁾ 18 U.S.C. § 2712.
- ⁽³⁹³⁾ 50 U.S.C. § 1810.
- ⁽³⁹⁴⁾ 50 U.S.C. § 1806.
- ⁽³⁹⁵⁾ Jf. henholdsvis *Brady v. Maryland*, 373 U.S. 83 (1963) og *Jencks Act*, 18 U.S.C. § 3500.
- ⁽³⁹⁶⁾ 18 U.S.C. § 1030.
- ⁽³⁹⁷⁾ 18 U.S.C. § 2701-2712.
- ⁽³⁹⁸⁾ 12 U.S.C. § 3417.
- ⁽³⁹⁹⁾ 5 U.S.C. § 702.
- ⁽⁴⁰⁰⁾ Generelt er det kun agents »endelige« — og ikke »foreløbige, proceduremæssige eller mellemliggende« — foranstaltninger, der er genstand for retslig prøvelse. Jf. 5 U.S.C. § 704.
- ⁽⁴⁰¹⁾ 5 U.S.C. § 706(2)(A).
- ⁽⁴⁰²⁾ *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015). Det i disse sager anfægtede program for masseindsamling af telefondata blev indstillet ved USA FREEDOM Act i 2015.

- (199) Endelig har enhver person ud over de klagemuligheder, der er nævnt i betragtning 176-198, ifølge FOIA ret til at søge indsigt i de amerikanske forbundsorganers eksisterende optegnelser, herunder når disse indeholder personens personoplysninger ⁽⁴⁰³⁾. En sådan indsigt kan også gøre det lettere at anlægge sag ved de almindelige domstole, herunder til støtte for ens søgsmålskompetence. Agenturerne kan tilbageholde oplysninger, der er omfattet af visse anførte undtagelser, herunder adgang til klassificerede informationer om den nationale sikkerhed og informationer om retshåndhævende efterforskning ⁽⁴⁰⁴⁾, men klager, som er utilfredse med svaret, kan anfægte tilbageholdelsen ved at anmode om administrativ og efterfølgende retlig prøvelse (ved forbundsdomstolene) ⁽⁴⁰⁵⁾.
- (200) Det følger af det ovenstående, at når amerikanske retshåndhævende myndigheder og nationale sikkerhedsmyndigheder får adgang til personoplysninger, der er omfattet af denne afgørelse, er en sådan adgang underlagt retlige rammer, der fastsætter betingelserne for adgang og sikrer, at adgangen til og den videre anvendelse af oplysningerne begrænses til det, der er nødvendigt og står i rimeligt forhold til det mål af almen interesse, der forfølges. Disse garantier kan påberåbes af personer, der har ret til effektiv klageadgang.

4. KONKLUSION

- (201) Kommissionen finder, at USA — gennem de principper, som det amerikanske handelsministerium har opstillet — sikrer et niveau af beskyttelse af personoplysninger, der overføres fra Unionen til certificerede organisationer i USA under EU-USA-databeskyttelsesrammen, der i det væsentlige svarer til det niveau, der er garanteret ved forordning (EU) 2016/679.
- (202) Kommissionen mener desuden, at den effektive anvendelse af principperne er garanteret ved gennemsigtighedskrav og handelsministeriets forvaltning af databeskyttelsesrammen. Derudover gør mekanismerne for tilsyn og klageadgang i amerikansk ret det muligt at identificere overtrædelser af databeskyttelsesreglerne og straffe disse i praksis, og de sikrer registrerede retsmidler med henblik på at få adgang til personoplysninger, som vedrører de pågældende, eller til at få sådanne oplysninger berigtiget eller slettet.
- (203) På baggrund af de tilgængelige oplysninger om den amerikanske retsorden, herunder oplysningerne i bilag VI og VII, mener Kommissionen endelig, at eventuelle indgreb af hensyn til offentlige interesser fra de amerikanske offentlige myndigheders side i de grundlæggende rettigheder for de personer, hvis personoplysninger overføres fra EU til USA under EU-USA-databeskyttelsesrammen, navnlig med henblik på strafferetlig håndhævelse og nationale sikkerhedsformål, vil blive begrænset til det, der er strengt nødvendigt for at nå det tilsigtede legitime mål, og at der er en effektiv retsbeskyttelse mod sådanne indgreb. I lyset af ovenstående konklusioner bør det derfor fastslås, at USA sikrer et tilstrækkeligt beskyttelsesniveau i henhold til artikel 45 i forordning (EU) 2016/679, fortolket i lyset af Den Europæiske Unions charter om grundlæggende rettigheder, for personoplysninger, der overføres fra EU til organisationer, der er certificeret i henhold til EU-USA-databeskyttelsesrammen.
- (204) Eftersom de begrænsninger, garantier og klagemekanismer, der er indført ved EO 14086, er væsentlige elementer i det amerikanske retsgrundlag, som Kommissionens vurdering er baseret på, er denne afgørelses vedtagelse navnlig baseret på, at alle amerikanske efterretningstjenester vedtager ajourførte politikker og procedurer til gennemførelse af EO 14086, og at Unionen udpeges som en kvalificeret organisation med henblik på den klagemekanisme, som har fundet sted henholdsvis den 3. juli 2023 (jf. betragtning 126) og den 30. juni 2023 (jf. betragtning 176).

⁽⁴⁰³⁾ 5 U.S.C. § 552. Der findes tilsvarende love på delstatsniveau.

⁽⁴⁰⁴⁾ I dette tilfælde vil den pågældende normalt kun modtage et standardsvar, hvor agenturet afslår at bekræfte eller benægte, at der foreligger optegnelser. Jf. *ACLU v CIA*, 710 F.3d 422 (D.C. Cir. 2014). Kriterierne for og varigheden af klassificeringen er fastsat i EO 13526, som generelt fastsætter, at der skal fastsættes en bestemt dato eller begivenhed for afklassificering på grundlag af varigheden af oplysningernes følsomhed over for den nationale sikkerhed, på hvilket tidspunkt oplysningerne automatisk skal afklassificeres (se Section 1.5 i EO 13526).

⁽⁴⁰⁵⁾ Domstolen træffer en de novo-afgørelse om, hvorvidt optegnelserne tilbageholdes lovligt, og kan tvinge de statslige myndigheder til at give adgang til optegnelser (5 U.S.C. § 552(a)(4)(B)).

5. VIRKNINGERNE AF DENNE AFGØRELSE OG DATABESKYTTELSESMYNDIGHEDERNES HANDLINGER

- (205) Medlemsstaterne og deres organer er forpligtet til at træffe de nødvendige foranstaltninger for at efterkomme EU-institutionernes retsakter, idet sidstnævnte formodes at være lovlige og derfor afføder retsvirkninger, indtil de trækkes tilbage, annulleres under et annulations søgsmål eller erklæres ugyldige som følge af en præjudiciel forelæggelse eller en ulovlighedsindsigelse.
- (206) En afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 er således bindende for alle de organer i medlemsstaterne, som den er rettet til, herunder deres uafhængige tilsynsmyndigheder. Overførsler fra en dataansvarlig eller databehandler i Unionen til certificerede organisationer i USA kan navnlig finde sted uden yderligere godkendelse.
- (207) Det bør bemærkes, at i henhold til artikel 58, stk. 5, i forordning (EU) 2016/679, og som Domstolen forklarede i *Schrems*-dommen ⁽⁴⁰⁶⁾, skal den nationale lovgivning, når en national databeskyttelsesmyndighed, herunder efter en klage, sætter spørgsmålstegn ved, om en afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet er forenelig med den enkeltes grundlæggende ret til privatlivets fred og databeskyttelse, give den mulighed for at gøre disse klagepunkter gældende for en national domstol, som eventuelt kan forelægge Domstolen et præjudicielt spørgsmål ⁽⁴⁰⁷⁾.

6. OVERVÅGNING OG REVISION AF DENNE AFGØRELSE

- (208) Ifølge Domstolens praksis ⁽⁴⁰⁸⁾ og som anerkendt i artikel 45, stk. 4, i forordning (EU) 2016/679 bør Kommissionen løbende overvåge den relevante udvikling i tredjelandet efter vedtagelsen af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet for at vurdere, hvorvidt tredjelandet stadig sikrer et i det væsentlige tilsvarende beskyttelsesniveau. En sådan undersøgelse skal under alle omstændigheder foretages, når Kommissionen modtager oplysninger, der rejser begrundet tvivl i denne henseende.
- (209) Kommissionen bør derfor løbende overvåge situationen i USA med hensyn til de retlige rammer og den faktiske praksis for behandling af personoplysninger som vurderet i denne afgørelse. For at fremme denne proces bør de amerikanske myndigheder straks underrette Kommissionen om væsentlige ændringer i den amerikanske retsorden, der har betydning for de retlige rammer, der er genstand for denne afgørelse, samt enhver udvikling i den praksis for behandling af personoplysninger, der vurderes i denne afgørelse, både hvad angår certificerede organisationers behandling af personoplysninger i USA og de begrænsninger og garantier, der gælder for offentlige myndigheders adgang til personoplysninger.
- (210) For at gøre det muligt for Kommissionen effektivt at udøve sin overvågningsfunktion bør medlemsstaterne desuden underrette Kommissionen om alle relevante foranstaltninger, der træffes af de nationale databeskyttelsesmyndigheder, navnlig vedrørende forespørgsler eller klager fra registrerede i Unionen vedrørende overførsel af personoplysninger fra Unionen til certificerede organisationer i USA. Kommissionen bør også underrettes om eventuelle tegn på, at de foranstaltninger, der træffes af de amerikanske offentlige myndigheder med ansvar for forebyggelse, efterforskning, afsløring og retsforfølgelse af lovovertrædelser eller for den nationale sikkerhed, herunder tilsynsorganer, ikke sikrer det nødvendige beskyttelsesniveau.

⁽⁴⁰⁶⁾ *Schrems*, præmis 65.

⁽⁴⁰⁷⁾ *Schrems*, præmis 65: »I denne henseende påhviler det den nationale lovgiver at fastsætte retsmidler, der gør det muligt for den pågældende nationale tilsynsmyndighed at gøre de klagepunkter, som den finder begrundede, gældende for de nationale domstole, således at disse, såfremt de deler myndighedens tvivl vedrørende gyldigheden af Kommissionens afgørelse, kan foretage en præjudiciel forelæggelse med henblik på en efterprøvelse af denne afgørelses gyldighed.«

⁽⁴⁰⁸⁾ *Schrems*, præmis 76.

- (211) I henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 ⁽⁴⁰⁹⁾ bør Kommissionen efter vedtagelsen af denne afgørelse med regelmæssige mellemrum undersøge, om konstateringen af, at USA sikrer et tilstrækkeligt beskyttelsesniveau under EU-USA-databeskyttelsesrammen, stadig er faktisk og retligt begrundet. Da navnlig EO 14086 og justitsministerens forordning kræver, at der oprettes nye mekanismer og indføres nye garantier, bør denne afgørelse underkastes en første revision senest et år efter dens ikrafttræden for at kontrollere, om alle relevante elementer er blevet gennemført fuldt ud og fungerer effektivt i praksis. Efter denne første revision og afhængigt af resultatet heraf vil Kommissionen i tæt samråd med det udvalg, der er nedsat i henhold til artikel 93, stk. 1, i forordning (EU) 2016/679 og Det Europæiske Databeskyttelsesråd, træffe afgørelse om hyppigheden af fremtidige revisioner ⁽⁴¹⁰⁾.
- (212) Med henblik på denne revision skal Kommissionen mødes med det amerikanske handelsministerium, FTC og det amerikanske transportministerium, i påkommende tilfælde ledsaget af repræsentanter fra andre ministerier og agenturer involveret i gennemførelsen af EU-USA-databeskyttelsesrammen, og i forbindelse med de statslige myndigheders adgang til oplysninger med repræsentanter fra justitsministeriet, ODNI (herunder CLPO), andre efterretningsenheder, DPRC og de særlige advokater. Repræsentanter fra Det Europæiske Databeskyttelsesråd bør have mulighed for at deltage i dette møde.
- (213) Revisionerne bør omfatte alle aspekter af denne afgørelses funktionsmåde i forbindelse med behandlingen af personoplysninger i USA, navnlig anvendelsen og gennemførelsen af principperne, idet der lægges særlig vægt på den beskyttelse, der ydes i tilfælde af videreoverførsel, den relevante udvikling i retspraksis, effektiviteten af udøvelsen af individuelle rettigheder, overvågningen og håndhævelsen af princippernes overholdelse samt begrænsninger og sikkerhedsforanstaltninger med hensyn til statslig adgang, navnlig gennemførelsen og anvendelsen af de garantier, der blev indført ved EO 14086, herunder gennem politikker og procedurer udviklet af efterretningsagenturer, samspillet mellem EO 14086 og Section 702 i FISA og EO 12333 og effektiviteten af tilsynsmekanismerne og klagemulighederne (herunder funktionen af den nye klagemekanisme, der blev oprettet i henhold til EO 14086). I forbindelse med sådanne revisioner vil der også blive lagt vægt på samarbejdet mellem databeskyttelsesmyndighederne og USA's kompetente myndigheder, herunder udvikling af retningslinjer og andre fortolkningsværktøjer vedrørende anvendelsen af principperne samt andre aspekter af rammens funktion.
- (214) Kommissionen bør udarbejde en offentlig rapport til Europa-Parlamentet og Rådet på grundlag af denne revision.

7. SUSPENSION, OPHÆVELSE ELLER ÆNDRING AF DENNE AFGØRELSE

- (215) Hvis tilgængelige oplysninger, navnlig oplysninger fra overvågningen af denne afgørelse eller fra USA's eller medlemsstaternes myndigheder, viser, at beskyttelsesniveauet for oplysninger, der overføres i henhold til denne afgørelse, muligvis ikke længere er tilstrækkeligt, bør Kommissionen straks underrette de kompetente amerikanske myndigheder herom og anmode om, at der træffes passende foranstaltninger inden for en angivet rimelig tidsramme.
- (216) Hvis de kompetente amerikanske myndigheder efter udløbet af den angivne tidsramme ikke har truffet disse foranstaltninger eller ikke på tilfredsstillende vis dokumenterer, at denne afgørelse fortsat er baseret på et tilstrækkeligt beskyttelsesniveau, vil Kommissionen indlede proceduren i artikel 93, stk. 2, i forordning (EU) 2016/679 med henblik på helt eller delvis at suspendere eller ophæve denne afgørelse.
- (217) Alternativt vil Kommissionen indlede den pågældende procedure med henblik på at ændre afgørelsen, f.eks. ved at underkaste dataoverførsler yderligere betingelser eller ved at begrænse anvendelsesområdet for konstateringen af et tilstrækkeligt beskyttelsesniveau til dataoverførsler, for hvilke der fortsat sikres et tilstrækkeligt beskyttelsesniveau.

⁽⁴⁰⁹⁾ Artikel 45, stk. 3, i forordning (EU) 2016/679 bestemmer, at »[i] den pågældende gennemførelsesretsakt fastsættes en mekanisme for regelmæssig revision, [...] som inddrager enhver relevant udvikling i tredjelandet eller den internationale organisation«.

⁽⁴¹⁰⁾ Artikel 45, stk. 3, i forordning (EU) 2016/679 fastsætter, at en regelmæssig revision skal foretages »mindst hvert fjerde år«. Jf. endvidere Det Europæiske Databeskyttelsesråd, Adequacy Referential, WP 254 rev. 01.

- (218) Kommissionen bør navnlig indlede proceduren for suspension eller ophævelse:
- (a) når der er tegn på, at organisationer, der har modtaget personoplysninger fra Unionen i henhold til denne afgørelse, ikke overholder principperne, og når en sådan manglende overholdelse ikke håndteres effektivt af de kompetente tilsyns- og håndhævelsesorganer,
 - (b) når der er tegn på, at de amerikanske myndigheder ikke overholder de gældende betingelser og begrænsninger for de amerikanske offentlige myndigheders adgang til personoplysninger, der overføres inden for rammerne af EU-USA-databeskyttelsesrammen med henblik på retshåndhævelse og beskyttelse af den nationale sikkerhed, eller
 - (c) når ODNI CLPO og/eller DPRC ikke behandler klager fra registrerede i EU effektivt.
- (219) Kommissionen bør ligeledes overveje at indlede proceduren med henblik på ændring, suspension eller ophævelse af denne afgørelse, hvis ikke de amerikanske myndigheder forelægger de oplysninger og præciseringer, der er nødvendige for at vurdere beskyttelsesniveauet for personoplysninger, der overføres fra Unionen til USA, eller med hensyn til overholdelsen af denne afgørelse. I den forbindelse bør Kommissionen tage hensyn til, i hvilket omfang de relevante oplysninger kan indhentes fra andre kilder.
- (220) I behørigt begrundede særligt hastende tilfælde, f.eks. hvis EO 14086 eller justitsministerens forordning ændres på en måde, der underminerer det beskyttelsesniveau, der er beskrevet i denne afgørelse, eller hvis den amerikanske justitsministers udpegelse af Unionen som en kvalificeret organisation med henblik på klagemekanismen trækkes tilbage, vil Kommissionen gøre brug af muligheden for efter proceduren i artikel 93, stk. 3, i forordning (EU) 2016/679 at vedtage gennemførelsesretsakter, der finder anvendelse straks, om suspension, ophævelse eller ændring af denne afgørelse.

8. AFSLUTTENDE BETRAGTNINGER

- (221) Det Europæiske Databeskyttelsesråd har offentliggjort sin udtalelse ⁽⁴¹¹⁾, som er blevet taget i betragtning ved udarbejdelsen af denne afgørelse.
- (222) Europa-Parlamentet vedtog en beslutning om tilstrækkeligheden af den beskyttelse, som EU-USA-databeskyttelsesrammen giver ⁽⁴¹²⁾.
- (223) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 93, stk. 1, i forordning (EU) 2016/679 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Med henblik på artikel 45 i forordning (EU) 2016/679 sikrer USA et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til organisationer i USA, som er opført på listen over deltagende organisationer i databeskyttelsesrammen (Data Privacy Framework List), der vedligeholdes og gøres offentligt tilgængelig af det amerikanske handelsministerium i overensstemmelse med afsnit I.3 i bilag I.

Artikel 2

Når de kompetente myndigheder i medlemsstaterne, med det formål at beskytte personer i forbindelse med behandlingen af deres personoplysninger, udøver deres beføjelser i medfør af artikel 58 i forordning (EU) 2016/679 for så vidt angår dataoverførsler, som er omhandlet i denne afgørelses artikel 1, underretter den pågældende medlemsstat straks Kommissionen herom.

⁽⁴¹¹⁾ Udtalelse 5/2023 om Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i henhold til EU-USA-databeskyttelsesrammen af 28. februar 2023.

⁽⁴¹²⁾ Europa-Parlamentets beslutning af 11. maj 2023 om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af rammen for databeskyttelse mellem EU og USA (2023/2501 (RSP)).

Artikel 3

1. Kommissionen overvåger løbende anvendelsen af den retlige ramme, der er omfattet af denne afgørelse, herunder betingelserne for videreoverførsel, for udøvelsen af individuelle rettigheder og for de amerikanske offentlige myndigheders adgang til oplysninger, der overføres på grundlag af denne afgørelse, for at vurdere, om USA fortsat sikrer et tilstrækkeligt beskyttelsesniveau, som omhandlet i artikel 1.
2. Medlemsstaterne og Kommissionen underretter hinanden om tilfælde, hvor organer i USA med lovbestemte beføjelser til at håndhæve overholdelsen af principperne i bilag I tilsyneladende ikke har indført effektive afslørings- og tilsynsmekanismer, der gør det muligt i praksis at identificere og sanktionere tilsidesættelser af principperne i bilag I.
3. Medlemsstaterne og Kommissionen underretter hinanden om tilfælde, hvor de amerikanske myndigheder med ansvar for den nationale sikkerhed, retshåndhævelse eller andre offentlige interesser tilsyneladende griber ind i den enkeltes ret til beskyttelse af sine personoplysninger på en måde, der går ud over, hvad der er nødvendigt og rimeligt, og/eller hvor der tilsyneladende ikke er en effektiv retsbeskyttelse mod sådanne indgreb.
4. Et år efter datoen for meddelelse af denne afgørelse til medlemsstaterne og herefter med en hyppighed, der besluttet i tæt samråd med det udvalg, der er nedsat i henhold til artikel 93, stk. 1, i forordning (EU) 2016/679, og Det Europæiske Databeskyttelsesråd, evaluerer Kommissionen konklusionen i artikel 1, stk. 1, på grundlag af alle tilgængelige oplysninger, herunder de oplysninger, der er indhentet som led i den revision, der er foretaget i samarbejde med de kompetente amerikanske myndigheder.
5. Hvis der er tegn på, at der ikke længere er sikret et tilstrækkeligt beskyttelsesniveau, underretter Kommissionen de kompetente amerikanske myndigheder herom. Den træffer om nødvendigt afgørelse om at suspendere, ændre eller ophæve denne afgørelse eller begrænse dens anvendelsesområde i overensstemmelse med artikel 45, stk. 5, i forordning (EU) 2016/679. Kommissionen kan desuden træffe en sådan afgørelse, hvis den amerikanske regerings manglende samarbejde forhindrer Kommissionen i at afgøre, om USA fortsat sikrer et tilstrækkeligt beskyttelsesniveau.

Artikel 4

Denne afgørelse er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 10. juli 2023.

På Kommissionens vegne
Didier REYNDERS
Medlem af Kommissionen

BILAG I**PRINCIPPERNE I EU-USA-DATABESKYTTELSESRAMMEN FRA DET AMERIKANSKE
HANDELSMINISTERIUM****I. OVERSIGT**

1. Selv om USA og Den Europæiske Union ("EU") har en fælles forpligtelse til at fremme beskyttelsen af privatlivets fred, retsstatsprincippet og en anerkendelse af betydningen af transatlantiske datastrømme for vores respektive borgere, økonomier og samfund, er den valgte fremgangsmåde ikke den samme. I USA anvendes således en fremgangsmåde på sektorplan med en kombination af lovgivning, administrative bestemmelser og selvregulering. Det amerikanske handelsministerium ("ministeriet") har i medfør af sine lovbestemte beføjelser udstedt principperne i EU-USA-databeskyttelsesrammen, herunder de supplerende principper (samlet benævnt "principperne") og bilag I til principperne ("bilag I"), med henblik på at fremme og udvikle den internationale handel (15 U.S.C. § 1512). Principperne er udviklet i samarbejde med Europa-Kommissionen ("Kommissionen"), industrien og andre interessenter for at fremme handelen mellem USA og EU. Principperne, som er et centralt element i EU-USA-databeskyttelsesrammen, giver organisationer i USA en pålidelig mekanisme til overførsel af personoplysninger til USA fra EU, samtidig med at det sikres, at registrerede i EU fortsat nyder effektive garantier og effektiv beskyttelse som krævet i EU-lovgivningen med hensyn til behandlingen af deres personoplysninger, når de er blevet overført til lande uden for EU. Principperne er udelukkende beregnet på at blive anvendt af berettigede amerikanske organisationer, der modtager personoplysninger fra EU, og som ønsker at leve op til kravene i EU-USA-databeskyttelsesrammen og således drage fordel af Europa-Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet ⁽¹⁾. Principperne har ingen indvirkning på anvendelsen af forordning (EU) 2016/679 ("den generelle forordning om databeskyttelse" eller "databeskyttelsesforordningen") ⁽²⁾, som vedrører behandling af personoplysninger i EU-medlemsstaterne. Principperne begrænser heller ikke andre forpligtelser til at sikre privatlivets fred i amerikansk ret.
2. For at kunne overføre personoplysninger fra EU under EU-USA-databeskyttelsesrammen skal en organisation gennemføre selvcertificering om tilslutning til principperne over for ministeriet (eller dets repræsentant). En organisation kan frit vælge, om den vil tilslutte sig EU-USA-databeskyttelsesrammen, men den skal overholde principperne fuldt ud. En organisation, der foretager selvcertificering over for ministeriet og offentligt erklærer, at den har tilsluttet sig principperne, skal således overholde principperne fuldt ud. Inden en organisation kan tilslutte sig EU-USA-databeskyttelsesrammen, skal den: a) omfattes af de undersøgelses- og håndhævelsesbeføjelser, der er tillagt Federal Trade Commission ("FTC"), det amerikanske transportministerium eller ethvert andet lovbestemt organ, der kan sikre overholdelse af principperne (*andre lovbestemte amerikanske organer, der er godkendt af EU, kan inkluderes som et bilag på et senere tidspunkt*), b) offentligt erklære, at den forpligter sig til at overholde principperne, c) offentliggøre sine politikker til beskyttelse af privatlivets fred i overensstemmelse med disse principper og d) gennemføre dem fuldt ud ⁽³⁾. Såfremt en organisation ikke overholder principperne, kan den drages til ansvar af FTC i henhold til Section 5 i Federal Trade Commission (FTC) Act, der forbyder illoyal eller vildledende praksis i forbindelse med handel (15 U.S.C. § 45), af transportministeriet i henhold til 49 U.S.C. § 41712, der forbyder transportører eller rejsebureauer at anvende en illoyal eller vildledende praksis i forbindelse med lufttransportydelser eller salg af lufttransportydelser, eller i henhold til andre love eller bestemmelser, der forbyder denne praksis.

⁽¹⁾ Forudsat at Kommissionens afgørelse om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU-USA-databeskyttelsesrammen, finder anvendelse på Island, Liechtenstein og Norge, omfatter EU-USA-databeskyttelsesrammen både EU og disse tre lande. Henvisninger til EU og EU's medlemsstater læses derfor som omfattende Island, Liechtenstein og Norge.

⁽²⁾ 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).

⁽³⁾ Principperne i EU's og USA's værn om privatlivets fred (EU-USA-privatlivsskjoldet) er blevet ændret til "principperne i EU-USA-databeskyttelsesrammen" (jf. det supplerende princip om selvcertificering).

3. Ministeriet vil oprette og offentliggøre en officiel liste over amerikanske organisationer, der har foretaget selvcertificering over for ministeriet og offentligt erklæret, at de har tilsluttet sig principperne ("listen over deltagere i databeskyttelsesrammen"). Organisationen drager fordel af EU-USA-databeskyttelsesrammen fra den dato, hvor ministeriet opfører organisationen på listen over deltagere i databeskyttelsesrammen. Ministeriet vil fjerne organisationer fra listen over deltagere i databeskyttelsesrammen, hvis de frivilligt trækker sig ud af EU-USA-databeskyttelsesrammen eller ikke indsender deres årlige anmeldelse om recertificering til ministeriet. Disse organisationer skal enten blive ved med at anvende principperne på de personoplysninger, som de modtog i henhold til EU-USA-databeskyttelsesrammen, og hvert år bekræfte over for ministeriet, at de fortsat vil anvende principperne (dvs. så længe de er i besiddelse af disse oplysninger), sikre en "tilstrækkelig" beskyttelse af personoplysningerne på en anden godkendt måde (f.eks. ved hjælp af en aftale, der fuldt ud afspejler kravene i de relevante standardkontraktbestemmelser, som Kommissionen har vedtaget) eller tilbagesende eller slette oplysningerne. Ministeriet vil ligeledes fjerne de organisationer fra listen over deltagere i databeskyttelsesrammen, der vedvarende overtræder principperne om beskyttelse af privatlivets fred. Disse organisationer skal tilbagesende eller slette personoplysninger modtaget under EU-USA-databeskyttelsesrammen. Hvis en organisation fjernes fra listen over deltagere i databeskyttelsesrammen, kan den ikke længere drage fordel af Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet til at modtage personoplysninger fra EU.
4. Ministeriet vil ligeledes oprette og offentliggøre en officiel fortegnelse over amerikanske organisationer, der tidligere har foretaget selvcertificering over for ministeriet, men som er blevet fjernet fra listen over deltagere i databeskyttelsesrammen. Ministeriet vil klart advare om, at disse organisationer ikke deltager i EU-USA-databeskyttelsesrammen, at fjernelse fra listen over deltagere i databeskyttelsesrammen betyder, at disse organisationer ikke kan hævde, at de overholder principperne i EU-USA-databeskyttelsesrammen, og skal undgå erklæringer eller vildledende praksis, der lader formode, at de deltager i databeskyttelsesrammen, og at disse organisationer ikke længere kan drage fordel af Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet til at modtage personoplysninger fra EU. FTC, transportministeriet eller andre håndhævelsesmyndigheder kan træffe håndhævelsesforanstaltninger over for en organisation, der fortsat hævder, at den deltager i EU-USA-databeskyttelsesrammen, eller afgiver andre urigtige oplysninger om EU-USA-databeskyttelsesrammen, efter at den er blevet fjernet fra listen over deltagere i databeskyttelsesrammen.
5. Tilslutning til disse principper kan være begrænset a) til et niveau, der er tilstrækkeligt til at efterkomme en retsafgørelse eller opfylde kravene med hensyn til den offentlige interesse, retshåndhævelsen eller den nationale sikkerhed, herunder når love eller administrative bestemmelser medfører modstridende forpligtelser, b) af love, retsafgørelser eller administrative bestemmelser, der medfører udtrykkelige tilladelser, såfremt organisationer i forbindelse med anvendelsen af sådanne tilladelser kan påvise, at de kun overtræder principperne i det omfang, som er nødvendigt for at tilgodese de altovervejende legitime interesser, som den pågældende tilladelse har til hensigt at fremme, eller c) i det omfang, databeskyttelsesforordningen tillader undtagelser eller dispensationer på de betingelser, der er fastsat deri, såfremt sådanne undtagelser eller dispensationer også finder anvendelse i sammenlignelig kontekst. I denne forbindelse omfatter garantier i amerikansk ret til beskyttelse af privatlivets fred og borgerlige frihedsrettigheder de garantier, der kræves i Executive Order 14086 ⁽⁴⁾, på de betingelser, der er fastsat deri (herunder kravene om nødvendighed og proportionalitet). I overensstemmelse med det overordnede mål om at fremme beskyttelsen af privatlivets fred bør organisationerne bestræbe sig på at gennemføre disse principper på fuldstændig og gennemskuelig vis, hvilket omfatter, at de i deres politikker til beskyttelse af privatlivets fred angiver, på hvilke punkter eventuelle undtagelser fra principperne i henhold til ovenstående punkt b) finder anvendelse. Når principperne og/eller amerikansk ret giver mulighed derfor, forventes organisationerne af samme årsag at vælge det højere beskyttelsesniveau, når det er muligt.
6. Organisationerne er forpligtet til at anvende principperne på alle personoplysninger overført under EU-USA-databeskyttelsesrammen, efter at de har tilsluttet sig EU-USA-databeskyttelsesrammen. En organisation, der ønsker at udvide sin dækning under EU-USA-databeskyttelsesrammen til også at omfatte personoplysninger om menneskelige ressourcer, der overføres fra EU med henblik på anvendelse inden for rammerne af et ansættelsesforhold, skal oplyse om dette, når den foretager selvcertificering over for handelsministeriet, og opfylde de krav, der er fastsat i det supplerende princip om selvcertificering.

⁽⁴⁾ Præsidentielt dekret af 7.10.2022, "Enhancing Safeguards for United States Signals Intelligence Activities".

7. Amerikansk ret finder anvendelse på fortolkningen og overholdelsen af principperne og relevante politikker til beskyttelse af privatlivets fred iværksat af organisationer, som deltager i EU-USA-databeskyttelsesrammen, undtagen når disse organisationer har forpligtet sig til at samarbejde med de europæiske databeskyttelsesmyndigheder. Medmindre andet er fastsat, finder alle bestemmelser i principperne anvendelse, når det er relevant.
8. Definitioner:
 - a. "personoplysninger": oplysninger, som kan henføres til en bestemt identificeret eller identificerbar person, som er omfattet af databeskyttelsesforordningen, som modtages fra EU af en organisation i USA, og som er registreret på en hvilken som helst måde.
 - b. "behandling" af personoplysninger: enhver operation eller række af operationer — med eller uden brug af elektronisk databehandling — som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse eller formidling og sletning eller tilintetgørelse.
 - c. "dataansvarlig": en person eller en organisation, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.
9. Principperne og bilag I til principperne finder anvendelse fra ikrafttrædelsesdatoen for Europa-Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

II. PRINCIPPER

1. OPLYSNINGSPLIGT

- a. En organisation skal oplyse registrerede om:
 - i. sin deltagelse i EU-USA-databeskyttelsesrammen og angive et link til eller webadressen for listen over deltagere i databeskyttelsesrammen
 - ii. typer indsamlede personoplysninger og i påkommende tilfælde de amerikanske enheder eller datterselskaber, der ligeledes har tilsluttet sig principperne
 - iii. sit tilsagn om at anvende principperne på alle personoplysninger modtaget fra EU under EU-USA-databeskyttelsesrammen
 - iv. hvilke formål der ligger til grund for indsamlingen og anvendelsen af personoplysninger om de pågældende
 - v. hvorledes organisationen kan kontaktes i tilfælde af forespørgsler eller klager, herunder det relevante organ i EU, som kan besvare sådanne forespørgsler eller klager
 - vi. til hvilken type tredjemand oplysningerne videregives, og formålet hermed
 - vii. den enkeltes ret til adgang til sine personoplysninger
 - viii. de valgmuligheder og midler, som organisationen tilbyder den enkelte med henblik på at begrænse anvendelsen eller videregivelsen af dennes personoplysninger
 - ix. den udpegede uafhængige tvistbilæggelsesinstans, der behandler klager og sikrer registrerede gratis passende klageadgang, og oplyse, om denne instans er: 1) det panel, som er oprettet af databeskyttelsesmyndighederne, 2) en alternativ tvistbilæggelsesinstans i EU eller 3) en alternativ tvistbilæggelsesinstans i USA
 - x. det forhold, at organisationen er omfattet af de undersøgelses- og håndhævelsesbeføjelser, der er tillagt FTC, transportministeriet eller ethvert andet amerikansk bemyndiget organ oprettet ved lov
 - xi. den enkeltes mulighed for på visse betingelser at kræve, at en sag afgøres ved bindende voldgift ⁽⁵⁾
 - xii. kravet om, at den skal videregive personoplysninger på grundlag af offentlige myndigheders lovlige anmodninger, herunder for at opfylde nationale sikkerheds- og retshåndhævelseskrav, og
 - xiii. sit ansvar for videreoverførsel til tredjemand.

⁽⁵⁾ Jf. f.eks. afsnit c. under princippet om klageadgang, håndhævelse og ansvar.

- b. Oplysningspligten skal formidles klart og tydeligt, når den enkelte første gang anmodes om at levere personoplysninger til organisationen, eller så hurtigt som muligt derefter, dog under alle omstændigheder inden organisationen anvender de pågældende personoplysninger til et andet formål end det, hvortil de oprindeligt blev indsamlet eller behandlet af den organisation, der har overført oplysningerne eller videregiver dem for første gang til tredjemand.

2. VALGFRIHED

- a. En organisation skal give den enkelte mulighed for at vælge (dvs. opt out), hvorvidt dennes personoplysninger kan i) videregives til tredjemand eller ii) anvendes til et formål, der er væsentligt forskelligt fra det eller de formål, hvortil personoplysningerne oprindeligt blev indsamlet, eller hvortil den enkelte efterfølgende har givet tilladelse. Den enkelte skal kunne anvende denne valgfrihed på en klar, åbenlys og let tilgængelig måde.
- b. Uanset ovennævnte finder princippet om valgfrihed ikke anvendelse ved videregivelse til tredjemand, som fungerer som mellemmand og udfører opgaver på vegne af organisationen og i henhold til dens instrukser. Organisationens skal imidlertid altid indgå en aftale med mellemmanden.
- c. I tilfælde af følsomme oplysninger (dvs. personoplysninger om helbredsforhold, race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmedlemskab eller oplysninger om seksuelle forhold) skal de pågældende organisationer indhente de pågældende personers udtrykkelige samtykke (dvs. opt in), hvis oplysningerne skal i) videregives til tredjemand eller ii) anvendes til et andet formål end det, hvortil de oprindeligt er blevet indsamlet, eller som de pågældende personer på grundlag af deres valgfrihed efterfølgende har givet tilladelse til. En organisation skal under alle omstændigheder behandle enhver personoplysning, som den modtager fra tredjemand, som følsom, når oplysningen af den pågældende tredjemand betegnes og behandles som sådan.

3. ANSVAR FOR VIDEREOVERFØRSEL

- a. En organisation må udelukkende overføre personoplysninger til tredjemand, der handler som dataansvarlig, hvis den overholder principperne om oplysningspligt og valgfrihed. Organisationer skal også indgå en aftale med den dataansvarlige tredjemand, som sikrer, at disse oplysninger kun behandles til begrænsede og bestemte formål, der er i overensstemmelse med den registreredes samtykke, og at modtageren sikrer det samme niveau af beskyttelse som i principperne og underretter organisationen, hvis det fastslås, at denne ikke længere kan opfylde denne pligt. Det skal fremgå af aftalen, at når dette fastslås, skal den dataansvarlige tredjemand ophøre med behandlingen eller træffe andre rimelige og passende korrigerende foranstaltninger.
- b. Ved overførsel af personoplysninger til tredjemand, der fungerer som mellemmand, skal organisationen: i) kun overføre disse oplysninger til begrænsede og bestemte formål, ii) bekræfte, at mellemmanden er forpligtet til at sikre mindst samme beskyttelse af privatlivets fred som i principperne, iii) træffe rimelige og passende foranstaltninger for at sikre, at mellemmanden rent faktisk behandler de overførte personoplysninger i overensstemmelse med organisationens forpligtelser i henhold til principperne, iv) kræve, at mellemmanden underretter organisationen, hvis det fastslås, at denne ikke længere kan opfylde sin pligt til at sikre samme beskyttelse af privatlivets fred som i principperne, v) efter varsel, som f.eks. under punkt iv), tage rimelige og passende skridt til at stoppe og afhjælpe uautoriseret behandling og vi) på anmodning forelægge ministeriet et sammendrag eller en repræsentativ kopi af de relevante bestemmelser om beskyttelse af privatlivets fred i aftalen med den pågældende mellemmand.

4. SIKKERHED

- a. Organisationer, der opretter, vedligeholder, anvender eller videregiver personoplysninger, skal træffe rimelige og passende foranstaltninger for at beskytte disse oplysninger mod tab, misbrug og uautoriseret adgang, videregivelse, ændring og tilintetgørelse under behørig hensyntagen til de risici, som behandlingen indebærer, og de pågældende oplysningers karakter.

5. DATAINTEGRITET OG FORMÅLSBEGRÆNSNING

- a. I overensstemmelse med principperne skal personoplysninger være begrænset til de oplysninger, der er relevante for formålene med behandlingen ⁽⁶⁾. En organisation må ikke behandle personoplysninger på en måde, der ikke er i overensstemmelse med de formål, hvortil de oprindeligt er blevet indsamlet, eller det formål, der efterfølgende er blevet godkendt af den registrerede. En organisation skal, i det omfang det er nødvendigt, træffe passende foranstaltninger for at sikre, at personoplysningerne er pålidelige, nøjagtige, fuldstændige og ajourførte. En organisation skal overholde principperne, så længe den er i besiddelse af disse oplysninger.
- b. Oplysninger må kun opbevares på en måde, der gør det muligt at identificere den enkelte person eller gøre denne identificerbar ⁽⁷⁾, så længe de tjener et formål for behandling i den i punkt 5.a. anvendte betydning. Denne forpligtelse forhindrer ikke organisationer i at behandle personoplysninger i længere perioder, men dog kun så længe og i det omfang en sådan behandling med rimelighed tjener til arkiveringsformål i offentlighedens interesse, til brug i journalistik, litteratur og kunst samt til videnskabelig eller historisk forskning og statistisk analyse. I disse tilfælde skal behandlingen underlægges de andre principper og bestemmelser i EU-USA-databeskyttelsesrammen. Organisationerne bør træffe rimelige og passende foranstaltninger for at overholde denne bestemmelse.

6. INDSIGT

- a. Den registrerede skal have adgang til de personoplysninger, som en organisation er i besiddelse af om den pågældende, og skal have mulighed for at rette, ændre eller fjerne ukorrekte oplysninger eller oplysninger behandlet i strid med principperne, medmindre meradministrationen eller meromkostningerne ved at give indsigt i det enkelte tilfælde ville være uforholdsmæssig store i forhold til risikoen for den pågældendes privatliv, eller medmindre andre personers rettigheder herved krænkes.

7. KLAGEADGANG, HÅNDHÆVELSE OG ANSVAR

- a. En effektiv beskyttelse af privatlivets fred forudsætter en række solide mekanismer til at sikre, at principperne overholdes, at den enkelte kan klage, hvis principperne ikke overholdes, og at det får konsekvenser for en organisation, hvis den ikke overholder principperne. Disse mekanismer skal som minimum omfatte:
 - i. let tilgængelige uafhængige klageprocedurer, der gør det muligt under henvisning til principperne at undersøge og hurtigt afgøre klager fra den registrerede uden omkostninger for den pågældende samt give erstatning, når der i medfør af loven eller private ordninger er mulighed derfor
 - ii. kontrolprocedurer med henblik på at undersøge, om organisationer lever op til de erklæringer og løfter, de har afgivet om deres databeskyttelsesforanstaltninger, og om disse foranstaltninger er blevet iværksat som beskrevet, navnlig i tilfælde af manglende overholdelse, og
 - iii. en forpligtelse til at afhjælpe eventuelle problemer, som skyldes, at en organisation, der har erklæret at ville tilslutte sig principperne, ikke overholder disse, samt til at overholde sanktioner for disse organisationer. Disse sanktioner skal være af en sådan karakter, at organisationerne tilskyndes til at overholde principperne.
- b. Organisationerne og deres udpegede uafhængige klageinstanser skal straks besvare forespørgsler og anmodninger fra ministeriet om oplysninger vedrørende EU-USA-databeskyttelsesrammen. Alle organisationer skal straks besvare klager over manglende overholdelse af principperne, som henvises af EU-medlemsstaternes myndigheder via ministeriet. Organisationer, der har valgt at samarbejde med databeskyttelsesmyndighederne, herunder organisationer, der behandler oplysninger om menneskelige ressourcer, skal underrette disse myndigheder direkte om undersøgelser og afgørelser af klager.

⁽⁶⁾ Eksempler på formål, der er forenelige med behandlingen, kan alt efter omstændighederne omfatte de formål, der med rimelighed tjener kunderelationer, efterlevelse og juridiske overvejelser, revision, sikkerhed og bekæmpelse af svig, bevarelse eller beskyttelse af organisationens juridiske rettigheder, eller andre formål, der stemmer overens med en fornuftig persons forventninger i lyset af baggrunden for indsamlingen.

⁽⁷⁾ I denne forbindelse anses en person for at være "identificerbar", såfremt den pågældende i betragtning af den med rimelighed forventede identifikationsmetode (under hensyntagen til bl.a. omkostningerne og det fornødne tidsforbrug ved identificeringen samt den på behandlingstidspunktet tilgængelige teknologi) og den måde, som oplysningerne opbevares på, med rimelighed kan identificeres af organisationen eller af en tredjemand, hvis denne har adgang til oplysningerne.

- c. Organisationer er forpligtet til at lade klager afgøre ved voldgift og overholde betingelserne i bilag I, hvis den registrerede har krævet klagen afgjort ved bindende voldgift ved fremsendelse af en meddelelse herom til den pågældende organisation i overensstemmelse med procedurerne og på de betingelser, der er anført i bilag I.
- d. I forbindelse med videreoverførsel har en organisation, der deltager i databeskyttelsesrammen, ansvaret for behandlingen af de personoplysninger, den modtager under EU-USA-databeskyttelsesrammen, og for efterfølgende overførsler til en tredjemand, der fungerer som mellemmand på dens vegne. Den deltagende organisation har fortsat ansvaret i henhold til principperne, hvis dens mellemmand behandler disse personoplysninger i strid med principperne, medmindre organisationen beviser, at den ikke er skyld i den skadevoldende hændelse.
- e. Når en organisation bliver genstand for en retsafgørelse om manglende overholdelse eller en afgørelse om manglende overholdelse fra et amerikansk lovbestemt organ (f.eks. FTC eller transportministeriet), som er opført i principperne eller i et fremtidigt bilag til principperne, skal organisationen offentliggøre alle relevante afsnit relateret til EU-USA-databeskyttelsesrammen i alle overholdelses- eller vurderingsrapporter forelagt retten eller det amerikanske lovbestemte organ, i det omfang det er foreneligt med fortrolighedskrav. Ministeriet har udpeget et særligt kontaktpunkt, som databeskyttelsesmyndighederne kan rette henvendelse til, når deltagende organisationer ikke overholder principperne. FTC og transportministeriet vil give højeste prioritet til sager om manglende overholdelse af principperne, som den får henvist fra ministeriet og EU-medlemsstaternes myndigheder, og vil udveksle oplysninger om henviste sager rettidigt med de henvisende statslige myndigheder, i det omfang det er foreneligt med fortrolighedskrav.

III. SUPPLERENDE PRINCIPPER

1. Følsomme oplysninger

- a. En organisation skal ikke indhente udtrykkeligt samtykke (dvs. opt in) i forbindelse med følsomme oplysninger, hvis behandlingen:
 - i. er nødvendig for at beskytte den registreredes eller andre personers vitale interesser
 - ii. er nødvendig for at fastslå eller forsvare et retskrav
 - iii. er nødvendig i forbindelse med medicinsk behandling eller diagnosticering
 - iv. foretages af en stiftelse, en forening eller et andet almenntilgængeligt organ, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, som led i organets legitime aktiviteter, på betingelse af at behandlingen alene vedrører organets medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at oplysningerne ikke videregives til tredjemand uden den registreredes samtykke
 - v. er nødvendig for overholdelsen af en organisations arbejdsretlige forpligtelser eller
 - vi. vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede.

2. Journalistiske undtagelser

- a. Henset til beskyttelsen af pressefriheden i henhold til den amerikanske forfatning skal der, når princippet om pressefrihed som nedfældet i den amerikanske forfatnings første amendement strider imod beskyttelsen af privatlivets fred, foretages en afvejning af disse interesser i henhold til første amendement, når det drejer sig om amerikanske borgeres eller organisationers aktiviteter.
- b. Personoplysninger, der indsamles med henblik på offentliggørelse, radio- eller TV-udsendelser eller andre former for offentlig kommunikation af journalistisk materiale, uanset om de anvendes, og oplysninger, der stammer fra tidligere offentliggjort materiale, der opbevares i et pressearkiv, er ikke underlagt principperne.

3. Subsidiært ansvar

- a. Internetudbydere, teleselskaber eller andre organisationer er ikke ansvarlige i henhold til principperne, når de på vegne af andre organisationer blot sender, dirigerer, omstiller eller lagrer oplysninger. EU-USA-databeskyttelsesrammen danner ikke grundlag for subsidiært ansvar. En organisation kan ikke drages til ansvar, når den udelukkende formidler oplysninger, der overføres af tredjemand, uden hverken at bestemme formålet med eller metoderne til behandling af de pågældende personoplysninger.

4. Udførelse af due diligence og revisioner

- a. Investeringsbankers og revisorers aktiviteter kan omfatte behandling af personoplysninger, uden at den enkelte har givet tilladelse dertil eller er vidende derom. Dette er tilladt i henhold til principperne om oplysningspligt, valgfrihed og indsigt under de nedenfor beskrevne omstændigheder.
- b. Offentlige aktieselskaber og nært ejede selskaber, herunder organisationer, som deltager i EU-USA-databeskyttelsesrammen, revideres jævnligt. Disse revisioner, navnlig revisioner, hvor der ses nærmere på eventuelle uregelmæssigheder, kan sættes på spil ved en for tidlig videregivelse. En organisation i EU-USA-databeskyttelsesrammen, der er involveret i en potentiel fusion eller overtagelse, skal udføre eller underkastes en "due diligence"-undersøgelse. Dette vil ofte indebære indsamling og behandling af personoplysninger såsom oplysninger om den øverste ledelse og andet nøglepersonale. En for tidlig videregivelse kunne hindre transaktionen eller endog være i strid med gældende værdipapirbestemmelser. Investeringsbanker og advokater, der foretager due diligence, og revisorer, der foretager en revision, kan kun behandle oplysninger, uden at den registrerede er vidende derom, i det omfang og i den periode, som er nødvendig for at overholde lovbestemte krav eller tilgodese vigtige samfundsinteresser, samt i andre situationer, hvor anvendelsen af disse principper vil være til skade for organisationens legitime interesser. Disse legitime interesser omfatter overvågningen af organisationers overholdelse af deres retlige forpligtelser og legitime regnskabsaktiviteter samt behovet for fortrolighed i forbindelse med eventuelle opkøb, fusioner, joint ventures eller lignende aktiviteter, der udøves af investeringsbanker eller revisorer.

5. Databeskyttelsesmyndighedernes rolle

- a. Organisationer skal opfylde deres forpligtelser til at samarbejde med databeskyttelsesmyndighederne som beskrevet nedenfor. Amerikanske organisationer, der modtager personoplysninger fra EU, er i medfør af EU-USA-databeskyttelsesrammen forpligtet til at iværksætte effektive metoder, der gør dem i stand til at overholde principperne. Mere specifikt skal de som fastsat i princippet om klageadgang, håndhævelse og ansvar: punkt a, nr. i, give de registrerede mulighed for at klage, punkt a, nr. ii, iværksætte kontrolprocedurer med henblik på at undersøge, om de lever op til de erklæringer og løfter, de har afgivet med hensyn til deres databeskyttelsesforanstaltninger, og punkt a, nr. iii, forpligte sig til at afhjælpe eventuelle problemer, som skyldes, at de ikke overholder principperne, samt til at overholde sanktioner for disse organisationer. En organisation kan opfylde punkt a, nr. i og iii, i princippet om klageadgang, håndhævelse og ansvar, hvis den opfylder følgende krav med hensyn til samarbejde med databeskyttelsesmyndighederne.
- b. En organisation forpligter sig til at samarbejde med databeskyttelsesmyndighederne ved i sin selvcertificeringsanmeldelse om tilslutning til EU-USA-databeskyttelsesrammen til ministeriet (se supplerende princip om selvcertificering) at erklære, at organisationen agter:
 - i. at overholde kravene i punkt a, nr. i og iii, i princippet om klageadgang, håndhævelse og ansvar ved at forpligte sig til at samarbejde med databeskyttelsesmyndighederne
 - ii. at samarbejde med databeskyttelsesmyndighederne med henblik på at undersøge og afgøre eventuelle klager, der modtages i henhold til principperne, og
 - iii. at rette sig efter enhver anbefaling fra databeskyttelsesmyndighederne, når de vurderer, at organisationen skal træffe specifikke foranstaltninger for at overholde principperne, herunder foretage udbedrende foranstaltninger eller betale skadeserstatning til de personer, der er berørt af den manglende overholdelse af disse principper, og at give databeskyttelsesmyndigheden en skriftlig bekræftelse på, at disse foranstaltninger er truffet.
- c. Paneler af databeskyttelsesmyndigheder
 - i. Samarbejdet med databeskyttelsesmyndighederne vil være baseret på disse myndigheders formidling af information og anbefalinger:
 1. Databeskyttelsesmyndighedernes anbefalinger vil blive formidlet gennem et uformelt panel af databeskyttelsesmyndigheder på EU-niveau, som bl.a. vil bidrage til at sikre en ensartet og sammenhængende fremgangsmåde på området.
 2. Panelet vil give de berørte amerikanske organisationer anbefalinger om endnu ikke afgjorte klager fra registrerede over behandlingen af personoplysninger, der er blevet overført fra EU under EU-USA-databeskyttelsesrammen. Disse anbefalinger vil blive udformet med henblik på at sikre en korrekt anvendelse af principperne og skal indeholde oplysninger om de retsmidler, som den eller de registrerede kan gøre brug af, og som databeskyttelsesmyndighederne finder passende.

3. Panelet vil fremsætte anbefalinger, når det får henvist en sag fra en organisation, og/eller når det modtager en klage direkte fra registrerede over organisationer, der har forpligtet sig til at samarbejde med databeskyttelsesmyndighederne inden for rammerne af EU-USA-databeskyttelsesrammen, og panelet vil opfordre de registrerede til og om nødvendigt hjælpe dem med i første omgang at anvende eventuelle interne klagemuligheder, som den pågældende organisation tilbyder.
 4. Anbefalingerne vil først blive afgivet, når begge parter i sagen har haft passende mulighed for at fremsætte bemærkninger og fremlægge enhver dokumentation, som de finder relevant. Panelet vil bestræbe sig på at afgive sine anbefalinger så hurtigt som muligt under hensyntagen til dette krav om behørig behandling. Panelet vil have som generel målsætning at afgive sine anbefalinger senest 60 dage efter modtagelsen af en klage eller en henvisning, og om muligt hurtigere.
 5. Panelet vil, såfremt det finder det formålstjenligt, offentliggøre resultaterne af sin behandling af klager.
 6. Panelet eller de enkelte databeskyttelsesmyndigheder kan ikke drages til ansvar for panelets anbefalinger.
- ii. Som beskrevet ovenfor skal en organisation, der vælger denne mulighed for bilæggelse af tvister, forpligte sig til at rette sig efter databeskyttelsesmyndighedernes anbefalinger. Hvis en organisation ikke har rettet sig efter en anbefaling senest 25 dage efter anbefalingens afgivelse og ikke har givet nogen tilfredsstillende forklaring på denne forsinkelse, vil panelet meddele, at det agter at indbringe sagen for FTC, transportministeriet eller et andet amerikansk organ med lovbestemte håndhævelsesbeføjelser i sager om illoyal eller vildledende praksis, eller at det vurderer, at der er sket en væsentlig overtrædelse af samarbejdsaftalen, der således skal betragtes som ugyldig. Panelet vil i sidstnævnte tilfælde underrette ministeriet med henblik på at få ændret listen over deltagere i databeskyttelsesrammen. Enhver misligholdelse af forpligtelsen til at samarbejde med databeskyttelsesmyndighederne og enhver overtrædelse af principperne vil kunne retsforfølges som vildledende praksis i henhold til Section 5 i Federal Trade Commission Act (15 U.S.C. § 45), 49 U.S.C. § 41712 eller en anden tilsvarende lov.
- d. En organisation, der deltager i EU-USA-databeskyttelsesrammen og ønsker, at oplysninger om menneskelige ressourcer, der overføres fra EU inden for rammerne af et ansættelsesforhold, skal være omfattet af principperne i EU-USA-databeskyttelsesrammen, skal forpligte sig til at samarbejde med databeskyttelsesmyndighederne om sådanne oplysninger (jf. det supplerende princip om oplysninger om menneskelige ressourcer).
 - e. Organisationer, der vælger denne løsning, vil blive anmodet om at betale et årligt gebyr til dækning af panelets driftsomkostninger. Derudover kan de blive anmodet om at dække eventuelle udgifter til oversættelse, som opstår som følge af panelets behandling af henviste sager eller klager. Gebyret fastsættes af ministeriet efter høring af Kommissionen. Gebyret kan opkræves af en tredjepart, der af ministeriet udvælges til at fungere som depotinstitution for de midler, der indsamles til dette formål. Ministeriet vil arbejde tæt sammen med Kommissionen og databeskyttelsesmyndighederne om at fastlægge passende procedurer for fordelingen af de midler, der indsamles gennem gebyret, samt om andre proceduremæssige og administrative aspekter vedrørende panelet. Ministeriet og Kommissionen kan indgå en aftale om at ændre den hyppighed, hvormed gebyret opkræves.

6. Selvcertificering

- a. Organisationen drager fordel af EU-USA-databeskyttelsesrammen fra den dato, hvor ministeriet opfører organisationen på listen over deltagere i databeskyttelsesrammen. Ministeriet vil først opføre en organisation på listen over deltagere i databeskyttelsesrammen, når det har fastslået, at organisationens indledende anmeldelse om selvcertificering er fuldstændig, og det vil fjerne organisationen fra listen, hvis den frivilligt trækker sig, ikke indsender den årlige anmeldelse om recertificering eller vedvarende overtræder principperne (jf. det supplerende princip om bilæggelse af tvister og håndhævelse).
- b. Når en organisation gennemfører den indledende selvcertificering og efterfølgende gennemfører recertificeringer om tilslutning til EU-USA-databeskyttelsesrammen, skal den fremsende en anmeldelse til ministeriet underskrevet af en ledende medarbejder på vegne af den organisation, der foretager selvcertificeringen eller recertificeringen om tilslutning til principperne ^(*). Anmeldelsen skal som minimum indeholde følgende oplysninger:

^(*) Anmeldelsen skal foretages via ministeriets websted for databeskyttelse af en person i organisationen, som er bemyndiget til at fremsætte erklæringer på vegne af organisationen og dens dækkede enheder vedrørende tilslutningen til principperne.

- i. navnet på den selvcertificerende eller recertificerende amerikanske organisation samt navnet/navnene på dets amerikanske enheder eller amerikanske datterselskaber, der også tilslutter sig principperne, og som organisationen ønsker at få dækket
 - ii. en beskrivelse af organisationens aktiviteter i relation til personoplysninger modtaget fra EU i henhold til EU-USA-databeskyttelsesrammen
 - iii. en beskrivelse af organisationens politik(ker) til beskyttelse af privatlivets fred med hensyn til disse personoplysninger, herunder:
 1. webadressen på det sted, hvor politikken til beskyttelse af privatlivets fred er tilgængelig, hvis organisationen har et offentligt websted, eller hvis organisationen ikke har et offentligt websted, adressen på det sted, hvor offentligheden kan få adgang til politikken til beskyttelse af privatlivets fred, og
 2. datoen for iværksættelse af denne politik
 - iv. en kontaktadresse for behandlingen af eventuelle klager, anmodninger om indsigt og andre anliggender i forbindelse med principperne ⁽⁹⁾, herunder:
 1. navn(e), stillingsbetegnelse(r), e-mailadresse(r) og telefonnummer(-numre) på den eller de relevante personer eller relevante kontaktadresser i organisationen og
 2. organisationens relevante amerikanske postadresse
 - v. det specifikke lovbestemte organ, der har kompetence til at behandle klager over organisationen vedrørende mulig illoyal eller vildledende praksis eller overtrædelser af gældende love eller bestemmelser om beskyttelse af privatlivets fred (og som er anført i principperne eller i et fremtidigt bilag til principperne)
 - vi. betegnelsen på ethvert program til beskyttelse af privatlivets fred, som organisationen deltager i
 - vii. den pågældende kontrolmetode (f.eks. selvevaluering eller ekstern kontrol af overholdelsen, herunder den tredjemand, der udfører denne kontrol) ⁽¹⁰⁾ og
 - viii. den eller de uafhængige klageinstans(er), der kan behandle uløste principrelaterede sager ⁽¹¹⁾.
- c. Hvis en organisation ønsker, at fordelene ved EU-USA-databeskyttelsesrammen også skal dække oplysninger om menneskelige ressourcer, der overføres fra EU til brug inden for rammerne af et ansættelsesforhold, kan den foretage sådanne overførsler, hvis der findes et lovbestemt organ, der har kompetence til at behandle klager over den pågældende organisation vedrørende oplysninger om menneskelige ressourcer, og som er anført i principperne eller i et fremtidigt bilag til principperne. Desuden skal organisationen anføre dette i sin indledende anmeldelse om selvcertificering og i alle anmeldelser om recertificering og angive, at den forpligter sig til at samarbejde med den eller de pågældende EU-myndigheder i overensstemmelse med de supplerende principper om oplysninger om menneskelige ressourcer og databeskyttelsesmyndighedernes rolle, og at den agter at følge disse myndigheders anbefalinger. Organisationens skal også fremsende en kopi af sin politik til beskyttelse af oplysninger om menneskelige ressourcer til ministeriet og oplyse, hvor de berørte medarbejdere kan få adgang til politikken til beskyttelse af privatlivets fred.

⁽⁹⁾ "Organisationens primære kontaktperson" eller "organisationens ledende medarbejder" kan ikke være en person uden for organisationen (f.eks. ekstern rådgiver eller ekstern konsulent).

⁽¹⁰⁾ Jf. det supplerende princip om kontrol (verifikation).

⁽¹¹⁾ Jf. det supplerende princip om bilægelse af tvister og håndhævelse.

- d. Ministeriet vil oprette listen over organisationer, der deltager i databeskyttelsesrammen, og som har fremsendt fuldstændige indledende anmeldelser om selvcertificering, og ministeriet vil offentliggøre listen og ajourføre den på grundlag af de fuldstændige årlige anmeldelser om recertificering og meddelelser, der modtages i overensstemmelse med det supplerende princip om bilæggelse af tvister og håndhævelse. Sådanne recertificeringsanmeldelser skal fremsendes mindst én gang om året. I modsat fald vil organisationen blive slettet fra listen over deltagere i databeskyttelsesrammen, og den kan ikke længere drage fordel af EU-USA-databeskyttelsesrammen. Alle organisationer, som ministeriet opfører på listen over deltagere i databeskyttelsesrammen, skal have relevante politikker til beskyttelse af privatlivets fred, som er i overensstemmelse med princippet om oplysningspligt, og i disse politikker angive, at de tilslutter sig principperne ⁽¹²⁾. Hvis en organisations politik til beskyttelse af privatlivets fred er tilgængelig online, skal den derudover indeholde et hyperlink til ministeriets websted for databeskyttelsesrammen samt et hyperlink til webstedet eller klageformularen for den uafhængige klageinstans, der gratis kan behandle fysiske personers uløste, principrelaterede klager.
- e. Principperne finder anvendelse straks efter selvcertificering. Deltagende organisationer, der tidligere har foretaget selvcertificering om tilslutning til principperne i EU-USA-privatlivsskjoldet, vil skulle ajourføre deres politikker til beskyttelse af privatlivets fred, så der i stedet henvises til "principperne i EU-USA-databeskyttelsesrammen". Sådanne organisationer skal indsatte denne henvisning hurtigst muligt og under alle omstændigheder senest tre måneder efter ikrafttrædelsesdatoen for principperne i EU-USA-databeskyttelsesrammen.
- f. En organisation skal anvende principperne på alle personoplysninger modtaget fra EU under EU-USA-databeskyttelsesrammen. Tilslutningen til principperne er ikke tidsbegrænset med hensyn til de personoplysninger, der modtages i den periode, hvor organisationen drager fordel af EU-USA-databeskyttelsesrammen. Hvis en organisation først har tilsluttet sig principperne, skal den fortsat anvende dem på sådanne oplysninger, så længe den lagrer, anvender eller videregiver oplysningerne, også selv om den af en hvilken som helst grund efterfølgende forlader EU-USA-databeskyttelsesrammen. En organisation, som ønsker at trække sig ud af EU-USA-databeskyttelsesrammen, skal meddele ministeriet dette på forhånd. Denne meddelelse skal også angive, hvad organisationen agter at gøre med de personoplysninger, den har modtaget i henhold til EU-USA-databeskyttelsesrammen (dvs. om den agter at beholde, tilbagesende eller slette oplysningerne, og, hvis den ønsker at beholde oplysningerne, de godkendte måder, hvorpå den vil beskytte oplysningerne). En organisation, som ønsker at træde ud af EU-USA-databeskyttelsesrammen, men ønsker at beholde oplysningerne, skal enten hvert år bekræfte over for ministeriet, at den fortsat vil anvende principperne på oplysningerne, eller sikre en "tilstrækkelig" beskyttelse af oplysningerne på en anden godkendt måde (f.eks. ved hjælp af en aftale, der fuldt ud afspejler kravene i de relevante standardkontraktbestemmelser, som Kommissionen har vedtaget). I modsat fald skal organisationen tilbagesende eller slette oplysningerne ⁽¹³⁾. En organisation, der træder ud af EU-USA-databeskyttelsesrammen, skal fjerne alle henvisninger til EU-USA-databeskyttelsesrammen i relevante politikker til beskyttelse af privatlivets fred, der lader formode, at organisationen fortsat deltager i EU-USA-databeskyttelsesrammen og er berettiget til at drage fordel heraf.

⁽¹²⁾ En organisation, der foretager selvcertificering for første gang, må ikke hævde, at den deltager i EU-USA-databeskyttelsesrammen, i sin endelige politik til beskyttelse af privatlivets fred, før ministeriet har underrettet organisationen om, at den må gøre det. Organisationen skal forelægge ministeriet et udkast til en politik til beskyttelse af privatlivets fred, som er i overensstemmelse med principperne, når den foretager sin indledende anmeldelse om selvcertificering. Når ministeriet har fastslået, at organisationens indledende anmeldelse om selvcertificering ellers er fuldstændig, underretter ministeriet organisationen om, at den skal færdiggøre (f. eks. i påkommende tilfælde offentliggøre) sin politik til beskyttelse af privatlivets fred, der er i overensstemmelse med EU-USA-databeskyttelsesrammen. Organisationen skal straks underrette ministeriet, når den relevante politik til beskyttelse af privatlivets fred er færdiggjort, hvorefter ministeriet opfører organisationen på listen over deltagere i databeskyttelsesrammen.

⁽¹³⁾ Hvis en organisation på tidspunktet for sin udtrædelse vælger at beholde de personoplysninger, den har modtaget i henhold til EU-USA-databeskyttelsesrammen, og hvert år bekræfte over for ministeriet, at den fortsat vil anvende principperne på disse oplysninger, skal organisationen en gang om året efter udtrædelsen over for ministeriet godtgøre (dvs. medmindre og indtil organisationen sikrer en "tilstrækkelig" beskyttelse af sådanne oplysninger på en anden godkendt måde eller tilbagesender eller sletter alle sådanne oplysninger og underretter ministeriet herom), hvad den har gjort med disse personoplysninger, hvad den vil gøre med de personoplysninger, som den fortsat beholder, og hvem der vil fungere som fast kontaktpunkt for principrelaterede spørgsmål.

- g. En organisation, der som følge af virksomhedsomlægninger i form af f.eks. fusion, overtagelse, konkurs eller opløsning ophører med at eksistere som særskilt retlig enhed, skal på forhånd underrette ministeriet herom. Organisationen skal i denne meddelelse ligeledes angive, om den enhed, der opstår som følge af virksomhedsomlægningen, i) fortsat vil deltage i EU-USA-databeskyttelsesrammen i kraft af en eksisterende selvcertificering, ii) vælger at foretage selvcertificering som en ny deltager i EU-USA-databeskyttelsesrammen (f.eks. når den nye enhed eller den overlevende enhed ikke allerede har en eksisterende selvcertificering, der giver den mulighed for at deltage i EU-USA-databeskyttelsesrammen), eller iii) iværksætter andre sikkerhedsforanstaltninger, herunder skriftlige aftaler, der sikrer fortsat anvendelse af principperne på alle personoplysninger, som organisationen har modtaget i henhold til EU-USA-databeskyttelsesrammen, og som organisationen beholder. Hvis hverken i), ii) eller iii) finder anvendelse, skal alle personoplysninger, som organisationen har modtaget under EU-USA-databeskyttelsesrammen, straks tilbagesendes eller slettes.
- h. Når en organisation forlader EU-USA-databeskyttelsesrammen af en eller anden årsag, skal den fjerne alle erklæringer, der lader formode, at organisationen fortsat deltager i EU-USA-databeskyttelsesrammen eller er berettiget til at drage fordel af EU-USA-databeskyttelsesrammen. Hvis certificeringsmarkedet for EU-USA-databeskyttelsesrammen anvendes, skal det ligeledes fjernes. En organisation, der afgiver urigtige oplysninger til offentligheden vedrørende dens tilslutning til principperne, kan indbringes for FTC, transportministeriet eller andre kompetente statslige organer. En organisation, der afgiver urigtige oplysninger til ministeriet, kan retsforfølges efter False Statements Act (18 U.S.C. § 1001).

7. Kontrol (verifikation)

- a. Organisationer skal iværksætte kontrolprocedurer med henblik på at undersøge, om de lever op til de erklæringer og løfter, de har afgivet om deres databeskyttelsesforanstaltninger inden for EU-USA-databeskyttelsesrammen, og om disse foranstaltninger er blevet iværksat som beskrevet i og i overensstemmelse med principperne.
- b. For at opfylde kontrolkravene i princippet om klageadgang, håndhævelse og ansvar skal en organisation kontrollere sådanne erklæringer og løfter ved hjælp af selvevaluering eller ekstern kontrol af overholdelsen.
- c. Hvis organisationen har valgt selvevaluering, skal det kontrolleres, om organisationens politik til beskyttelse af privatlivets fred vedrørende personoplysninger, der modtages fra EU, er i overensstemmelse med de faktiske forhold, og om den er dækkende, let tilgængelig, i overensstemmelse med principperne og fuldstændig iværksat (dvs. at den overholdes). Det skal ligeledes fremgå af denne kontrol, om de registrerede er informeret om eventuelle interne muligheder for klagebehandling og om de eksterne uafhængige klageinstanser, som de har adgang til, om den pågældende organisation har udarbejdet procedurer for uddannelse af de ansatte i gennemførelsen af disse foranstaltninger og for håndtering af deres manglende overholdelse af foranstaltningerne, samt om organisationen har interne procedurer for regelmæssig og objektiv kontrol af ovenstående. Mindst én gang om året skal en ledende medarbejder eller en anden bemyndiget repræsentant for organisationen underskrive en erklæring om selvevaluering, og der skal gives adgang til denne erklæring på den registreredes anmodning eller i forbindelse med en undersøgelse eller en klage over manglende overholdelse.
- d. Hvis organisationen har valgt ekstern kontrol af overholdelsen, skal denne kontrol påvise, at organisationens politik til beskyttelse af privatlivets fred vedrørende personoplysninger, der modtages fra EU, er i overensstemmelse med de faktiske forhold, og om den er dækkende, let tilgængelig, i overensstemmelse med principperne og fuldstændig iværksat (dvs. at den overholdes). Det skal ligeledes fremgå af denne kontrol, om de registrerede er informeret om klageinstanser, som de har adgang til. Kontrolmetoderne kan uden begrænsning omfatte revision, uvarslet kontrol, anvendelse af fiktive oplysninger ("decoys") eller passende teknologiske midler. Mindst én gang om året skal kontrollanten, en ledende medarbejder eller en anden bemyndiget repræsentant for organisationen underskrive en erklæring om, at der er foretaget en ekstern kontrol af overholdelsen, og der skal gives adgang til denne erklæring på den registreredes anmodning eller i forbindelse med en undersøgelse eller en klage over manglende overholdelse.
- e. Organisationer skal føre protokol over iværksættelsen af deres databeskyttelsesforanstaltninger inden for EU-USA-databeskyttelsesrammen og gøre denne protokol tilgængelig efter anmodning derom i forbindelse med en undersøgelse eller en klage over manglende overholdelse til det uafhængige organ, som har ansvaret for at undersøge klager, eller til den myndighed, der har kompetence i sager om illoyal eller vildledende praksis. Organisationerne skal ligeledes straks besvare forespørgsler og andre anmodninger fra ministeriet om oplysninger om organisationens tilslutning til principperne.

8. Indsigt

a. Princippet om indsigt i praksis

- i. I henhold til principperne er retten til indsigt af afgørende betydning for beskyttelsen af privatlivets fred, især fordi den giver den enkelte mulighed for at kontrollere nøjagtigheden af sine personoplysninger. Princippet om indsigt indebærer, at registrerede har ret til at:
 1. få oplyst, om en organisation behandler personoplysninger om dem ⁽¹⁴⁾
 2. få udleveret oplysningerne, således at de kan kontrollere nøjagtigheden heraf og behandlingens lovlighed
 3. få oplysningerne rettet, ændret eller slettet, hvis de er ukorrekte eller behandles i strid med principperne.
- ii. Registrerede skal ikke begrunde en anmodning om indsigt i egne personoplysninger. Organisationer, der modtager en anmodning om indsigt fra registrerede, bør først og fremmest koncentrere sig om det, som i første omgang har ført til anmodningen. Hvis en anmodning om indsigt er for vag eller for bredt defineret, kan organisationen f.eks. indgå i en dialog med den pågældende for bedre at kunne forstå motiverne bag anmodningen og give de relevante oplysninger. Organisationen kan anmode om at få oplyst, hvilke(n) del(e) af organisationen den pågældende har haft med at gøre, eller hvilken slags oplysninger eller anvendelse der er genstand for anmodningen om indsigt.
- iii. Organisationer skal i overensstemmelse med selve princippet om indsigt altid udvise imødekommenhed i deres bestræbelser på at give indsigt. Hvis visse oplysninger f.eks. skal beskyttes og nemt kan adskilles fra andre personoplysninger, hvori der anmodes om indsigt, skal organisationen bortredigere de beskyttede oplysninger og give indsigt i de andre oplysninger. Hvis en organisation beslutter at begrænse indsigten i personoplysninger i særlige tilfælde, skal den redegøre for sin beslutning over for den person, der har anmodet om indsigt, og oplyse, hvor den pågældende kan henvende sig for yderligere oplysninger.

b. Meromkostningerne eller meradministrationen ved at give indsigt

- i. Retten til indsigt i personoplysninger kan begrænses under særlige omstændigheder, hvor det ville medføre en krænkelse af andre personers legitime rettigheder, eller hvor meradministrationen eller meromkostningerne ved at give indsigt i disse oplysninger ville være uforholdsmæssig store i forhold til risikoen for de pågældende personers privatliv i det pågældende tilfælde. Meromkostninger og meradministration er vigtige faktorer, der bør tages i betragtning, men de er ikke afgørende for vurderingen af, om det er rimeligt at give indsigt.
- ii. Hvis personoplysningerne f.eks. danner grundlag for beslutninger, der har afgørende betydning for den enkelte (f.eks. afgørelser i økonomiske anliggender, herunder vedrørende forsikringer, lån eller ansættelse), skal organisationen i overensstemmelse med de øvrige bestemmelser i disse supplerende principper give indsigt i de pågældende oplysninger, selv om det giver anledning til uforholdsmæssig meradministration eller uforholdsmæssigt store meromkostninger. Hvis de personoplysninger, der anmodes om, hverken er følsomme oplysninger eller danner grundlag for beslutninger, der har afgørende betydning for den enkelte, men er let tilgængelige og med få omkostninger kan stilles til rådighed, skal en organisation give indsigt i disse oplysninger.

c. Fortrolige forretningsoplysninger

- i. Fortrolige forretningsoplysninger er oplysninger, som en organisation har truffet foranstaltninger for at beskytte imod videregivelse, fordi en sådan videregivelse ville være til fordel for en konkurrent på markedet. Organisationer kan nægte at give indsigt eller give begrænset indsigt, hvis de ved at give fuld indsigt risikerer at afsløre deres egne fortrolige forretningsoplysninger, f.eks. markedsføringsparametre eller -klassifikationer, som organisationen har udarbejdet, eller andres fortrolige forretningsoplysninger, når disse oplysninger i henhold til en aftale skal behandles fortroligt.

⁽¹⁴⁾ Organisationen skal besvare anmodninger fra registrerede om, hvad formålene med behandlingen er, hvilke kategorier af personoplysninger der er tale om, og hvilke modtagere eller kategorier af modtagere personoplysningerne videregives til.

- ii. Hvis fortrolige forretningsoplysninger nemt kan adskilles fra andre oplysninger, hvori der anmodes om indsigt, skal organisationen bortredigere de fortrolige forretningsoplysninger og give indsigt i de ikkefortrolige oplysninger.

d. Organisering af databaser

- i. En organisation kan give indsigt ved at videregive de relevante personoplysninger til de pågældende personer, som således ikke skal have adgang til organisationens database.
- ii. Der skal kun gives indsigt i det omfang, en organisation lagrer personoplysningerne. Princippet om indsigt forpligter ikke i sig selv en organisation til at opbevare, vedligeholde, organisere eller omstrukturere registre med personoplysninger.

e. Begrænset indsigt

- i. Da organisationer altid skal udvise imødekommenhed i deres bestræbelser på at give registrerede indsigt i deres personoplysninger, kan de kun begrænse denne indsigt i begrænsede tilfælde, og enhver begrundelse for at begrænse indsigten skal tage udgangspunkt i specifikke forhold. Som under databeskyttelsesforordningen kan en organisation give begrænset indsigt i oplysninger, hvis en videregivelse kan antages at vanskeliggøre beskyttelsen af vigtige altovervejende offentlige interesser, herunder den nationale sikkerhed, forsvaret eller den offentlige sikkerhed. Det er desuden muligt at nægte indsigt, når personoplysningerne udelukkende behandles med henblik på forskning eller i statistisk øjemed. Der kan f.eks. også nægtes indsigt eller gives begrænset indsigt, når denne indsigt:
 - 1. griber ind i lovens gennemførelse eller håndhævelse eller private søgsmål, herunder forebyggelse, efterforskning, afsløring af lovovertrædelser eller retten til en retfærdig rettergang
 - 2. medfører krænkelse af andre personers legitime rettigheder eller interesser
 - 3. er et brud på retten eller forpligtelsen til fortrolighed mellem advokat og klient
 - 4. vanskeliggør sikkerhedsundersøgelser eller behandlingen af personalesager eller i forbindelse med personaleplanlægning og -omstrukturering eller
 - 5. vanskeliggør den nødvendige fortrolige behandling af oplysninger i forbindelse med overvågning, kontrol eller regulering inden for rammerne af god forvaltning eller under kommende eller igangværende forhandlinger, som organisationen er involveret i.
- ii. En organisation, der påberåber sig en undtagelse, skal dokumentere nødvendigheden af denne undtagelse, og registrerede skal oplyses om begrundelsen for begrænsningen af indsigten og om, hvor de kan henvende sig for yderligere oplysninger.

f. Retten til at modtage bekræftelse og opkrævning af et gebyr til dækning af omkostningerne til indsigt

- i. En registreret har ret til at få oplyst, om en organisation behandler personoplysninger om den pågældende. En registreret har ret til at få udleveret sine personoplysninger. En organisation kan opkræve et gebyr, der ikke er uforholdsmæssigt stort.
- ii. Det kan være berettiget at opkræve et gebyr, f.eks. hvis anmodninger om indsigt er tydeligt overdrevne, navnlig fordi de gentages.
- iii. Der må ikke nægtes indsigt under henvisning til omkostningerne, hvis den registrerede tilbyder at afholde disse selv.

g. Gentagne eller chikanerende anmodninger om indsigt

- i. Organisationer kan fastsætte en passende maksimumsgrænse for det antal gange, anmodninger om indsigt fra en bestemt person inden for en bestemt periode vil blive behandlet. Organisationer skal ved fastsættelsen af disse kriterier tage højde for, hvor hyppigt oplysningerne ajourføres, til hvilket formål de anvendes, og hvilken slags oplysninger det drejer sig om.

h. Svigagtige anmodninger om indsigt

- i. Organisationer er ikke forpligtet til at give indsigt, medmindre de fra rekvirenten modtager tilstrækkelige oplysninger til at kontrollere vedkommendes identitet.

i. Svarfrist

- i. Organisationer bør besvare anmodninger om indsigt inden for en rimelig frist og på en rimelig måde, som er let forståelig for den registrerede. En organisation, der regelmæssigt udleverer oplysninger til registrerede, kan besvare en individuel anmodning om indsigt i forbindelse med organisationens regelmæssige fremsendelse af oplysninger, hvis det ikke medfører en for stor forsinkelse.

9. **Oplysninger om menneskelige ressourcer**

a. Anvendelsesområdet for EU-USA-databeskyttelsesrammen

- i. Når en organisation i EU overfører personoplysninger om sine (forhenværende eller nuværende) ansatte, der er indsamlet inden for rammerne af ansættelsesforholdet, til en tjenesteudbyder i USA, det være sig et moderselskab, en associeret organisation eller en ikkeassocieret organisation, som deltager i EU-USA-databeskyttelsesrammen, er overførslen underlagt denne databeskyttelsesramme. I disse tilfælde finder både indsamlingen og behandlingen af oplysninger forud for overførslen typisk sted i overensstemmelse med national ret i den EU-medlemsstat, hvor oplysningerne er indsamlet, og enhver betingelse eller begrænsning for overførsel i henhold til denne lovgivning skal overholdes.
- ii. Principperne finder kun anvendelse ved overførsel af eller indsigt i individuelt identificerede eller identificerbare personoplysninger. Statistisk materiale, der bygger på en sammenføring af ansættelsesoplysninger, og som ikke indeholder personoplysninger eller data, der registreres anonymt, er ikke omfattet af beskyttelsen af privatlivets fred.

b. Anvendelse af principperne om oplysningspligt og valgfrihed

- i. En amerikansk organisation, der inden for EU-USA-databeskyttelsesrammen har modtaget ansættelsesoplysninger fra EU, må kun videregive disse oplysninger til tredjemand eller anvende dem til andre formål, såfremt det sker i overensstemmelse med principperne om oplysningspligt og valgfrihed. Når en amerikansk organisation f.eks. agter at anvende personoplysninger, der er indsamlet i forbindelse med et ansættelsesforhold, til ikkeansættelsesrelaterede formål, f.eks. til markedsføringshenvendelser, skal den først give de berørte personer den nødvendige valgfrihed, medmindre de allerede har tilladt anvendelsen af oplysningerne til sådanne formål. Denne anvendelse må ikke være uforenelig med de formål, hvortil personoplysningerne er indsamlet eller efterfølgende godkendt af den enkelte person. De ansattes valg må desuden ikke give anledning til forskelsbehandling eller sanktioner mod de pågældende ansatte.
- ii. Det skal bemærkes, at visse bestemmelser, der generelt finder anvendelse på overførsel af personoplysninger fra visse EU-medlemsstater, kan forhindre andre anvendelser af disse oplysninger, selv efter overførsel til et land uden for EU, og sådanne bestemmelser skal overholdes.
- iii. Arbejdsgiverne skal endvidere bestræbe sig på så vidt muligt at respektere de ansattes ønsker om hemmeligholdelse af personoplysninger. Det kan bl.a. omfatte, at der kun gives begrænset indsigt i personoplysninger, at visse oplysninger gøres anonyme, eller at der anvendes koder eller pseudonymer, når de rigtige navne ikke er nødvendige for de pågældende formål.
- iv. En organisation er ikke forpligtet til at anvende principperne om oplysningspligt eller valgfrihed i det omfang og i den periode, det er nødvendigt for ikke at skade den pågældende organisations muligheder for at foretage fremsendelser eller udnævnelser eller behandle andre personaleanliggender af lignende karakter.

c. Anvendelse af princippet om indsigt

- i. Begrundelserne for at nægte at give indsigt eller for at give begrænset indsigt i oplysninger om menneskelige ressourcer efter anmodning derom fremgår af det supplerende princip om indsigt. Arbejdsgivere i EU skal naturligvis overholde de nationale regler på området og sikre, at arbejdstagere i EU gives indsigt i sådanne oplysninger, således som det er påbudt af loven i deres hjemland, uanset i hvilket land oplysningerne behandles og lagres. En organisation, der behandler denne type oplysninger i USA, er i henhold til EU-USA-databeskyttelsesrammen forpligtet til at samarbejde med henblik på at give indsigt enten direkte eller gennem arbejdsgiveren i EU.

d. Håndhævelse

- i. I det omfang personoplysninger udelukkende anvendes inden for rammerne af et ansættelsesforhold, er organisationen i EU hovedansvarlig for oplysningerne over for den enkelte ansatte. Hvis europæiske arbejdstagere klager over krænkelse af deres ret til databeskyttelse og ikke er tilfredse med resultaterne af de forskellige interne kontrol-, klage- eller appelprocedurer (eller enhver anden klageprocedure inden for rammerne af en kontrakt med en fagforening), skal de henvises til de kompetente nationale databeskyttelses- eller arbejdsmarkedsmyndigheder i den jurisdiktion, de arbejder i. Dette gælder også i sager, hvor ansvaret for den formodede forkerte behandling af deres personoplysninger påhviler den amerikanske organisation, der har modtaget oplysningerne fra arbejdsgiveren, og således medfører et formodet brud på principperne. Dette vil være den mest effektive fremgangsmåde for at behandle de ofte overlappende rettigheder og pligter, som er fastsat i arbejdsretten og arbejdsoverenskomster samt i databeskyttelseslovgivningen.
- ii. En amerikansk organisation, der deltager i EU-USA-databeskyttelsesrammen og anvender EU-oplysninger om menneskelige ressourcer, der er overført fra EU inden for rammerne af et ansættelsesforhold, og som ønsker, at disse overførsler skal være omfattet af principperne i EU-USA-databeskyttelsesrammen, skal således forpligte sig til at samarbejde i undersøgelser, der foretages af de kompetente EU-myndigheder i disse sager, og til at rette sig efter deres anbefalinger.

e. Anvendelse af princippet om ansvar for videreoverførsel

- i. I forbindelse med lejlighedsvis ansættelsesrelaterede operationelle behov i den deltagende organisation for at overføre personoplysninger under EU-USA-databeskyttelsesrammen, f.eks. i forbindelse med booking af et fly, hotelværelse eller forsikringsdækning, kan overførsler af personoplysninger om et lille antal medarbejdere til dataansvarlige ske uden at anvende princippet om indsigt eller indgå en aftale med den dataansvarlige tredjemand, hvilket ellers er et krav i henhold til princippet om ansvar for videreoverførsel, forudsat at den deltagende organisation har overholdt principperne om oplysningspligt og valgfrihed.

10. Obligatoriske aftaler om videreoverførsel

a. Aftaler om behandling af oplysninger

- i. Uanset databehandlerens deltagelse i EU-USA-databeskyttelsesrammen skal der indgås en aftale, når personoplysninger overføres fra EU til USA udelukkende med henblik på behandling.
- ii. Dataansvarlige i EU skal altid indgå en aftale, selv når oplysninger kun overføres med henblik på behandling, og dette uanset om denne behandling foregår i eller uden for EU, og uanset om databehandleren deltager i EU-USA-databeskyttelsesrammen eller ej. Formålet med aftalen er at sikre, at databehandleren:
 1. kun handler efter instruks fra den dataansvarlige,
 2. iværksætter de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikkeautoriseret adgang og ved, om videreoverførsel er tilladt, og
 3. tager hensyn til behandlingens karakter og bistår den dataansvarlige med at besvare anmodninger fra registrerede, der udøver deres rettigheder under principperne.

- iii. Da de deltagende organisationer anses for at give en tilstrækkelig beskyttelse, kræver aftaler med sådanne organisationer, der udelukkende vedrører behandling af oplysninger, ingen forudgående tilladelse.
- b. Overførsler i en kontrolleret gruppe af selskaber eller enheder
 - i. Når personoplysninger overføres mellem to dataansvarlige i en kontrolleret gruppe af selskaber eller enheder, er det ikke altid nødvendigt at indgå en aftale i henhold til princippet om ansvar for videreoverførsel. Dataansvarlige i en kontrolleret gruppe af selskaber eller enheder kan basere disse overførsler på andre instrumenter såsom EU's bindende virksomhedsregler eller andre koncerninterne instrumenter (f.eks. overholdelses- og kontrolprogrammer), der sikrer kontinuitet i beskyttelsen af personoplysninger i henhold til principperne. I forbindelse med disse overførsler har den deltagende organisation fortsat ansvaret for, at principperne overholdes.
- c. Overførsler mellem dataansvarlige
 - i. I forbindelse med overførsler mellem dataansvarlige behøver den modtagende dataansvarlige ikke være en deltagende organisation eller have en uafhængig klageinstans. Den deltagende organisation skal indgå en aftale med den modtagende dataansvarlige tredjemand, der sikrer samme beskyttelsesniveau som under EU-USA-databeskyttelsesrammen, men den dataansvarlige tredjemand behøver ikke være en deltagende organisation eller have en uafhængig klageinstans, forudsat at tredjemanden stiller en tilsvarende mekanisme til rådighed.

11. Bilæggelse af tvister og håndhævelse

- a. Kravene til håndhævelse af EU-USA-databeskyttelsesrammen fastsættes i princippet om klageadgang, håndhævelse og ansvar. Det fastsættes i det supplerende princip om kontrol (verifikation), hvorledes kravene i princippets punkt a, nr. ii, skal overholdes. Dette supplerende princip omhandler punkt a, nr. i og iii, hvor der stilles krav om uafhængige klageinstanser. Databeskyttelsesrammen kan håndhæves ved hjælp af forskellige mekanismer, der dog alle skal opfylde kravene i princippet om klageadgang, håndhævelse og ansvar. En organisation kan opfylde kravene: i) ved at overholde programmer til beskyttelse af privatlivets fred udviklet i den private sektor og baseret på principperne, som omfatter effektive håndhævelsesmekanismer af den type, der er beskrevet i princippet om klageadgang, håndhævelse og ansvar, ii) ved at være underlagt tilsynsmyndigheder, der er oprettet ved lov eller administrativt, og som varetager behandlingen af individuelle klager og bilæggelsen af tvister, eller iii) ved at forpligte sig til at samarbejde med databeskyttelsesmyndighederne i EU eller deres bemyndigede repræsentanter.
- b. Denne liste er blot beskrivende og ikke udtømmende, eftersom der i den private sektor kan oprettes yderligere håndhævelsesmekanismer, når blot kravene i princippet om klageadgang, håndhævelse og ansvar og de supplerende principper overholdes. Bemærk, at kravene i princippet om klageadgang, håndhævelse og ansvar supplerer kravet om, at selvregulering skal kunne håndhæves efter Section 5 i Federal Trade Commission Act (15 U.S.C. § 45), der forbyder illoyal eller vildledende praksis, 49 U.S.C. § 41712, der forbyder transportører eller rejsebureauer at anvende en illoyal eller vildledende praksis i forbindelse med lufttransportydelser eller salg af lufttransportydelser, eller en anden tilsvarende lov.
- c. Organisationer og deres uafhængige klageinstanser skal tilvejebringe oplysninger om EU-USA-databeskyttelsesrammen, når ministeriet anmoder herom, for at medvirke til at sikre, at de opfylder deres forpligtelser under EU-USA-databeskyttelsesrammen, og for at lette forvaltningen af programmet. Organisationer skal desuden straks besvare klager over deres manglende overholdelse af principperne, som databeskyttelsesmyndighederne henviser via ministeriet. Svaret skal indeholde en vurdering af klagens berettigelse, og såfremt den er berettiget, oplysninger om, hvordan organisationen vil afhjælpe problemet. Ministeriet vil beskytte modtagne fortrolige oplysninger i overensstemmelse med amerikansk ret.

d. Klageinstanser

- i. Registrerede skal opfordres til først at klage til den pågældende organisation, inden de indbringer deres klage for uafhængige klageinstanser. Organisationerne skal svare de registrerede senest 45 dage efter modtagelse af klagen. En klageinstans er navnlig uafhængig, hvis den er upartisk, hvis der er åbenhed omkring sammensætningen og finansieringen, og hvis der foreligger dokumenteret erfaring. De klagemuligheder, som den enkelte har adgang til, skal i henhold til princippet om klageadgang, håndhævelse og ansvar være let tilgængelige og gratis. Uafhængige tvistbilæggesinstanser skal behandle hver enkelt klage, som de modtager fra registrerede, medmindre klagerne tydeligt er ubegrundede eller useriøse. Dette udelukker ikke, at klageinstansen kan fastsætte kriterier for modtagelse af klager, men sådanne kriterier skal være gennemskuelige og begrundede (og f.eks. have til formål at udelukke klager, der ikke er omfattet af programmet, eller som skal behandles i et andet forum), og de må ikke have som konsekvens at underminere forpligtelsen til at behandle legitime klager. Disse klageinstanser skal desuden ved modtagelsen af en klage give de registrerede fuldstændige og let tilgængelige oplysninger om, hvorledes tvistbilæggesproceduren fungerer. Disse oplysninger skal omfatte en meddelelse om klageinstansens databeskyttelsesforanstaltninger i overensstemmelse med principperne. Klageinstanserne skal desuden medvirke til at udvikle forskellige værktøjer, herunder standardklageformularer, der skal gøre det nemmere at behandle klager.
- ii. Uafhængige klageinstanser skal angive oplysninger om principperne og om de tjenester, de tilbyder under EU-USA-databeskyttelsesrammen, på deres offentlige websteder. Disse oplysninger skal omfatte: 1) oplysninger om eller et link til kravene vedrørende uafhængige klageinstanser i henhold til principperne, 2) et link til ministeriets websted for databeskyttelsesrammen, 3) oplysninger om, at deres tvistbilægges-tjenester under EU-USA-databeskyttelsesrammen er gratis for registrerede, 4) oplysninger om indgivelse af klager vedrørende principperne, 5) oplysninger om tidsrammen for behandling af klager vedrørende principperne og 6) oplysninger om de forskellige potentielle retsmidler.
- iii. Uafhængige klageinstanser skal offentliggøre en årlig rapport med aggregeret statistik over deres tvistbilægges-tjenester. Den årlige rapport skal indeholde oplysninger om: 1) det samlede antal klager vedrørende principperne modtaget i rapporteringsåret, 2) typen af modtagne klager, 3) kvalitetsmål for tvistbilægges såsom klagebehandlingstid og 4) resultaterne af de modtagne klager, navnlig antal og typer retsmidler eller pålagte sanktioner.
- iv. Som anført i bilag I har den registrerede i forbindelse med øvrige krav mulighed for at indbringe sagen til voldgift for at få afgjort, om en deltagende organisation har misligholdt sine forpligtelser over for den pågældende i henhold til principperne, og om denne misligholdelse fortsat ikke er helt eller delvist afhjulpet. Voldgift kan kun anvendes til disse formål. Der er f.eks. ikke adgang til voldgift i forbindelse med undtagelserne til principperne⁽¹⁵⁾ eller i forbindelse med en påstand om tilstrækkeligheden af EU-USA-databeskyttelsesrammen. Denne mulighed for voldgift giver udelukkende "panelet i EU-USA-databeskyttelsesrammen" (der består af en eller tre voldgiftsmænd som aftalt mellem parterne) beføjelser til at pålægge den nødvendige individuelle ikkepengemæssige rimelige afhjælpning (f.eks. indsigt, berigtigelse, sletning eller tilbagesendelse af den pågældendes oplysninger) for at afhjælpe overtrædelsen af principperne i forhold til de registrerede. Registrerede og deltagende organisationer har adgang til domstolsprøvelse og håndhævelse af voldgiftsafgørelser i henhold til amerikansk ret under Federal Arbitration Act.

e. Retsmidler og sanktioner

- i. Anvendelsen af de retsmidler, som tvistbilæggesinstansen giver adgang til, bør resultere i, at den pågældende organisation så vidt muligt udbedrer konsekvenserne af den manglende overholdelse, at organisationens fremtidige behandling sker i overensstemmelse med principperne, og at behandlingen af personoplysningerne om den person, der har indbragt klagen, i påkommende tilfælde ophører. Sanktionerne skal være tilstrækkeligt strenge til at få organisationen til at overholde principperne. Tvistbilæggesinstanser vil ved hjælp af en række sanktioner af forskellig strenghedsgrad have mulighed for på passende vis at reagere på forskellige grader af manglende overholdelse. Disse sanktioner bør omfatte offentliggørelse af konstateringerne af manglende overholdelse og påbud om i visse tilfælde at

⁽¹⁵⁾ Principperne, oversigt, punkt 5.

slette oplysninger ⁽¹⁶⁾. Andre sanktioner kan være suspendering eller tilbagetrækning af en godkendelse, betaling af skadeserstatning til registrerede for tab som følge af en overtrædelse af principperne og forbud eller påbud. Tvistbilæggesinstanser og selvregulerende instanser i den private sektor skal underrette den kompetente statslige instans eller i påkommende tilfælde domstolene samt ministeriet om deltagende organisationer, der ikke efterlever deres afgørelser.

f. FTC's behandling af klager

- i. FTC har forpligtet sig til at give højeste prioritet til behandling af sager om påstået overtrædelse af principperne, som den får henvist fra i) selvregulerende instanser med kompetence inden for beskyttelse af privatlivets fred og andre uafhængige tvistbilæggesinstanser, ii) EU-medlemsstaterne og iii) ministeriet, for at fastslå, om Section 5 i Federal Trade Commission Act, der forbyder illoyal eller vildledende praksis inden for handel, er blevet overtrådt. Hvis FTC konkluderer, at der er grund til at antage, at Section 5 er blevet overtrådt, kan den løse sagen ved at forsøge at opnå et administrativt forbud (administrative cease and desist order) mod den pågældende praksis eller ved at indgive en klage til en forbundsdomstol, hvilket, såfremt klageren får medhold, kan resultere i en retsafgørelse med samme indhold truffet af forbundsdomstolen. Dette omfatter falske påstande om tilslutning til principperne eller deltagelse i EU-USA-databeskyttelsesrammen fremsat af organisationer, der ikke længere er opført på listen over deltagere i databeskyttelsesrammen eller aldrig har foretaget selvcertificering over for ministeriet. FTC kan opnå, at overtræderen idømmes civilretlige sanktioner, hvis et administrativt forbud ikke overholdes, og FTC kan indlede civilretlige eller strafferetlige sager for undladelse af at efterkomme en retsafgørelse, der er truffet af en forbundsdomstol. FTC skal underrette ministeriet om ethvert søgsmål, som den anlægger. Ministeriet opfordrer de øvrige statslige organer til at underrette ministeriet om den endelige afgørelse i sådanne sager eller om andre afgørelser om tilslutning til principperne.

g. Vedvarende overtrædelse af principperne

- i. Hvis en organisation vedvarende overtræder principperne, kan den ikke længere drage fordel af EU-USA-databeskyttelsesrammen. Organisationer, der vedvarende overtræder principperne, vil af ministeriet blive fjernet fra listen over deltagere i databeskyttelsesrammen, og de skal tilbagesende eller slette personoplysninger, de har modtaget under EU-USA-databeskyttelsesrammen.
- ii. En vedvarende overtrædelse af principperne forekommer, når en organisation, der har foretaget selvcertificering over for ministeriet, nægter at rette sig efter den endelige afgørelse truffet af en uafhængig selvregulerende tvistbilæggesinstans med kompetence inden for beskyttelse af privatlivets fred eller af en statslig instans, eller når en sådan instans, herunder ministeriet, fastslår, at en organisation hyppigt har overtrådt principperne i et sådant omfang, at det ikke længere er rimeligt at påstå, at den overholder principperne. Hvis en sådan afgørelse træffes af et andet organ end ministeriet, skal organisationen straks underrette ministeriet derom. En organisation, der ikke opfylder denne forpligtelse, kan retsforfølges efter False Statements Act (18 U.S.C. § 1001). En organisation, der trækker sig fra et selvreguleringsprogram til beskyttelse af privatlivets fred i den private sektor eller fra en uafhængig selvregulerende tvistbilæggesinstans i den private sektor, skal stadig overholde principperne, og såfremt dette ikke er tilfældet, vil det blive betragtet som en vedvarende overtrædelse.
- iii. Ministeriet vil på baggrund af enhver meddelelse om vedvarende overtrædelse, uanset om det modtager denne meddelelse fra organisationen selv, fra en selvregulerende instans med kompetence inden for beskyttelse af privatlivets fred, fra en anden uafhængig tvistbilæggesinstans eller fra en statslig instans, fjerne organisationen fra listen over deltagere i databeskyttelsesrammen, dog først efter at have givet den pågældende organisation en frist på 30 dage og en mulighed for at svare ⁽¹⁷⁾. Det vil således tydeligt fremgå af ministeriets liste over deltagere i databeskyttelsesrammen, hvilke organisationer der er eller ikke er dækket af EU-USA-databeskyttelsesrammen.
- iv. En organisation, der ønsker at tilslutte sig en selvregulerende instans med henblik på igen at kvalificere sig til EU-USA-databeskyttelsesrammen, skal give denne instans fuldstændige oplysninger om sin tidligere deltagelse i EU-USA-databeskyttelsesrammen.

⁽¹⁶⁾ Uafhængige tvistbilæggesinstanser skønner selv, under hvilke omstændigheder disse sanktioner skal anvendes. Spørgsmålet om de pågældende oplysningers følsomhed og spørgsmålet om, hvorvidt en organisation har indsamlet, anvendt eller videregivet oplysninger i åbenlys strid med principperne, er nogle af de faktorer, der skal tages i betragtning, når det skal beslutes, hvorvidt der skal kræves sletning af data.

⁽¹⁷⁾ Ministeriet angiver i meddelelsen, hvor lang tid — altså nødvendigvis mindre end 30 dage — organisationen har til at svare på meddelelsen.

12. Valgfrihed og tidsfristen for at vælge fra (opt out)

- a. Formålet med princippet om valgfrihed er generelt at sikre, at personoplysninger anvendes og videregives i overensstemmelse med den registreredes forventninger og valg. Den registrerede skal således til enhver tid kunne vælge ikke at lade sine personoplysninger anvende til direkte markedsføring (opt out). Den pågældende organisation kan dog fastsætte passende tidsfrister for denne valgfrihed, f.eks. for at have tid til at indføre dette fravalg i systemet. En organisation kan ligeledes anmode om tilstrækkelige oplysninger for at bekræfte identiteten på den person, der ønsker at vælge fra. I USA kan registrerede gøre brug af denne valgfrihed ved hjælp af en central fravalgsordning. Den registrerede skal under alle omstændigheder nemt og uden uforholdsmæssigt store omkostninger kunne gøre brug af denne valgfrihed.
- b. På samme måde kan en organisation anvende oplysninger til visse direkte markedsføringsformål, når det i praksis er umuligt at give den registrerede mulighed for at vælge fra, inden oplysningerne anvendes, dog kun såfremt organisationen straks giver den pågældende mulighed for samtidig (eller efter anmodning til enhver tid) (uden omkostninger for den pågældende) at afslå at modtage yderligere direkte markedsføringshenvendelser, og såfremt organisationen overholder den pågældendes ønsker.

13. Passageroplysninger

- a. Oplysninger om pladsreservation for flypassagerer og andre passageroplysninger, f.eks. oplysninger om hyppige flyvninger (frequent flyer) eller hotelreservation eller om særlige behov, herunder religiøst betingede krav til måltider eller fysisk assistance, kan overføres til organisationer uden for EU i flere forskellige tilfælde. Når der ikke foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, kan personoplysninger i henhold til databeskyttelsesforordningen overføres til et tredjeland, hvis der er givet de fornødne databeskyttelsesgarantier, jf. databeskyttelsesforordningens artikel 46, eller i særlige situationer, hvis en af betingelserne i databeskyttelsesforordningens artikel 49 er opfyldt (f.eks. når den registrerede udtrykkeligt har givet sit samtykke til overførslen). Amerikanske organisationer, der tilslutter sig EU-USA-databeskyttelsesrammen, giver en tilstrækkelig beskyttelse af personoplysninger og kan derfor modtage dataoverførsler fra EU på grundlag af databeskyttelsesforordningens artikel 45 uden at skulle indføre et overførselsinstrument i henhold til databeskyttelsesforordningens artikel 46 eller opfylde betingelserne i databeskyttelsesforordningens artikel 49. Eftersom EU-USA-databeskyttelsesrammen omfatter specifikke regler for følsomme oplysninger, kan denne type oplysninger (som f.eks. indsamles i forbindelse med kundernes behov for fysisk assistance) være omfattet af overførsler til deltagende organisationer. Den organisation, der overfører oplysninger, skal dog under alle omstændigheder overholde lovgivningen i de EU-medlemsstater, hvor den udøver sine aktiviteter, hvilket bl.a. kan medføre særlige krav til behandlingen af følsomme oplysninger.

14. Farmaceutiske og medicinske produkter

- a. Anvendelse af EU's/medlemsstaternes lovgivning eller principperne
 - i. EU's/medlemsstaternes lovgivning finder anvendelse på indsamlingen af personoplysninger og på enhver behandling, der foretages forud for overførslen til USA. Principperne finder først anvendelse på oplysningerne, efter at de er blevet overført til USA. Oplysninger, der anvendes til farmaceutisk forskning og andre formål, skal i passende omfang anonymiseres.
- b. Fremtidig videnskabelig forskning
 - i. Personoplysninger, der opnås gennem specifik medicinsk eller farmaceutisk forskning, spiller ofte en vigtig rolle for fremtidig videnskabelig forskning. Hvis personoplysninger indsamlet til et bestemt forskningsprojekt overføres til en organisation i USA, som deltager i EU-USA-databeskyttelsesrammen, kan organisationen anvende personoplysningerne til ny videnskabelig forskning, hvis principperne om oplysningspligt og valgfrihed er blevet overholdt fra start af. Eventuelle fremtidige specifikke anvendelser af de pågældende personoplysninger, f.eks. regelmæssig kontrol, beslægtede undersøgelser eller markedsføring, skal fremgå af den meddelelse, der gives i medfør af princippet om oplysningspligt.

- ii. Det er naturligvis ikke muligt at specificere alle fremtidige anvendelser af oplysningerne, eftersom anvendelsen i et nyt forskningsprojekt eventuelt kan bygge på ny viden, som er opnået ved hjælp af de oprindelige personoplysninger, nye medicinske opdagelser eller fremskridt eller udviklingen inden for offentlig sundhed eller lovgivningen på sundhedsområdet. Meddelelsen skal derfor i givet fald omfatte en forklaring om, at personoplysninger kan anvendes i fremtidige, men uforudsigelige medicinske eller farmaceutiske forskningsprojekter. Hvis anvendelsen ikke er forenelig med de(t) generelle forskningsformål, hvortil personoplysningerne oprindeligt blev indsamlet, eller som den enkelte efterfølgende har godkendt, skal der indhentes en ny tilladelse.
- c. Tilbagetrækning fra et klinisk forsøg
 - i. Deltagere kan til enhver tid beslutte eller blive anmodet om at trække sig ud af et klinisk forsøg. Alle personoplysninger, der indsamles forud for tilbagetrækningen, må stadig behandles sammen med de øvrige oplysninger, der indsamles i forbindelse med det kliniske forsøg, dog kun såfremt den pågældende deltager klart har fået meddelt dette i forbindelse med tilmeldingen til forsøget.
- d. Overførsler med henblik på regulering og kontrol
 - i. Virksomheder, der fremstiller farmaceutiske eller medicinske anordninger, må udlevere personoplysninger, der er opnået i forbindelse med kliniske forsøg i EU, til tilsynsmyndighederne i USA med henblik på regulering og kontrol. Det er tilladt at foretage lignende overførsler til andre end tilsynsmyndighederne, f.eks. virksomheder eller andre forskere, i overensstemmelse med principperne om oplysningspligt og valgfrihed.
- e. Blindundersøgelser
 - i. For at gøre de kliniske forsøg så objektive som muligt har deltagerne og til tider undersøgerne selv ikke adgang til oplysninger om den specifikke behandling, som hver deltager modtager. En sådan indsigt ville skade forskningsprojektet og resultaterne. Deltagere i sådanne kliniske forsøg (også kaldet "blindundersøgelser") skal ikke gives indsigt i oplysningerne om deres behandling under forsøget, hvis de fik oplyst denne begrænsning ved tilmeldingen til forsøget, og hvis videregivelsen af sådanne oplysninger ville være til skade for forskningsarbejdet.
 - ii. Man anses ved at acceptere at deltage i forsøget på disse betingelser for at give afkald på retten til indsigt. Deltagerne skal, såfremt de anmoder derom, have indsigt i deres personoplysninger, når forsøget er overstået, og når resultaterne er blevet analyseret. De skal først henvende sig til den læge eller behandler, som de er blevet behandlet af i forbindelse med det kliniske forsøg, hvorefter de eventuelt kan henvende sig til den sponsorerende organisation.
- f. Produktsikkerhed og kontrol
 - i. En virksomhed, der fremstiller farmaceutiske eller medicinske anordninger, behøver ikke anvende principperne om oplysningspligt, valgfrihed, ansvar for videreoverførsel og indsigt i sine produktsikkerheds- og kontrolaktiviteter, herunder i meddelelser om negative konstateringer og registreringer af patienter/registrerede, der anvender bestemte lægemidler eller medicinske anordninger, i det omfang princippernes anvendelse kolliderer med overholdelsen af de gældende lovkrav. Det gælder både med hensyn til f.eks. rapporteringen fra behandlere til virksomheder, der fremstiller farmaceutiske eller medicinske anordninger, og med hensyn til rapporteringen fra disse virksomheder til myndighederne, f.eks. Food and Drug Administration.
- g. Kodede data
 - i. Som regel koder undersøgeren forskningsoplysningerne entydigt ved kilden for ikke at afsløre de enkelte registreredes identitet. De farmaceutiske virksomheder, der sponsorerer en sådan forskning, modtager ikke en nøgle til denne kode. Det er udelukkende forskeren, der er i besiddelse af den entydige nøgle, således at han/hun under særlige forhold er i stand til at identificere den enkelte forskningsdeltager (f.eks. hvis der er behov for efterfølgende medicinsk kontrol). En overførsel fra EU til USA af oplysninger, der er kodet på den måde, hvorpå personoplysninger i EU kodes i henhold til EU-retten, vil være omfattet af principperne.

15. Oplysninger i offentlige registre og offentligt tilgængelige oplysninger

- a. En organisation skal anvende principperne om sikkerhed, dataintegritet og formålsbegrænsning og om klageadgang, håndhævelse og ansvar på personoplysninger fra offentligt tilgængelige kilder. Disse principper finder ligeledes anvendelse på personoplysninger indsamlet fra offentlige registre (f.eks. registrene hos statsorganer eller statslige enheder på ethvert niveau, som er offentligt tilgængelige).
- b. Det er ikke nødvendigt at anvende principperne om oplysningspligt, valgfrihed og ansvar for videreoverførsel på oplysninger i offentlige registre, såfremt de ikke sammenføres med oplysninger i ikkeoffentlige registre, og såfremt alle betingelser for indsigt, der fastsættes af den kompetente myndighed, overholdes. Det er generelt heller ikke nødvendigt at anvende principperne om oplysningspligt, valgfrihed og ansvar for videreoverførsel på offentligt tilgængelige oplysninger, medmindre den europæiske dataafsender meddeler, at de pågældende oplysninger er underlagt begrænsninger, der kræver, at den pågældende organisation anvender disse principper til de tilsigtede formål. Organisationer er ikke ansvarlige for den måde, hvorpå disse oplysninger anvendes af andre, der indhenter oplysningerne fra offentliggjort materiale.
- c. Organisationer vil blive udelukket fra EU-USA-databeskyttelsesrammen, hvis det konstateres, at de med fuldt overlæg og i strid med principperne har offentliggjort personoplysninger, således at de selv eller andre kan drage fordel af disse undtagelser.
- d. Det er ikke nødvendigt at anvende princippet om indsigt på oplysninger i offentlige registre, såfremt de ikke sammenføres med andre personoplysninger (undtagen små mængder oplysninger, der anvendes til at indeksere eller strukturere oplysninger fra offentlige registre). Enhver betingelse for indsigt i sådanne oplysninger, der fastsættes af den kompetente myndighed, skal dog overholdes. Hvis oplysninger fra offentlige registre derimod sammenføres med andre oplysninger, der ikke er offentligt tilgængelige (andre end de specifikt ovenfor anførte), skal en organisation give indsigt i alle disse oplysninger, såfremt de ikke er underlagt andre tilladte undtagelser.
- e. Ligesom for offentligt tilgængelige oplysninger er det ikke nødvendigt at anvende princippet om indsigt på oplysninger, der allerede er offentligt tilgængelige, såfremt disse oplysninger ikke er sammenført med oplysninger, der ikke er offentligt tilgængelige. Organisationer, der beskæftiger sig med salg af offentligt tilgængelige oplysninger, kan opkræve et gebyr efter deres normale takst for at besvare anmodninger om indsigt. Den registrerede kan også vælge at anmode om indsigt i sine oplysninger hos den organisation, der oprindeligt har indsamlet de pågældende oplysninger.

16. Offentlige myndigheders anmodninger om indsigt

- a. Med henblik på at sikre gennemsigtighed omkring offentlige myndigheders lovlige anmodninger om indsigt i personoplysninger kan deltagende organisationer frivilligt udarbejde regelmæssige gennemsigtighedsrapporter om det antal anmodninger om personoplysninger, de modtager fra offentlige myndigheder begrundet i hensynet til retshåndhævelse eller den nationale sikkerhed, i det omfang denne offentliggørelse er tilladt i henhold til loven.
 - b. De oplysninger, som de deltagende organisationer offentliggør i disse rapporter, samt oplysninger offentliggjort af det amerikanske efterretningssamfund kan sammen med andre oplysninger anvendes i den regelmæssige fælles evaluering af, om EU-USA-databeskyttelsesrammen fungerer i overensstemmelse med principperne.
 - c. Manglende overholdelse af oplysningspligten i henhold til punkt a, nr. xii, i princippet om oplysningspligt forhindrer eller forringer ikke muligheden for, at en organisation kan besvare en lovlig anmodning.
-

BILAG I: VOLDGIFTSMODEL

I dette bilag I angives de betingelser, hvorunder organisationer, som deltager i EU-USA-databeskyttelsesrammen, skal lade klager afgøre ved voldgift i medfør af princippet om klageadgang, håndhævelse og ansvar. Muligheden for bindende voldgift som beskrevet nedenfor gælder for visse "øvrige" krav vedrørende oplysninger omfattet af EU-USA-databeskyttelsesrammen. Formålet med voldgift er at give den registrerede mulighed for at vælge en hurtig, uafhængig og fair mekanisme, der kan behandle klager over påståede overtrædelser af principperne, som ikke er blevet afgjort af eventuelle andre instanser i EU-USA-databeskyttelsesrammen.

A. Anvendelsesområde

Den registrerede har adgang til voldgift i forbindelse med øvrige krav for at få afgjort, om en deltagende organisation har misligholdt sine forpligtelser over for den pågældende i henhold til principperne, og om denne misligholdelse fortsat ikke er helt eller delvist afhjulpet. Voldgift kan kun anvendes til disse formål. Der er f.eks. ikke adgang til voldgift i forbindelse med undtagelserne til principperne ⁽¹⁾ eller i forbindelse med en påstand om tilstrækkeligheden af EU-USA-databeskyttelsesrammen.

B. Tilgængelige retsmidler

Denne mulighed for voldgift giver udelukkende "panelet i EU-USA-databeskyttelsesrammen" (der består af en eller tre voldgiftsmænd som aftalt mellem parterne) beføjelser til at pålægge den nødvendige individuelle ikkepengemæssige rimelige afhjælpning (f.eks. indsigt, berigtigelse og sletning eller tilbagesendelse af den pågældendes oplysninger) for at afhjælpne overtrædelser af principperne i forhold til de registrerede. Dette er de eneste beføjelser, som panelet i EU-USA-databeskyttelsesrammen har, for så vidt angår retsmidler. Panelet skal tage højde for andre retsmidler, der allerede er blevet pålagt gennem andre mekanismer i EU-USA-databeskyttelsesrammen, når det træffer afgørelse om retsmidler. Der er ikke mulighed for erstatning, for dækning af omkostninger og salærer eller for andre retsmidler. Den enkelte part afholder egne omkostninger til advokatsalær.

C. Krav forud for voldgiften

En person, der beslutter sig for at kræve voldgift, skal træffe følgende foranstaltninger inden indgivelse af en begæring om voldgift: 1) rette direkte henvendelse til organisationen og fremføre den påståede overtrædelse og give organisationen mulighed for at løse problemet inden for den tidsramme, der er anført i punkt d, nr. i, i det supplerende princip om bilægelse af tvister og håndhævelse, 2) gøre brug af den uafhængige klageinstans i henhold til principperne, hvilket er gratis for den pågældende, og 3) rejse sagen gennem den pågældendes databeskyttelsesmyndighed over for ministeriet og give ministeriet mulighed for at gøre sit yderste for at løse problemet inden for de tidsfrister, der er anført i brevet fra det amerikanske handelsministeriums International Trade Administration, uden omkostninger for den pågældende.

Der kan ikke stilles krav om voldgift, hvis den samme påståede overtrædelse af principperne 1) tidligere har været genstand for bindende voldgift, 2) har været genstand for en endelig dom afsagt i en retssag, som den pågældende var part i, eller 3) tidligere er blevet bilagt af parterne. Der kan derudover ikke gøres brug af denne mulighed, hvis en databeskyttelsesmyndighed 1) er bemyndiget i henhold til det supplerende princip om databeskyttelsesmyndighedernes rolle eller det supplerende princip om oplysninger om menneskelige ressourcer, eller 2) er bemyndiget til at rette direkte henvendelse til organisationen for at finde en løsning på den påståede overtrædelse. En databeskyttelsesmyndigheds kompetence til at afgøre den samme sag mod en dataansvarlig i EU udelukker ikke i sig selv muligheden for at stille krav om voldgift over for en anden retlig enhed, der ikke er underlagt databeskyttelsesmyndighedens kompetence.

D. Afgørelsernes bindende karakter

Den registrerede vælger helt frivilligt at stille krav om bindende voldgift. Voldgiftsafgørelser vil være bindende for alle voldgiftsparter. Når den registrerede har stillet krav om voldgift, kan den pågældende ikke længere søge den samme påståede overtrædelse afhjulpet i et andet forum. Hvis den ikkepengemæssige rimelige afhjælpning ikke afhjælper den påståede overtrædelse fuldt ud, udelukker den registreredes krav om voldgift dog ikke muligheden for at kræve erstatning ved domstolene.

⁽¹⁾ Principperne, oversigt, punkt 5.

E. Domstolsprøvelse og håndhævelse

Registrerede og deltagende organisationer har adgang til domstolsprøvelse og håndhævelse af voldgiftsafgørelser i henhold til amerikansk ret under Federal Arbitration Act ⁽²⁾. Disse sager skal indbringes for den forbundsdistriktsdomstol (federal district court), inden for hvis jurisdiktion hovedforretningsstedet for den deltagende organisation er beliggende.

Formålet med voldgift er at bilægge individuelle tvister, og det er ikke hensigten, at voldgiftsafgørelser skal fungere som overbevisende eller bindende præcedens i sager, der involverer andre parter, herunder i fremtidige voldgiftssager, for domstole i EU eller USA eller i FTC-sager.

F. Voldgiftspanel

Parterne skal vælge voldgiftsmændene til panelet i EU-USA-databeskyttelsesrammen fra den nedenfor omhandlede liste over voldgiftsmænd.

I overensstemmelse med gældende ret vil ministeriet og Kommissionen udarbejde en liste med mindst 10 voldgiftsmænd valgt på baggrund af deres uafhængighed, integritet og ekspertviden. Processen er som følger:

Voldgiftsmænd:

- 1) er opført på listen i en periode på 3 år, der ekstraordinært kan forlænges af ministeriet efter forudgående meddelelse til Kommissionen i yderligere perioder på tre år
- 2) må ikke modtage instrukser fra eller være tilknyttet nogen part eller nogen deltagende organisation, USA, EU eller nogen EU-medlemsstat eller nogen anden statslig myndighed, offentlig myndighed eller håndhævelsesmyndighed og
- 3) skal have tilladelse til at arbejde som advokat i USA og være ekspert i amerikansk privatret og have ekspertviden om EU's databeskyttelsesregler.

⁽²⁾ Det fastslås i kapitel 2 i Federal Arbitration Act ("FAA"), at "en voldgiftsaftale eller voldgiftskendelse, der følger af et kontraktligt eller ikkekontraktligt retsforhold, som betragtes som kommercielt, herunder en transaktion, kontrakt eller aftale som beskrevet i [Section 2 i FAA], henhører under konventionen [om anerkendelse og fuldbyrdelse af udenlandske voldgiftskendelser af 10.6.1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York-konventionen")]". 9 U.S.C. § 202. Det fastslås endvidere i FAA, at "en aftale eller voldgiftskendelse, der følger af et sådant forhold, som udelukkende eksisterer mellem to amerikanske statsborgere, ikke anses for at henhøre under [New York-konventionen], medmindre dette forhold involverer ejendom i udlandet, skal gennemføres eller håndhæves i udlandet eller har en anden rimelig forbindelse til en eller flere fremmede stater". Idem. I henhold til kapitel 2 "kan enhver part i voldgiftssagen anmode enhver kompetent domstol under dette kapitel om en kendelse, der bekræfter voldgiftskendelsen afsagt mod enhver anden part i voldgiftssagen. Domstolen bekræfter voldgiftskendelsen, medmindre den konstaterer tilstedeværelsen af en af de grunde til at nægte eller udsætte anerkendelsen eller fuldbyrdelsen af voldgiftskendelsen, der er angivet i [New York-konventionen]". Idem § 207. Det fastslås endvidere i kapitel 2, at "distriktsdomstolene (district courts) i USA [...] har oprindelig kompetence over [...] sager [omfattet af New York-konventionen], uanset beløbsstørrelsen". Idem § 203.

Det fastslås endvidere i kapitel 2, at "kapitel 1 finder anvendelse på sager anlagt under dette kapitel, i det omfang det pågældende kapitel ikke er i strid med dette kapitel eller [New York-konventionen] som ratificeret af USA". Idem § 208. Det fastslås i kapitel 1, at "en skriftlig bestemmelse i [...] en kontrakt om en transaktion, der involverer handel, hvor en strid, der efterfølgende opstår som følge af denne kontrakt eller transaktion eller af nægtelsen af at opfylde hele eller dele heraf, skal afgøres ved voldgift, eller en skriftlig aftale om, at en eksisterende tvist opstår som følge af en sådan aftale, transaktion eller nægtelse skal afgøres ved voldgift, er gyldig, uigenkaldelig og eksigibel, medmindre der er andre grunde i henhold til loven eller ifølge billighedsretten for ophævelse af kontrakter". Idem § 2. Det fastslås endvidere i kapitel 1, at "enhver part i voldgiftssagen kan anmode den kompetente domstol om en kendelse, der bekræfter voldgiftskendelsen, og domstolen skal herefter afsige en sådan kendelse, medmindre voldgiftskendelsen omstødes, ændres eller rettes som foreskrevet i Section 10 og Section 11 i [FAA]". Idem § 9.

G. Voldgiftsprocedurer

I henhold til gældende ret er ministeriet og Kommissionen nået til enighed om at vedtage voldgiftsregler, som finder anvendelse på sager, der indbringes for panelet i EU-USA-databeskyttelsesrammen ⁽³⁾. Hvis voldgiftsreglerne skal ændres, vil ministeriet og Kommissionen i påkommende tilfælde indgå aftale om at ændre disse regler eller nå til enighed om en række eksisterende vejetablerede amerikanske voldgiftsprocedurer, under hensyntagen til følgende:

1. En person kan indlede en bindende voldgiftssag, forudsat at ovennævnte krav forud for voldgiften er opfyldt, ved at fremsende en meddelelse ("notice") til organisationen. Meddelelsen skal indeholde en sammenfatning af de skridt, der er taget i henhold til punkt C, for at løse sagen, en beskrivelse af den påståede overtrædelse og — efter klagerens valg — eventuelle støttedokumenter og -materiale og/eller en redegørelse for de regler, der finder anvendelse på den påståede overtrædelse.
2. Der vil blive udviklet procedurer, der sikrer, at den samme påståede overtrædelse ikke omfattes af flere retsmidler eller procedurer.
3. Der kan anlægges FTC-sager parallelt med voldgiftsbehandling.
4. Ingen repræsentant fra USA, EU, ingen medlemsstat eller anden statslig myndighed, offentlig myndighed eller håndhævelsesmyndighed må deltage i disse voldgiftssager. EU's databeskyttelsesmyndigheder må kun bistå ved udarbejdelsen af meddelelsen, hvis den registrerede i EU anmoder herom, men de må ikke få adgang til fremlæggelsesmateriale eller andet materiale vedrørende voldgiftssagerne.
5. Voldgiftsbehandlingen vil finde sted i USA, og den registrerede kan vælge at deltage via video- eller telefonkonference uden omkostninger for den pågældende. Det er ikke nødvendigt at møde personligt op.
6. Medmindre parterne har aftalt andet, foregår voldgiftsbehandlingen på engelsk. På grundlag af en begrundet anmodning og under hensyntagen til, om den registrerede møder ved advokat, vil der uden omkostninger for den registrerede være tolkning under voldgiftsbehandlingen, og materiale vedrørende voldgiftssagen vil blive oversat, medmindre panelet i EU-USA-databeskyttelsesrammen beslutter, at dette i den specifikke voldgiftssag ville føre til uberettigede eller uforholdsmæssigt store omkostninger.
7. Materiale forelagt voldgiftsmænd vil blive behandlet fortroligt og vil kun blive anvendt i forbindelse med voldgiftsbehandlingen.
8. Individuel fremlæggelse kan tillades, hvis den er nødvendig, og parterne vil behandle denne fremlæggelse fortroligt, og den vil kun blive anvendt i forbindelse med voldgiftsbehandlingen.
9. Voldgiftsbehandlingen bør afsluttes senest 90 dage efter meddelelsens forelæggelse for den pågældende organisation, medmindre parterne aftaler andet.

⁽³⁾ Ministeriet har udvalgt International Centre for Dispute Resolution ("ICDR"), den internationale afdeling af American Arbitration Association ("AAA") (samlet benævnt "ICDR-AAA"), til at forvalte voldgiftssager i henhold til — og til at administrere den voldgiftsfond, der er omhandlet i — bilag I til principperne. Den 15. september 2017 enedes ministeriet og Kommissionen om vedtagelsen af et sæt voldgiftsregler for bindende voldgiftsprocedurer, der er beskrevet i bilag I til principperne, samt en adfærdskodeks for voldgiftsmænd, der er i overensstemmelse med almindeligt anerkendte etiske standarder for handelsvoldgiftsmænd og bilag I til principperne. Ministeriet og Kommissionen blev enige om at tilpasse voldgiftsreglerne og adfærdskodeksen, så de afspejler ajourføringer i henhold til EU-USA-databeskyttelsesrammen, og ministeriet vil samarbejde med ICDR-AAA om at foretage disse ajourføringer.

H. Omkostninger

Voldgiftsmænd bør træffe rimelige foranstaltninger for at minimere voldgiftsomkostningerne og -gebyrerne.

Under iagttagelse af gældende ret vil ministeriet etablere en fond, der skal finansieres via bidrag fra de deltagende organisationer, som til dels er baseret på organisationens størrelse, og fonden vil dække voldgiftsomkostningerne, herunder voldgiftsmændenes honorarer, op til fastsatte maksimumsbeløb. Fonden vil blive forvaltet af en tredjemand, der regelmæssigt vil rapportere til ministeriet om fondens drift. Ministeriet vil i samarbejde med tredjemanden regelmæssigt evaluere fondens drift, herunder behovet for at justere bidragene eller maksimumsbeløbene for voldgiftsomkostningerne, og vil bl.a. se på antallet af voldgiftssager, voldgiftsomkostningerne og behandlingstiden ud fra den holdning, at de deltagende organisationer ikke må pålægges en urimelig stor økonomisk byrde. Ministeriet underretter Kommissionen om resultatet af disse evalueringer, som udføres i samarbejde med tredjeparten, og underretter på forhånd Kommissionen om eventuelle justeringer af bidragenes størrelse. Advokatsalærer er ikke omfattet af denne bestemmelse eller nogen fond under denne bestemmelse.

BILAG II



UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

Den 6. juli 2023

Didier Reynders
Kommissær for retlige anliggender
Europa-Kommissionen
Rue de la Loi/ Wetstraat 200
1049 Bruxelles/Brussel
Belgien

Kære kommissær Didier Reynders,

Det glæder mig på vegne af USA at kunne fremsende en pakke med dokumenter vedrørende EU-USA-databeskyttelsesrammen, som sammen med præsidentielt dekret 14086 (Executive Order 14086) med titlen "Enhancing Safeguards for United States Signals Intelligence Activities" og 28 CFR part 201 om ændring af justitsministeriets forordninger med henblik på oprettelse af "Data Protection Review Court" afspejler en række vigtige og omfattende forhandlinger om styrkelse af beskyttelsen af privatlivets fred og de borgerlige frihedsrettigheder. Disse forhandlinger har udmøntet sig i nye garantier, som skal sikre, at de amerikanske signalefterretningsaktiviteter er nødvendige og forholdsmæssige i forfølgelsen af definerede nationale sikkerhedsmål, og en ny mekanisme, der gør det muligt for personer fra Den Europæiske Union ("EU") at indgive en klage, hvis de mener, at de ulovligt er mål for signalefterretningsaktiviteter. Tilsammen vil disse to tiltag sikre beskyttelsen af personoplysninger fra EU. EU-USA-databeskyttelsesrammen vil understøtte en inklusiv og konkurrencedygtig digital økonomi. Vi bør begge være stolte af de forbedringer, som denne ramme afspejler, og som vil styrke beskyttelsen af privatlivets fred i hele verden. Denne pakke udgør sammen med det præsidentielle dekret, forordningerne og andet materiale fra offentlige kilder et meget solidt grundlag for Europa-Kommissionens vedtagelse af en ny afgørelse om tilstrækkeligheden af beskyttelsesniveauet ⁽¹⁾.

Følgende materiale er vedlagt:

- principperne i EU-USA-databeskyttelsesrammen, herunder de supplerende principper (samlet benævnt "principperne") og bilag I til principperne (dvs. et bilag, der indeholder de betingelser, hvorunder organisationer inden for databeskyttelsesrammen er forpligtet til at lade visse øvrige krav vedrørende personoplysninger, der er omfattet af principperne, afgøre ved voldgift)
- et brev fra ministeriets International Trade Administration, som forvalter programmet for databeskyttelse, hvor der redegøres for de tilsagn, som ministeriet har afgivet for at sikre, at EU-USA-databeskyttelsesrammen fungerer effektivt
- et brev fra Federal Trade Commission (FTC), hvor der redegøres for FTC's håndhævelse af principperne
- et brev fra transportministeriet, hvor der redegøres for dets håndhævelse af principperne
- et brev fra Office of the Director of National Intelligence (ODNI) vedrørende de garantier og begrænsninger, der finder anvendelse på de amerikanske nationale sikkerhedsmyndigheder, og
- et brev fra det amerikanske justitsministerium vedrørende garantier og begrænsninger for den amerikanske regerings adgang til personoplysninger med henblik på retshåndhævelse og andre offentlige interesser.

⁽¹⁾ Forudsat at Kommissionens afgørelse om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU-USA-databeskyttelsesrammen, finder anvendelse på Island, Liechtenstein og Norge, omfatter pakken vedrørende EU-USA-databeskyttelsesrammen både Den Europæiske Union og disse tre lande.

Den samlede pakke vedrørende EU-USA-databeskyttelsesrammen vil blive offentliggjort på ministeriets websted for databeskyttelse, og principperne og bilag I til principperne vil træde i kraft på ikrafttrædelsesdatoen for Europa-Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

USA tager disse tilsagn meget alvorligt. Vi glæder os til vores samarbejde om gennemførelsen af EU-USA-databeskyttelsesrammen og i den kommende fase i denne proces.

Med venlig hilsen



Gina M. RAIMONDO

BILAG III



UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

Den 12. december 2022

Didier Reynders
Kommissær for retlige anliggender
Europa-Kommissionen
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
Belgien

Kære kommissær Didier Reynders,

Det glæder mig på vegne af International Trade Administration ("ITA") at redegøre for de tilsagn, som det amerikanske handelsministerium ("ministeriet") har afgivet for at sikre beskyttelsen af personoplysninger i dets forvaltning og overvågning af programmet for databeskyttelse. Færdiggørelsen af EU-USA-databeskyttelsesrammen er et vigtigt skridt for privatlivets fred og for virksomheder på begge sider af Atlanten. Den giver personer i EU en tro på, at deres oplysninger vil blive beskyttet, og at de vil have adgang til retsmidler til afhjælpning af problemer i forbindelse med deres oplysninger, og den sikrer, at tusindvis af virksomheder fortsat kan investere og gøre forretninger på tværs af Atlanten, hvilket er til gavn for vores respektive økonomier og borgere. EU-USA-databeskyttelsesrammen afspejler flere års hårdt arbejde og samarbejde med Dem og Deres kolleger i Europa-Kommissionen ("Kommissionen"). Vi glæder os til vores fortsatte samarbejde med Kommissionen om at sikre, at dette samarbejde fungerer effektivt.

EU-USA-databeskyttelsesrammen indebærer en række væsentlige fordele for både personer og virksomheder. For det første er der en række vigtige bestemmelser om beskyttelse af EU-borgeres personoplysninger, som overføres til USA. De deltagende amerikanske organisationer skal udvikle en overensstemmende politik til beskyttelse af privatlivets fred, offentligt forpligte sig til at overholde "principperne i EU-USA-databeskyttelsesrammen", herunder de supplerende principper (samlet benævnt "principperne") og bilag I til principperne (dvs. et bilag, der indeholder de betingelser, hvorunder organisationer inden for EU-USA-databeskyttelsesrammen er forpligtet til at lade visse øvrige krav vedrørende personoplysninger, der er omfattet af principperne, afgøre ved voldgift), således at forpligtelsen kan kræves opfyldt i henhold til amerikansk ret ⁽¹⁾, årligt recertificere deres overholdelse over for ministeriet, give privatpersoner i EU gratis adgang til en uafhængig tvistbilæggelsestjeneste og være underlagt de undersøgelses- og håndhævelsesbeføjelser, som et amerikansk lovbestemt organ, der er anført i principperne (f.eks. Federal Trade Commission eller transportministeriet), eller et amerikansk lovbestemt organ, der er anført i et fremtidigt bilag til principperne, er tillagt. Selv om en organisation selv afgør, om den vil foretage selvcertificering, kan Federal Trade Commission, transportministeriet eller et andet amerikansk lovbestemt organ, afhængigt af hvilken myndighed der har kompetence over den deltagende organisation, når først organisationen offentligt har forpligtet sig til at overholde principperne i EU-USA-databeskyttelsesrammen, håndhæve organisationens tilsagn i henhold til amerikansk ret. For det andet vil EU-USA-databeskyttelsesrammen give

⁽¹⁾ Organisationer, som har foretaget selvcertificering af deres tilslutning til principperne i EU's og USA's værn om privatlivets fred (EU-USA-privatlivsskjoldet), og som ønsker at drage fordel af EU-USA-databeskyttelsesrammen, skal overholde "principperne i EU-USA-databeskyttelsesrammen". Denne forpligtelse til at overholde "principperne i EU-USA-databeskyttelsesrammen" skal afspejles i de deltagende organisationers politik til beskyttelse af privatlivets fred hurtigst muligt og under alle omstændigheder senest tre måneder efter ikrafttrædelsesdatoen for "principperne i EU-USA-databeskyttelsesrammen". (Jf. punkt e. i det supplerende princip om selvcertificering).

virksomheder i USA og datterselskaber af europæiske virksomheder i USA mulighed for at modtage personoplysninger fra EU for at fremme datastrømme, som understøtter den transatlantiske handel. Datastrømmene mellem USA og EU er de mest omfattende i verden og underbygger det økonomiske forhold mellem USA og EU, som løber op i 7,1 bio. USD og understøtter millioner af arbejdspladser på begge sider af Atlanten. De virksomheder, der er afhængige af transatlantiske datastrømme, kommer fra alle industrisektorer og omfatter store Fortune 500-selskaber samt mange små og mellemstore virksomheder. Transatlantiske datastrømme giver amerikanske organisationer mulighed for at behandle oplysninger, der er nødvendige for at tilbyde europæiske borgere varer, tjenester og beskæftigelsesmuligheder.

Ministeriet vil arbejde tæt og produktivt sammen med vores EU-modparter for effektivt at forvalte og føre tilsyn med programmet for databeskyttelse. Dette tilsagn afspejles i ministeriets udvikling og fortsatte finjustering af en række ressourcer for at bistå organisationer med selvcertificeringsprocessen, oprettelse af et websted med målrettet information til interessenter, samarbejde med Kommissionen og de europæiske databeskyttelsesmyndigheder med henblik på at opstille retningslinjer, der klarlægger vigtige elementer i EU-USA-databeskyttelsesrammen, opsøgende arbejde for at fremme forståelsen af organisationernes databeskyttelsesforpligtelser og tilsyn med og overvågning af organisationernes opfyldelse af programmets krav.

Vores fortsatte samarbejde med vores EU-modparter vil gøre det muligt for ministeriet at sikre, at EU-USA-databeskyttelsesrammen fungerer effektivt. USA's regering har længe arbejdet sammen med Kommissionen om at fremme fælles databeskyttelsesprincipper, bygge bro mellem vores forskellige retlige procedurer og samtidig fremme handel og økonomisk vækst i EU og USA. Vi er af den opfattelse, at EU-USA-databeskyttelsesrammen, som er et eksempel på dette samarbejde, vil give Kommissionen mulighed for at udstede en ny afgørelse om tilstrækkeligheden af beskyttelsesniveauet, så organisationer kan anvende EU-USA-databeskyttelsesrammen til at overføre personoplysninger fra EU til USA i overensstemmelse med EU-retten.

Det amerikanske handelsministeriums forvaltning af og tilsyn med programmet for databeskyttelse

Ministeriet er fast besluttet på at sikre en effektiv forvaltning og overvågning af programmet for databeskyttelse og vil gøre en passende indsats herfor og afsætte passende ressourcer hertil. Ministeriet vil oprette og offentliggøre en officiel liste over amerikanske organisationer, der har foretaget selvcertificering over for ministeriet og offentligt erklæret, at de har tilsluttet sig principperne ("listen over deltagere i databeskyttelsesrammen"), som den vil ajourføre på grundlag af de deltagende organisationers årlige anmeldelser om recertificering og ved at fjerne organisationer, der frivilligt trækker sig, ikke indsender den årlige anmeldelse om recertificering i overensstemmelse med ministeriets procedurer eller vedvarende overtræder principperne. Ministeriet vil ligeledes oprette og offentliggøre en officiel fortegnelse over amerikanske organisationer, der er blevet fjernet fra listen over deltagere i databeskyttelsesrammen, og vil angive årsagerne til, at de enkelte organisationer er blevet fjernet fra listen. Ovennævnte officielle liste og fortegnelse vil være tilgængelig for offentligheden på ministeriets websted for databeskyttelsesrammen. På webstedet for databeskyttelsesrammen vil det tydeligt fremgå, at alle organisationer, der er fjernet fra listen over deltagere i databeskyttelsesrammen, ikke længere må hævde, at de deltager i eller overholder principperne i eller kan modtage personoplysninger i henhold til EU-USA-databeskyttelsesrammen. Sådanne organisationer skal ikke desto mindre stadig anvende principperne på de personoplysninger, som de modtog, mens de deltog i EU-USA-databeskyttelsesrammen, så længe de er i besiddelse af disse oplysninger. Med henblik på at fremme sit faste, overordnede tilsagn om at sikre en effektiv forvaltning og overvågning af programmet for databeskyttelse forpligter ministeriet sig navnlig til følgende:

Kontrol af selvcertificeringskrav

- Ministeriet vil forud for afslutningen af behandlingen af en organisations indledende selvcertificering eller årlige recertificering (samlet benævnt "selvcertificering") og opførelsen af en organisation på listen over deltagere i databeskyttelsesrammen kontrollere, at organisationen som minimum har opfyldt de relevante krav i det supplerende princip om selvcertificering med hensyn til, hvilke oplysninger en organisation skal give i sin anmeldelse om selvcertificering over for ministeriet, og rettidigt har fremlagt en relevant politik til beskyttelse af privatlivets fred, der informerer de registrerede om alle de 13 elementer, der er opregnet i princippet om oplysningspligt. Ministeriet kontrollerer, at organisationen:

- har identificeret den organisation, der indgiver sin anmeldelse om selvcertificering, samt alle de amerikanske enheder eller amerikanske datterselskaber af den selvcertificerende organisation, som også tilslutter sig principperne, og som organisationen ønsker skal være omfattet af dets selvcertificering,
- har anført de krævede kontaktoplysninger for organisationen (f.eks. kontaktoplysninger for bestemte personer og/eller kontorer i den organisation, der foretager selvcertificering, som har ansvaret for at behandle klager, anmodninger om indsigt og alle andre spørgsmål, der måtte opstå i forbindelse med EU-USA-databeskyttelsesrammen),
- har beskrevet det eller de formål, hvortil organisationen vil indsamle og anvende personoplysninger modtaget fra EU,
- har angivet, hvilke personoplysninger der vil blive modtaget fra EU i henhold til EU-USA-databeskyttelsesrammen, og som derfor er omfattet af selvcertificeringen,
- har angivet webadressen på det sted, hvor den relevante politik til beskyttelse af privatlivets fred er let tilgængelig, hvis organisationen har et offentligt websted, eller hvis organisationen ikke har et offentligt websted, fremsendt en kopi af den relevante politik til beskyttelse af privatlivets fred, og angivet, hvor de berørte personer kan få adgang til politikken til beskyttelse af privatlivets fred (dvs. de berørte ansatte, hvis den relevante politik til beskyttelse af privatlivets fred vedrører menneskelige ressourcer, eller offentligheden, hvis den relevante politik ikke vedrører menneskelige ressourcer),
- i sin relevante politik til beskyttelse af privatlivets fred rettidigt (dvs. i første omgang i et udkast til en politik til beskyttelse af privatlivets fred, som indgives sammen med anmeldelsen, hvis der er tale om en indledende selvcertificering, og ellers i en endelig og i påkommende tilfælde offentliggjort politik til beskyttelse af privatlivets fred) har angivet, at den tilslutter sig principperne, og har indsat et hyperlink til ministeriets websted for databeskyttelsesrammen (f.eks. hjemmesiden eller webadressen for listen over deltagere i databeskyttelsesrammen),
- i sin relevante politik til beskyttelse af privatlivets fred rettidigt har angivet alle de 12 øvrige elementer, der er opregnet i princippet om oplysningspligt (f.eks. at de berørte EU-borgere på visse betingelser kan påberåbe sig bindende voldgift, kravet om, at personoplysninger skal videregives som svar på lovlige anmodninger fra offentlige myndigheder, herunder for at opfylde kravene med hensyn til den nationale sikkerhed eller retshåndhævelse, og dens ansvar i tilfælde af videreoverførsel til tredjemand),
- har angivet det specifikke lovbestemte organ, der har kompetence til at behandle klager over organisationen vedrørende mulig illoyal eller vildledende praksis eller overtrædelser af gældende love eller bestemmelser om beskyttelse af privatlivets fred (og som er anført i principperne eller i et fremtidigt bilag til principperne),
- har angivet ethvert program til beskyttelse af privatlivets fred, som organisationen deltager i,
- har angivet, hvorvidt den relevante metode (dvs. de kontrolprocedurer, som organisationen skal iværksætte) til kontrol af overholdelsen af principperne er "selvevaluering" (dvs. intern kontrol) eller "ekstern kontrol af overholdelsen" (dvs. tredjemandskontrol), og hvis den har angivet den relevante metode som ekstern kontrol af overholdelsen, om den har angivet den tredjemand, der har foretaget kontrollen,
- har angivet den passende uafhængige klageinstans, der kan behandle klager indgivet i henhold til principperne og sikre de berørte personer passende gratis klageadgang.
 - Hvis organisationen har valgt en uafhængig klageinstans, der stilles til rådighed af et organ til alternativ tvistbilæggelse i den private sektor, har den i sin relevante politik til beskyttelse af privatlivets fred indsat et hyperlink til eller webadressen på det relevante websted eller klageformularen for den instans, der kan behandle uløste klager indgivet i henhold til principperne.
 - Hvis organisationen enten er forpligtet til (dvs. med hensyn til oplysninger om menneskelige ressourcer, der overføres fra EU til brug inden for rammerne af et ansættelsesforhold) eller har valgt at samarbejde med de kompetente databeskyttelsesmyndigheder i forbindelse med undersøgelsen og behandlingen af klager indgivet i henhold til principperne, har den angivet, at den vil samarbejde med databeskyttelsesmyndighederne og rette sig efter deres anbefalinger om at iværksætte specifikke foranstaltninger for at overholde principperne.

- Ministeriet vil ligeledes kontrollere, at organisationens anmeldelse om selvcertificering er i overensstemmelse med dens relevante politik(ker) til beskyttelse af privatlivets fred. Hvis en organisation, som foretager selvcertificering, ønsker at lade certificeringen dække en eller flere af sine amerikanske enheder eller et eller flere af sine amerikanske datterselskaber, som har særskilte, relevante politikker til beskyttelse af privatlivets fred, vil ministeriet også gennemgå sådanne dækkede enheders eller datterselskabers relevante politikker til beskyttelse af privatlivets fred for at sikre, at de omfatter alle de elementer, der er fastsat i princippet om oplysningspligt.
- Ministeriet vil samarbejde med lovbestemte organer (f.eks. FTC og transportministeriet) for at kontrollere, at organisationerne er underlagt det relevante lovbestemte organs jurisdiktion, som er angivet i deres anmeldelser om selvcertificering, hvis ministeriet har grund til at betvivle, at de er underlagt denne jurisdiktion.
- Ministeriet vil samarbejde med organer til alternativ tvistbilæggelse i den private sektor for at kontrollere, at organisationerne er aktivt registreret ved den uafhængige klageinstans, der er angivet i deres anmeldelse om selvcertificering, og samarbejde med disse organer om at kontrollere, at organisationerne er aktivt registreret med henblik på den eksterne kontrol af overholdelsen, der er angivet i deres anmeldelse om selvcertificering, såfremt disse organer tilbyder begge tjenester.
- Ministeriet vil samarbejde med den tredjemand, som ministeriet har udvalgt til at fungere som depotinstitution for de midler, der indsamles via gebyret til panelet af databeskyttelsesmyndigheder (dvs. det årlige gebyr til dækning af panelet af databeskyttelsesmyndigheders driftsomkostninger), for at kontrollere, at organisationerne har betalt dette gebyr for det relevante år, såfremt organisationerne har anført databeskyttelsesmyndighederne som den relevante uafhængige klageinstans.
- Ministeriet vil samarbejde med den tredjemand, som ministeriet har udvalgt til at forvalte voldgiftssager i henhold til — og til at administrere den voldgiftsfond, der er omhandlet i — bilag I til principperne, for at kontrollere, at organisationerne har bidraget til denne voldgiftsfond.
- Hvis ministeriet konstaterer problemer i forbindelse med undersøgelsen af organisationernes anmeldelser om selvcertificering, vil det underrette dem om, at de skal afhjælpe alle sådanne problemer inden for den af ministeriet fastsatte passende tidsfrist ⁽²⁾. Ministeriet vil endvidere oplyse dem om, at manglende svar inden for de af ministeriet fastsatte tidsfrister eller manglende indsendelse af anmeldelsen om selvcertificering i overensstemmelse med ministeriets procedurer af andre årsager vil føre til, at de pågældende anmeldelser om selvcertificering anses for at være opgivet, og at FTC, transportministeriet eller andre relevante statslige organer kan træffe håndhævelsesforanstaltninger over for en organisation, der afgiver urigtige oplysninger om organisationens deltagelse i eller overholdelse af principperne i EU-USA-databeskyttelsesrammen. Ministeriet vil underrette organisationerne ud fra de kontaktoplysninger, som organisationerne har givet ministeriet.

Fremme af samarbejdet med alternative tvistbilæggesorganer, som tilbyder principrelaterede tjenester

- Ministeriet vil samarbejde med organer til alternativ tvistbilæggelse i den private sektor, der stiller uafhængige klageinstanser til rådighed med henblik på at behandle uløste klager, der indgives i henhold til principperne, for at kontrollere, at de som minimum opfylder kravene i det supplerende princip om bilæggelse af tvister og håndhævelse. Ministeriet kontrollerer, at de:
 - angiver oplysninger om principperne og om de tjenester, de tilbyder under EU-USA-databeskyttelsesrammen, på deres offentlige websteder. Disse oplysninger skal omfatte: 1) oplysninger om eller et hyperlink til kravene vedrørende uafhængige klageinstanser i henhold til principperne, 2) et hyperlink til ministeriets websted for databeskyttelsesrammen, 3) oplysninger om, at deres tvistbilægges tjenester under EU-USA-databeskyttelsesrammen er gratis for registrerede, 4) oplysninger om indgivelse af principrelaterede klager, 5) oplysninger om tidsrammen for behandling af klager vedrørende principperne og 6) oplysninger om de forskellige potentielle retsmidler. Ministeriet vil i god tid underrette organerne om væsentlige ændringer i ministeriets tilsyn med og forvaltning af databeskyttelsesrammen, hvis sådanne ændringer er nært forestående eller allerede er foretaget, og sådanne ændringer er relevante for den rolle, som organerne spiller under EU-USA-databeskyttelsesrammen.

⁽²⁾ Med hensyn til recertificering forventes det f.eks., at organisationerne afhjælper alle problemer inden for 45 dage, medmindre ministeriet angiver en anden passende frist.

- offentliggør en årlig rapport med aggregeret statistik over deres tvistbilæggelsestjenester. Den årlige rapport skal indeholde oplysninger om: 1) det samlede antal principrelaterede klager modtaget i rapporteringsåret, 2) typen af modtagne klager, 3) kvalitetsmål for tvistbilæggelse såsom klagebehandlingstid og 4) resultaterne af de modtagne klager, navnlig antal og typer retsmidler eller pålagte sanktioner. Ministeriet vil opstille specifikke, supplerende retningslinjer for organerne om, hvilke oplysninger de skal afgive i de årlige rapporter, som uddyber disse krav (f. eks. en liste over de specifikke kriterier, som en klage skal opfylde for at kunne anses for en principrelateret klage med henblik på den årlige rapport) og angiver andre typer oplysninger, de skal afgive (f.eks. hvis organet også tilbyder en principrelateret kontroltjeneste, en beskrivelse af, hvorledes organet undgår faktiske eller potentielle interessekonflikter i situationer, hvor det leverer både kontroltjenester og tvistbilæggelsestjenester til en organisation). Det vil ligeledes fremgå af ministeriets supplerende retningslinjer, hvornår organernes årlige rapporter skal offentliggøres for de relevante rapporteringsperioder.

Opfølgningsindsats over for organisationer, der ønsker at blive eller er blevet fjernet fra listen over deltagere i databeskyttelsesrammen

- Hvis en organisation ønsker at træde ud af EU-USA-databeskyttelsesrammen, vil ministeriet kræve, at organisationen fjerner enhver henvisning til EU-USA-databeskyttelsesrammen, der lader formode, at den fortsat deltager i EU-USA-databeskyttelsesrammen, og at den kan modtage personoplysninger i henhold til EU-USA-databeskyttelsesrammen, fra alle relevante politikker til beskyttelse af privatlivets fred (jf. beskrivelsen af ministeriets tilsagn om at søge efter falske påstande om deltagelse). Ministeriet vil ligeledes kræve, at organisationen udfylder og indsender et spørgeskema til ministeriet for at kontrollere:
 - dens ønske om at trække sig ud,
 - hvad den vil gøre med de personoplysninger, som den modtog i henhold til EU-USA-databeskyttelsesrammen, mens den deltog i EU-USA-databeskyttelsesrammen: a) Vil den beholde oplysningerne, fortsætte med at anvende principperne på oplysningerne og hvert år bekræfte over for ministeriet, at den fortsat vil anvende principperne på oplysningerne? b) Vil den beholde oplysningerne og sikre "tilstrækkelig" beskyttelse af oplysningerne på en anden godkendt måde? c) Eller vil den tilbagesende eller slette alle oplysningerne inden en bestemt dato? og
 - hvem der vil fungere som fast kontaktpunkt for principrelaterede spørgsmål.
- Hvis en organisation vælger a) som beskrevet umiddelbart ovenfor, vil ministeriet desuden kræve, at den hvert år efter udtrædelsen (dvs. på den første årsdag for udtrædelsen og på alle efterfølgende årssdage, medmindre og indtil organisationen enten sikrer en "tilstrækkelig" beskyttelse af sådanne oplysninger på en anden godkendt måde eller tilbagesender eller sletter alle sådanne oplysninger og underretter ministeriet herom) udfylder et spørgeskema og indsender det til ministeriet, for at kontrollere, hvad den har gjort med disse personoplysninger, hvad den vil gøre med de personoplysninger, som den fortsat beholder, og hvem der vil fungere som fast kontaktpunkt for principrelaterede spørgsmål.
- Hvis en organisation har ladet sin selvcertificering udløbe (dvs. ikke har indsendt sin årlige recertificeringsanmeldelse om tilslutning til principperne eller er blevet fjernet fra listen over deltagere i databeskyttelsesrammen af andre årsager såsom udtrædelse), vil ministeriet pålægge den at udfylde et spørgeskema og indsende det til ministeriet for at kontrollere, om organisationen ønsker at træde ud eller foretage recertificering,
 - og hvis den ønsker at træde ud, yderligere kontrollere, hvad den vil gøre med de personoplysninger, som den har modtaget i henhold til EU-USA-databeskyttelsesrammen, mens den deltog i databeskyttelsesrammen (jf. tidligere beskrivelse af det, som en organisation skal kontrollere, hvis den ønsker at træde ud),
 - og hvis den agter at foretage recertificering, yderligere kontrollere, at den i den periode, hvor dens certificering var udløbet, anvendte principperne på personoplysninger modtaget under EU-USA-databeskyttelsesrammen, og præcisere, hvilke skridt den vil tage for at afhjælpe de uløste problemer, der har forsinket recertificeringen.

- Hvis en organisation fjernes fra listen over deltagere i databeskyttelsesrammen af en af følgende årsager: a) udtrædelse af EU-USA-databeskyttelsesrammen, b) manglende indsendelse af den årlige recertificeringsanmeldelse om dens tilslutning til principperne (dvs. at organisationen enten påbegyndte, men ikke afsluttede den årlige recertificeringsproces rettidigt, eller slet ikke påbegyndte den årlige recertificeringsproces), eller c) "vedvarende overtrædelse", sender ministeriet en meddelelse til de(n) kontakt(er), der er angivet i organisationens anmeldelse om selvcertificering, med angivelse af årsagen til fjernelsen og en forklaring om, at den skal ophøre med eksplicit eller implicit at hævde, at den deltager i eller overholder principperne i EU-USA-databeskyttelsesrammen, og at den kan modtage personoplysninger i henhold til EU-USA-databeskyttelsesrammen. I denne meddelelse, som også kan indeholde andre oplysninger, der er specifikke for årsagen til fjernelsen, angives det, at FTC, transportministeriet eller et andet relevant statsligt organ kan træffe håndhævelsesforanstaltninger over for organisationer, der afgiver urigtige oplysninger om deres deltagelse i eller overholdelse af principperne i EU-USA-databeskyttelsesrammen, herunder hvis de oplyser, at de deltager i EU-USA-databeskyttelsesrammen efter at være blevet fjernet fra listen over deltagere i databeskyttelsesrammen.

Søgning efter og håndtering af falske påstande om deltagelse i databeskyttelsesrammen

- Når en organisation: a) træder ud af EU-USA-databeskyttelsesrammen, b) ikke indsender den årlige recertificeringsanmeldelse om dens tilslutning til principperne (dvs. at den enten påbegyndte, men ikke afsluttede den årlige recertificeringsproces rettidigt, eller slet ikke påbegyndte den årlige recertificeringsproces), c) fjernes fra listen over deltagere i EU-USA-databeskyttelsesrammen, navnlig for "vedvarende overtrædelse", eller d) ikke foretager den indledende selvcertificering af dens tilslutning til principperne (dvs. at den påbegyndte, men ikke afsluttede den indledende selvcertificeringsproces rettidigt), vil ministeriet ex officio kontrollere, at ingen af organisationens relevante offentliggjorte politikker til beskyttelse af privatlivets fred indeholder henvisninger til EU-USA-databeskyttelsesrammen, der lader formode, at organisationen deltager i databeskyttelsesrammen, og at den kan modtage personoplysninger i henhold til EU-USA-databeskyttelsesrammen. Hvis ministeriet finder sådanne henvisninger, vil det underrette organisationen om, at ministeriet i påkommende tilfælde vil henvise sagen til det relevante organ med henblik på eventuel håndhævelse, hvis organisationen bliver ved med at afgive urigtige oplysninger om dens deltagelse i EU-USA-databeskyttelsesrammen. Ministeriet underretter organisationen via de kontaktoplysninger, som organisationen har stillet til rådighed for ministeriet, eller om nødvendigt på anden passende måde. Hvis organisationen hverken fjerner henvisningerne eller foretager selvcertificering af dens tilslutning til principperne i EU-USA-databeskyttelsesrammen i overensstemmelse med ministeriets procedurer, vil ministeriet ex officio henvise sagen til FTC, transportministeriet eller et andet relevant håndhævelsesorgan eller træffe andre passende foranstaltninger for at sikre, at certificeringsmærket for EU-USA-databeskyttelsesrammen anvendes korrekt.
- Ministeriet vil træffe andre foranstaltninger for at identificere falske påstande om deltagelse i EU-USA-databeskyttelsesrammen og uretmæssig brug af certificeringsmærket for EU-USA-databeskyttelsesrammen, herunder hidrørende fra organisationer, der i modsætning til de organisationer, der er beskrevet umiddelbart ovenfor, aldrig har påbegyndt selvcertificeringsprocessen (dvs. foretage passende internetsøgninger for at identificere henvisninger til EU-USA-databeskyttelsesrammen i organisationernes politikker til beskyttelse af privatlivets fred). Hvis ministeriet ved disse foranstaltninger identificerer falske påstande om deltagelse i EU-USA-databeskyttelsesrammen og uretmæssig brug af certificeringsmærket for EU-USA-databeskyttelsesrammen, underretter ministeriet organisationen om, at det i påkommende tilfælde vil henvise sagen til det relevante organ med henblik på eventuel håndhævelse, hvis organisationen bliver ved med at afgive urigtige oplysninger om dens deltagelse i EU-USA-databeskyttelsesrammen. Ministeriet underretter organisationen via de kontaktoplysninger, som organisationen har stillet til rådighed for ministeriet, hvis den har stillet sådanne oplysninger til rådighed, og ellers om nødvendigt på anden passende måde. Hvis organisationen hverken fjerner henvisningerne eller foretager selvcertificering af dens tilslutning til principperne i EU-USA-databeskyttelsesrammen i overensstemmelse med ministeriets procedurer, vil ministeriet ex officio henvise sagen til FTC, transportministeriet eller et andet relevant håndhævelsesorgan eller træffe andre passende foranstaltninger for at sikre, at certificeringsmærket for EU-USA-databeskyttelsesrammen anvendes korrekt.
- Ministeriet vil straks gennemgå og behandle specifikke seriøse klager over falske påstande om deltagelse i EU-USA-databeskyttelsesrammen, som ministeriet modtager (f.eks. klager modtaget fra databeskyttelsesmyndighederne, uafhængige klageinstanser, der stilles til rådighed af organer til alternativ tvistbilæggelse i den private sektor, registrerede, virksomheder i EU og USA og andre tredjeparter).
- Ministeriet kan træffe andre passende korrigerende foranstaltninger. En organisation, der afgiver urigtige oplysninger til ministeriet, kan retsforfølges efter False Statements Act (18 U.S.C. § 1001).

Gennemførelse af regelmæssige ex officio-kontroller og -vurderinger af programmet for databeskyttelse

- Ministeriet vil løbende træffe foranstaltninger for at overvåge de deltagende organisationers effektive overholdelse af EU-USA-databeskyttelsesrammen for at identificere problemer, som kan berettige opfølgning. Ministeriet vil navnlig foretage rutinemæssig ex officio-stikprøvekontrol af tilfældigt udvalgte organisationer under EU-USA-databeskyttelsesrammen samt ad hoc-stikprøvekontrol af specifikke organisationer under EU-USA-databeskyttelsesrammen, når der konstateres potentielle overtrædelser (f.eks. potentielle overtrædelser, som tredjemand har gjort ministeriet opmærksom på), for at kontrollere: a) at det eller de kontaktpunkter, der er ansvarlige for behandlingen af klager, anmodninger om indsigt og andre spørgsmål, der opstår i forbindelse med EU-USA-databeskyttelsesrammen, er tilgængelige, b) at organisationens offentlige politik til beskyttelse af privatlivets fred i påkommende tilfælde er let tilgængelig for offentligheden, både på organisationens offentlige websted og via et hyperlink på listen over deltagere i databeskyttelsesrammen, c) at organisationens politik til beskyttelse af privatlivets fred fortsat opfylder de selvcertificeringskrav, der er beskrevet i principperne, og d) at den uafhængige klageinstans, som organisationen har udpeget, er til rådighed til at behandle klager indgivet under EU-USA-databeskyttelsesrammen. Ministeriet vil endvidere aktivt holde øje med rapporter i nyhederne, der giver troværdig dokumentation for deltagende organisationers manglende overholdelse.
- Som led i kontrollen af overholdelsen vil ministeriet kræve, at organisationerne under EU-USA-databeskyttelsesrammen udfylder et detaljeret spørgeskema og indsender det til ministeriet: a) når ministeriet har modtaget specifikke seriøse klager over en organisations manglende overholdelse af principperne, b) når en organisation ikke besvarer forespørgsler fra ministeriet om oplysninger om EU-USA-databeskyttelsesrammen på tilfredsstillende vis, eller c) når der er troværdig dokumentation for, at en organisation ikke opfylder sine forpligtelser under EU-USA-databeskyttelsesrammen. Hvis ministeriet har sendt et sådant detaljeret spørgeskema til en organisation, og organisationen ikke besvarer spørgeskemaet tilfredsstillende, underretter ministeriet organisationen om, at ministeriet i påkommende tilfælde vil henvise sagen til det relevante organ med henblik på eventuel håndhævelse, hvis ikke ministeriet modtager et rettidigt og tilfredsstillende svar fra organisationen. Ministeriet underretter organisationen via de kontaktoplysninger, som organisationen har stillet til rådighed for ministeriet, eller om nødvendigt på anden passende måde. Hvis ikke organisationen giver et rettidigt og tilfredsstillende svar, vil ministeriet ex officio henvise sagen til FTC, transportministeriet eller et andet relevant håndhævelsesorgan eller træffe andre passende foranstaltninger for at sikre overholdelse. Ministeriet vil, når det er relevant, drøfte denne kontrol af overholdelsen med de kompetente databeskyttelsesmyndigheder.
- Ministeriet vil regelmæssigt vurdere forvaltningen af og tilsynet med programmet for databeskyttelse for at sikre, at overvågningsindsatsen, herunder enhver sådan indsats, der gøres ved hjælp af søgeværktøjer (f.eks. for at kontrollere, om der er døde links til de deltagende organisationers politikker til beskyttelse af privatlivets fred), er tilstrækkelig til at tackle eksisterende problemer og nye problemer, efterhånden som de opstår.

Skræddersyet websted for databeskyttelsesrammen til bestemte målgrupper

Ministeriet vil skræddersy webstedet for databeskyttelsesrammen til følgende målgrupper: privatpersoner og virksomheder i EU, amerikanske virksomheder og databeskyttelsesmyndigheder. Medtagelsen af materiale, der er direkte henvendt til privatpersoner og virksomheder i EU, vil øge gennemsigtigheden på flere måder. Med hensyn til privatpersoner i EU vil der blive redegjort klart for: 1) privatpersoner i EU's rettigheder under EU-USA-databeskyttelsesrammen, 2) de klageinstanser, som privatpersoner i EU har adgang til, når de mener, at en organisation ikke har opfyldt sin forpligtelse til at overholde principperne, og 3) hvor man kan finde oplysninger om en organisations selvcertificering under EU-USA-databeskyttelsesrammen. Med hensyn til EU-virksomheder vil det blive lettere at kontrollere: 1) om en organisation deltager i EU-USA-databeskyttelsesrammen, 2) den type oplysninger, der er dækket af en organisations selvcertificering under EU-USA-databeskyttelsesrammen, 3) den politik til beskyttelse af privatlivets fred, som de dækkede oplysninger er omfattet af, og 4) den metode, som organisationen anvender til at verificere sin tilslutning til principperne. Med hensyn til amerikanske virksomheder vil der blive redegjort klart for: 1) fordelene ved at deltage i EU-USA-databeskyttelsesrammen, 2) hvordan man tilslutter sig EU-USA-databeskyttelsesrammen, og hvordan man foretager recertificering og træder ud af EU-USA-databeskyttelsesrammen, og 3) hvordan USA forvalter og håndhæver EU-USA-databeskyttelsesrammen. Medtagelsen af materiale, der er rettet direkte mod databeskyttelsesmyndighederne (f.eks. oplysninger om ministeriets særlige kontaktpunkt for databeskyttelsesmyndigheder og et hyperlink til principrelateret indhold på FTC's websted), vil fremme både samarbejdet og gennemsigtigheden. Ministeriet vil også på ad hoc-basis samarbejde med Kommissionen og Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") for at udvikle yderligere aktuelt materiale (f.eks. svar på ofte stillede spørgsmål) til brug på webstedet for databeskyttelsesrammen, hvor sådanne oplysninger vil fremme en effektiv forvaltning og overvågning af programmet for databeskyttelse.

Fremme af samarbejdet med databeskyttelsesmyndighederne

For at øge mulighederne for samarbejde med databeskyttelsesmyndighederne vil ministeriet udpege et særligt kontaktpunkt i ministeriet, der skal være bindeled mellem ministeriet og databeskyttelsesmyndighederne. Hvis en databeskyttelsesmyndighed mener, at en organisation under EU-USA-databeskyttelsesrammen ikke overholder principperne, herunder på baggrund af en klage fra en privatperson i EU, kan databeskyttelsesmyndigheden henvende sig til det særlige kontaktpunkt i ministeriet med henblik på en yderligere kontrol af organisationen. Ministeriet vil gøre sit yderste for at fremme afgørelsen af klager i samarbejde med organisationen i EU-USA-databeskyttelsesrammen. Ministeriet vil informere databeskyttelsesmyndigheden om status senest 90 dage efter modtagelsen af en klage. Det særlige kontaktpunkt vil ligeledes få henvist sager om organisationer, der fremsætter falske påstande om deltagelse i EU-USA-databeskyttelsesrammen. Det særlige kontaktpunkt vil identificere alle de henvisninger, som ministeriet modtager fra databeskyttelsesmyndighederne, og i forbindelse med den nedenfor beskrevne fælles undersøgelse vil ministeriet udarbejde en rapport, hvor de klager, ministeriet modtager hvert år, analyseres i aggregeret form. Det særlige kontaktpunkt vil bistå databeskyttelsesmyndigheder, der søger oplysninger om en specifik organisations selvcertificering eller tidligere deltagelse i EU-USA-databeskyttelsesrammen, og det særlige kontaktpunkt vil besvare databeskyttelsesmyndighedernes forespørgsler om gennemførelsen af specifikke krav under EU-USA-databeskyttelsesrammen. Ministeriet vil derudover samarbejde med Kommissionen og Databeskyttelsesrådet om de proceduremæssige og administrative aspekter af panelet af databeskyttelsesmyndigheder, herunder fastlæggelse af passende procedurer for fordelingen af de midler, der indsamles via gebyret til panelet af databeskyttelsesmyndigheder. Vi har forstået, at Kommissionen vil samarbejde med ministeriet om at fremme løsningen af eventuelle problemer, der måtte opstå i forbindelse med disse procedurer. Ministeriet vil ligeledes give databeskyttelsesmyndighederne materiale om EU-USA-databeskyttelsesrammen, som de kan offentliggøre på deres egne websteder for at øge gennemsigtigheden for privatpersoner og virksomheder i EU. Øget kendskab til EU-USA-databeskyttelsesrammen og rettigheder og forpligtelser under databeskyttelsesrammen bør gøre det lettere at identificere problemer, efterhånden som de opstår, således at de kan tackles på passende vis.

Opfyldelse af forpligtelserne i henhold til bilag I til principperne

Ministeriet vil opfylde sine forpligtelser i henhold til bilag I til principperne, herunder føre en liste over voldgiftsmænd, der er valgt i samarbejde med Kommissionen på grundlag af deres uafhængighed, integritet og ekspertviden, og det vil efter behov støtte den tredjemand, som ministeriet har udvalgt til at forvalte voldgiftssager i henhold til — og til at administrere den voldgiftsfond, der er omhandlet i — bilag I til principperne ⁽³⁾. Ministeriet vil samarbejde med tredjemanden for bl.a. at kontrollere, at tredjemanden har et websted med retningslinjer om voldgiftsproceduren, herunder om: 1) indledning af proceduren og fremlæggelse af dokumenter, 2) listen over voldgiftsmænd, som ministeriet fører, og hvordan voldgiftsmænd udvælges fra listen, 3) de gældende voldgiftsprocedurer og den adfærdskodeks for voldgiftsmænd, som ministeriet og Kommissionen har vedtaget ⁽⁴⁾ og 4) opkrævning og betaling af voldgiftsgebyrer. Ministeriet vil i samarbejde med tredjemanden regelmæssigt evaluere fondens drift, herunder behovet for at justere bidragene eller maksimumsbeløbene for voldgiftsomkostningerne, og vil bl.a. se på antallet af voldgiftssager, voldgiftsomkostningerne og behandlingstiden ud fra den holdning, at organisationerne under EU-USA-databeskyttelsesrammen ikke må pålægges en urimelig stor økonomisk byrde. Ministeriet underretter Kommissionen om resultatet af disse evalueringer, som udføres i samarbejde med tredjeparten, og underretter på forhånd Kommissionen om eventuelle justeringer af bidragenes størrelse.

Fælles undersøgelser af, hvordan EU-USA-databeskyttelsesrammen fungerer

Ministeriet og andre organer vil i påkommende tilfælde regelmæssigt afholde møder med Kommissionen, interesserede databeskyttelsesmyndigheder og relevante repræsentanter fra Databeskyttelsesrådet, hvor ministeriet vil gøre status over EU-USA-databeskyttelsesrammen. Møderne vil omfatte drøftelser af aktuelle spørgsmål om programmet for databeskyttelses funktion, gennemførelse, overvågning og håndhævelse. Hvor det er relevant, kan møderne omfatte drøftelse af relaterede emner, såsom andre dataoverførselsmekanismer, der er omfattet af sikkerhedsforanstaltningerne under EU-USA-databeskyttelsesrammen.

⁽³⁾ Ministeriet har udvalgt International Centre for Dispute Resolution ("ICDR"), den internationale afdeling af American Arbitration Association ("AAA") (samlet benævnt "ICDR-AAA"), til at forvalte voldgiftssager i henhold til — og til at administrere den voldgiftsfond, der er omhandlet i — bilag I til principperne.

⁽⁴⁾ Den 15. september 2017 enedes ministeriet og Kommissionen om vedtagelsen af et sæt voldgiftsregler for bindende voldgiftsprocedurer, der er beskrevet i bilag I til principperne, samt en adfærdskodeks for voldgiftsmænd, der er i overensstemmelse med almindeligt anerkendte etiske standarder for handelsvoldgiftsmænd og bilag I til principperne. Ministeriet og Kommissionen blev enige om at tilpasse voldgiftsreglerne og adfærdskodeksen, så de afspejler ajourføringer i henhold til EU-USA-databeskyttelsesrammen, og ministeriet vil samarbejde med ICDR-AAA om at foretage disse ajourføringer.

Opdatering af lovgivning

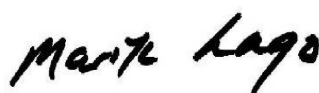
Ministeriet vil bestræbe sig på så vidt muligt at underrette Kommissionen om den materielle udvikling inden for den amerikanske lovgivning, såfremt den er relevant i forhold til EU-USA-databeskyttelsesrammen for så vidt angår databeskyttelsen og de begrænsninger og garantier, der gælder for amerikanske myndigheders adgang til og efterfølgende anvendelse af personoplysninger.

De amerikanske statslige myndigheders adgang til personoplysninger

USA har udstedt præsidentielt dekret 14086 (Executive Order 14086) med titlen "Enhancing Safeguards for United States Signals Intelligence Activities" og 28 CFR part 201 om ændring af justitsministeriets forordninger med henblik på oprettelse af Data Protection Review Court ("DPRC"), som sikrer omfattende beskyttelse af personoplysninger i forbindelse med statslige myndigheders adgang til oplysninger til nationale sikkerhedsformål. Denne beskyttelse omfatter: en styrkelse af sikkerhedsforanstaltningerne med hensyn til privatlivets fred og de borgerlige frihedsrettigheder for at sikre, at de amerikanske signalefterretningsaktiviteter er nødvendige og forholdsmæssige i forfølgelsen af definerede nationale sikkerhedsmål, oprettelse af en ny klageinstans med uafhængig og bindende kompetence og forbedring af det eksisterende strenge tilsyn i flere niveauer med amerikanske signalefterretningsaktiviteter. Med denne beskyttelse kan personer i EU indgive klager til en ny klageinstans i flere niveauer, som omfatter en uafhængig DPRC, der består af personer valgt uden for de amerikanske statslige myndigheder, og som har fuld beføjelse til at træffe afgørelse om krav og om nødvendigt om direkte afhjælpende foranstaltninger. Ministeriet vil føre et register over EU-borgere, der indgiver en klage, som opfylder kravene, i henhold til præsidentielt dekret 14086 og 28 CFR part 201. Ministeriet vil fem år efter datoen for dette brev og derefter hvert femte år kontakte de relevante organer for at indhente oplysninger om, hvorvidt oplysninger vedrørende behandlingen af klager, der opfylder kravene, eller behandlingen af eventuelle anmodninger om behandling indgivet til DPRC er blevet afklassificeret. Hvis sådanne oplysninger er blevet afklassificeret, vil ministeriet samarbejde med den relevante databeskyttelsesmyndighed for at underrette den pågældende EU-borger herom. Disse forbedringer bekræfter, at personoplysninger fra EU, der overføres til USA, vil blive behandlet på en måde, der er i overensstemmelse med EU's retlige krav med hensyn til statslige myndigheders adgang til oplysninger.

På grundlag af principperne, præsidentielt dekret 14086, 28 CFR part 201 og de ledsagende breve og materialer, herunder ministeriets tilsagn vedrørende forvaltningen af og tilsynet med programmet for databeskyttelse, forventer vi, at Kommissionen vil vurdere, at EU-USA-databeskyttelsesrammen giver en tilstrækkelig beskyttelse i henhold til EU-retten, og at der fortsat vil blive overført oplysninger fra EU til organisationer, der deltager i EU-USA-databeskyttelsesrammen. Derudover forventer vi, at overførslerne til amerikanske organisationer på grundlag af EU's standardkontraktbestemmelser eller EU's bindende virksomhedsregler vil blive lettet yderligere i kraft af disse ordninger.

Med venlig hilsen



Marisa LAGO

BILAG IV



UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

Den 9. juni 2023

Didier Reynders
Kommissær for retlige anliggender
Europa-Kommissionen
Rue de la Loi / Wetstraat 200
1049 Bruxelles/Brussel
Belgien

Kære kommissær Didier Reynders,

United States Federal Trade Commission ("FTC") glæder sig over at få lejlighed til at redegøre for sin håndhævelsesrolle i forbindelse med principperne i EU-USA-databeskyttelsesrammen. FTC har længe haft fokus på at beskytte forbrugerne og privatlivets fred på tværs af grænser og vil håndhæve de kommercielle aspekter af denne ramme. FTC har varetaget en sådan rolle siden 2000 i forbindelse med safe harbour-rammen mellem USA og EU og senest siden 2016 i forbindelse med EU's og USA's værn om privatlivets fred (EU-USA-privatlivsskjoldet) ⁽¹⁾. Den 16. juli 2020 annullerede Den Europæiske Unions Domstol ("EU-Domstolen") Europa-Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet, der lå til grund for EU-USA-privatlivsskjoldet, på grund af problemer, der ikke vedrørte de kommercielle principper, som FTC håndhævede. USA og Europa-Kommissionen har siden forhandlet sig frem til EU-USA-databeskyttelsesrammen som svar på denne afgørelse fra EU-Domstolen.

Jeg skriver for at bekræfte FTC's tilsagn om at håndhæve principperne i EU-USA-databeskyttelsesrammen stramt. Vi bekræfter navnlig vores tilsagn på tre hovedområder: 1) prioritering af henviste sager og undersøgelser, 2) anmodning om og overvågning af afgørelser og 3) håndhævelsessamarbejde med EU's databeskyttelsesmyndigheder.

I. Indledning

a. FTC's foranstaltninger og strategi for beskyttelse af privatlivets fred

FTC har vide civilretlige håndhævelsesbeføjelser til at fremme forbrugerbeskyttelsen og konkurrencen på det kommercielle område. Inden for rammerne af sine forbrugerbeskyttelsesbeføjelser håndhæver FTC en lang række forskellige love for at beskytte og sikre forbrugeroplysninger og forbrugernes privatliv og sikkerhed. Den vigtigste lov, som FTC håndhæver, FTC

⁽¹⁾ Brev fra formanden, Edith Ramirez, til Věra Jourová, kommissær for retlige anliggender, forbrugere og ligestilling mellem mænd og kvinder i Europa-Kommissionen, hvori der redegøres for Federal Trade Commissions håndhævelse af den nye ordning for EU-USA-privatlivsskjoldet (29.2.2016), findes på <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european>. FTC har også tidligere forpligtet sig til at håndhæve safe harbour-programmet mellem USA og EU. Brev fra Robert Pitofsky, formand for FTC, til John Mogg, direktør for GD for det Indre Marked, Europa-Kommissionen (14.7.2000), findes på <https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission>. Dette brev erstatter disse tidligere tilsagn.

Act, forbyder "illoyal" eller "vildledende" adfærd eller praksis i forbindelse med handel ^(?). FTC håndhæver ligeledes særlige love om beskyttelse af sundhedsoplysninger, kreditoplysninger og andre finansielle oplysninger og om børns onlineoplysninger og har udstedt forordninger til gennemførelse af disse love ^(?).

FTC har også for nylig gennemført en lang række initiativer for at styrke vores arbejde inden for området privatlivets fred. I august 2022 meddelte FTC, at den overvejer regler for at slå ned på skadelig kommerciel overvågning og løs datasikkerhed ⁽⁴⁾. Formålet med projektet er at indsamle omfattende offentlige tilkendegivelser om, hvorvidt FTC bør udstede regler om praksis inden for kommerciel overvågning og datasikkerhed, og hvordan sådanne regler eventuelt skal se ud. Det glæder os, at vi har modtaget bemærkninger fra EU-interessenter om dette og andre initiativer.

Vores "PrivacyCon"-konferencer samler fortsat førende forskere for at drøfte den seneste forskning og de seneste tendenser vedrørende forbrugernes privatliv og sikkerheden af forbrugeroplysninger. Vi har endvidere gjort os bedre til at holde trit med den teknologiske udvikling, der ligger til grund for en stor del af vores arbejde med privatlivets fred, ved at opbygge et stadig større team af teknologer og tværfaglige forskere. Som De ved, fører vi også en fælles dialog med Dem og Deres kolleger i Europa-Kommissionen, hvor vi bl.a. ser på privatlivsrelaterede emner såsom skjulte mønstre og forretningsmodeller, der er kendetegnet ved alt for omfattende dataindsamling ⁽⁵⁾. Vi har desuden for nylig udsendt en rapport til Kongressen om de skader, der er forbundet med brugen af kunstig intelligens ("AI"), hvor vi ser på de onlinerelaterede skader, som Kongressen har identificeret. Denne rapport gav anledning til bekymring med hensyn til unøjagtighed, forudindtagethed, forskelsbehandling og skred i den kommercielle overvågning ⁽⁶⁾.

b. Amerikansk retsbeskyttelse til gavn for EU-forbrugere

EU-USA-databeskyttelsesrammen fungerer inden for rammerne af de generelle amerikanske regler om beskyttelse af privatlivets fred, som også beskytter forbrugerne på forskellige måder. Forbuddet i FTC Act mod illoyal eller vildledende adfærd eller praksis beskytter ikke kun amerikanske forbrugere mod amerikanske virksomheder, da loven ligeledes omfatter praksis, der 1) forårsager eller vil kunne forårsage skade i USA, som med rimelighed kan forudses, eller 2) involverer den faktiske adfærd i USA. FTC kan desuden anvende alle tilgængelige retsmidler til beskyttelse af amerikanske forbrugere til at beskytte udenlandske forbrugere ⁽⁷⁾.

FTC håndhæver ligeledes andre relevante love, hvis bestemmelser også finder anvendelse på ikkeamerikanske forbrugere, f. eks. Children's Online Privacy Protection Act ("COPPA"). I henhold til COPPA skal operatører af websteder og onlinetjenester rettet mod børn eller websteder rettet mod den brede offentlighed, som bevidst indsamler personoplysninger om børn under 13 år, bl.a. underrette forældrene og indhente verificerbart forældresamtykke. USA-baserede websteder og -tjenester, der er omfattet af COPPA og indsamler personoplysninger om udenlandske børn, skal overholde COPPA. Udenlandske websteder og onlinetjenester skal ligeledes overholde COPPA, hvis de henvender sig til

^(?) 15 U.S.C. § 45(a). FTC har ingen kompetence inden for strafferetlig håndhævelse eller nationale sikkerhedsanliggender. De fleste andre statslige foranstaltninger henhører heller ikke under FTC's kompetence. Der er desuden en række undtagelser med hensyn til FTC's kompetence inden for kommercielle aktiviteter, herunder med hensyn til banker, luftfartsselskaber, forsikringsvirksomhed og telekommunikationsudbydere fælles bærertjenester. FTC har heller ikke kompetence over de fleste nonprofitorganisationer, men har kompetence over falske velgørenhedsorganisationer eller andre nonprofitorganisationer, der rent faktisk arbejder med gevinst for øje. FTC har også kompetence over nonprofitorganisationer, der arbejder med gevinst for øje til deres profitsøgende medlemmer, herunder ved at skaffe væsentlige økonomiske fordele til disse medlemmer. I nogle tilfælde falder FTC's kompetence sammen med andre retshåndhævende organers kompetence. Vi har udviklet et tæt forhold til forbunds- og delstatsmyndighederne og samarbejder tæt med disse myndigheder om koordineringen af undersøgelser eller henvisning af sager, når det er relevant.

⁽⁴⁾ Jf. FTC, Privacy and Security, <https://www.ftc.gov/business-guidance/privacy-security>.

⁽⁵⁾ Jf. Press Release, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (11.8.2022), <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices>.

⁽⁶⁾ Jf. den fælles pressemeddelelse fra Didier Reynnders, kommissær for retlige anliggender i Europa-Kommissionen, og Lina Khan, formand for United States Federal Trade Commission (30.3.2022), findes på https://www.ftc.gov/system/files/ftc_gov/pdf/joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

⁽⁶⁾ Jf. Press Release, Fed. Trade Comm'n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (16.6.2022), findes på <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems>.

⁽⁷⁾ 15 U.S.C. § 45(a)(4)(B). Endvidere omfatter "illoyal eller vildledende adfærd eller praksis" adfærd eller praksis, der involverer udenlandsk handel, som i) forårsager eller vil kunne forårsage skade i USA, som med rimelighed kan forudses, eller ii) involverer den faktiske adfærd, der udøves i USA. 15 U.S.C. § 45(a)(4)(A).

børn i USA, eller hvis de bevidst indsamler personoplysninger fra børn i USA. Ud over de amerikanske forbundslove, der håndhæves af FTC, kan der desuden være andre love om forbrugerbeskyttelse, brud på datasikkerheden og beskyttelse af privatlivets fred på forbunds- og delstatsniveau, som sikrer EU-forbrugere yderligere fordele.

c. FTC's håndhævelse

FTC har anlagt sager under både safe harbour-rammen mellem USA og EU og EU-USA-privatlivsskjoldet og fortsatte med at håndhæve EU-USA-privatlivsskjoldet, også efter at EU-Domstolen annullerede den afgørelse om tilstrækkeligheden af beskyttelsesniveauet, der lå til grund for EU-USA-privatlivsskjoldet ⁽⁸⁾. Flere af FTC's seneste klager har indeholdt påstande om, at virksomheder har overtrådt bestemmelserne i EU-USA-privatlivsskjoldet, herunder i sager mod Twitter ⁽⁹⁾, CafePress ⁽¹⁰⁾ og Flo ⁽¹¹⁾. I forbindelse med sagen mod Twitter sikrede FTC 150 mio. USD fra Twitter for selskabets overtrædelse af en tidligere FTC-afgørelse med praksisser, der berørte mere end 140 mio. kunder, herunder overtrædelse af princip 5 i EU-USA-privatlivsskjoldet (dataintegritet og formålsbegrænsning). Derudover indebar handelskommissionens afgørelse, at Twitter skal give brugerne mulighed for at anvende sikre multifaktorgodkendelsesmetoder, der ikke kræver, at brugerne oplyser deres telefonnumre.

I *CafePress* hævdede FTC, at virksomheden undlod at beskytte forbrugernes følsomme oplysninger, dækkede over et større brud på datasikkerheden og krænkede princip 2 (valgfrihed), 4 (sikkerhed) og 6 (indsigt) i EU-USA-privatlivsskjoldet. FTC's afgørelse kræver, at virksomheden erstatter utilstrækkelige godkendelsesforanstaltninger med multifaktorgodkendelse, i det væsentlige begrænser mængden af data, som virksomheden indsamler og opbevarer, krypterer socialsikringsnumre og får tredjemand til at vurdere sine informationssikkerhedsprogrammer og udlevere en kopi heraf til FTC, der kan offentliggøres.

I *Flo* hævdede FTC, at appen til fertilitetssporing videregav brugersundhedsoplysninger til tredjepartsudbydere af dataanalyser efter at have forpligtet sig til at hemmeligholde sådanne oplysninger. FTC's klage vedrørte specifikt virksomhedens interaktion med forbrugere i EU, og at Flo havde overtrådt princip 1 (oplysningspligt), 2 (valgfrihed), 3 (ansvar for videreoverførsel) og 5 (dataintegritet og formålsbegrænsning) i EU-USA-privatlivsskjoldet. I henhold til FTC's afgørelse skal Flo bl.a. underrette de berørte brugere om videregivelsen af deres personoplysninger og pålægge enhver tredjemand, der har modtaget brugernes sundhedsoplysninger, at destruere disse data. Det er vigtigt at bemærke, at FTC's afgørelser beskytter alle forbrugere overalt i verden, som interagerer med en amerikansk virksomhed, og ikke kun de forbrugere, der har indgivet klager.

Mange tidligere sager om håndhævelse af safe harbour-ordningen mellem USA og EU og EU-USA-privatlivsskjoldet involverede organisationer, som havde foretaget den indledende selvcertificering gennem handelsministeriet, men fortsatte med at fremstille sig selv som deltagere uden at foretage den årlige selvcertificering. Andre sager vedrørte falske påstande om deltagelse fra organisationer, der aldrig havde foretaget den indledende selvcertificering gennem handelsministeriet. Vi forventer, at vi i vores proaktive håndhævelsesindsats fremover vil fokusere på de typer af væsentlige overtrædelser af principperne i EU-USA-databeskyttelsesrammen, der blev fremsat påstand om i f.eks. Twitter-, CafePress- og Flo-sagerne. I mellemtiden vil handelsministeriet forvalte og føre tilsyn med selvcertificeringsprocessen, oprette den officielle liste over deltagere i EU-USA-databeskyttelsesrammen og se på andre problemer med påstande om deltagelse i programmet ⁽¹²⁾. Det er vigtigt at bemærke, at FTC kan træffe håndhævelsesforanstaltninger over for organisationer, der hævder at overholde principperne i EU-USA-databeskyttelsesrammen, selv om de ikke foretager den indledende eller årlige selvcertificering gennem handelsministeriet.

⁽⁸⁾ Jf. tillæg A for en liste over FTC-sager under safe harbour og privatlivsskjoldet.

⁽⁹⁾ Jf. Press Release, Fed. Trade Comm'n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (25.5.2022), findes på <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>.

⁽¹⁰⁾ Jf. Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (15.3.2022), findes på <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover>.

⁽¹¹⁾ Jf. Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (22.6.2021), findes på <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>.

⁽¹²⁾ Brev fra Marisa Lago, viceminister for international handel, til Didier Reynders, kommissær for retlige anliggender, Europa-Kommissionen (12. december 2022).

II. Prioritering af henviste sager og undersøgelser

Som inden for safe harbour-rammen mellem USA og EU og EU-USA-privatlivsskjoldet vil FTC give højeste prioritet til sager vedrørende principperne i EU-USA-databeskyttelsesrammen, der henvises fra handelsministeriet og EU-medlemsstaterne. Vi vil ligeledes prioritere sager om manglende overholdelse af principperne i EU-USA-databeskyttelsesrammen, der henvises fra selvregulerende instanser med kompetence inden for beskyttelse af privatlivets fred og andre uafhængige tvistbilæggelsesinstanser.

For at lette EU-medlemsstaternes henvisning af sager under EU-USA-databeskyttelsesrammen har FTC udviklet en standardiseret henvisningsprocedure og vejledning til EU-medlemsstaterne om den type oplysninger, der giver FTC det bedste grundlag for at undersøge en henvist sag. FTC har i denne forbindelse udpeget et kontaktpunkt i FTC for henvisninger fra EU-medlemsstaterne. Det er meget nyttigt, hvis den henvisende myndighed har foretaget en indledende undersøgelse af den påståede overtrædelse og kan samarbejde med FTC om undersøgelsen.

Efter modtagelsen af en sådan henvisning fra handelsministeriet, en EU-medlemsstat, en selvregulerende instans eller en anden uafhængig tvistbilæggelsesinstans kan FTC træffe en række forskellige foranstaltninger i forhold til de henviste sager. Vi kan f.eks. gennemgå organisationens politikker til beskyttelse af privatlivets fred, indhente yderligere oplysninger direkte fra organisationen eller fra tredjemand, følge op over for den henvisende instans, vurdere, om der er et overtrædelsesmønster eller et betydeligt antal berørte forbrugere, vurdere, om den henviste sag vedrører spørgsmål, der henhører under handelsministeriet, vurdere, om det ville være nyttigt at gøre en yderligere indsats for at oplyse markedsdeltagerne, og eventuelt indlede en håndhævelsesprocedure.

Ud over prioriteringen af henviste sager fra handelsministeriet, EU-medlemsstaterne, selvregulerende instanser med kompetence inden for beskyttelse af privatlivets fred eller andre uafhængige tvistbilæggelsesinstanser under EU-USA-databeskyttelsesrammen ⁽¹³⁾ vil FTC på eget initiativ og i relevant omfang undersøge mulige overtrædelser af principperne i EU-USA-databeskyttelsesrammen ved brug af en række redskaber. Som led i FTC's program for undersøgelser af aspekter af privatlivets fred og sikkerhed i relation til kommercielle organisationer har FTC rutinemæssigt undersøgt, om de pågældende enheder havde afgivet oplysninger om EU-USA-privatlivsskjoldet. Hvis enheden havde afgivet sådanne oplysninger, og undersøgelsen viste, at principperne under EU-USA-privatlivsskjoldet tydeligvis var blevet overtrådt, medtog FTC påstande om overtrædelser af EU-USA-privatlivsskjoldet i sine håndhævelsessager. Vi vil fortsætte denne proaktive tilgang, nu med hensyn til principperne i EU-USA-databeskyttelsesrammen.

III. Anmodning om og overvågning af afgørelser

FTC bekræfter ligeledes, at den vil anmode om og overvåge håndhævelsesafgørelser for at sikre, at principperne i EU-USA-databeskyttelsesrammen overholdes. Vi vil stille krav om, at principperne i EU-USA-databeskyttelsesrammen overholdes, gennem en række forskellige relevante bestemmelser om forbud i fremtidige FTC-afgørelser under databeskyttelsesrammen. Overtrædelser af FTC's administrative afgørelser kan resultere i idømmelse af civile retlige sanktioner på op til 50 120 USD for hver overtrædelse eller 50 120 USD pr. dag, hvis overtrædelsen fortsætter ⁽¹⁴⁾, hvilket i tilfælde af en praksis, der berører mange forbrugere, kan løbe op i flere millioner USD. Enhver forligsafgørelse vil ligeledes indeholde bestemmelser om selvrapportering og overholdelse. Enheder omfattet af forligsafgørelser skal opbevare dokumentation for deres overholdelse i et nærmere bestemt antal år. Afgørelserne skal ligeledes formidles til ansatte med ansvar for overholdelsen af afgørelser.

FTC overvåger systematisk overholdelsen af eksisterende afgørelser vedrørende principperne i EU-USA-privatlivsskjoldet, som den gør med alle sine afgørelser, og den anlægger sager med henblik på håndhævelse af disse afgørelser, når det er nødvendigt ⁽¹⁵⁾. Det er vigtigt at understrege, at FTC-afgørelser fortsat vil beskytte alle forbrugere verden over, som har været i kontakt med en virksomhed, og ikke kun de forbrugere, der har indgivet klager. Endelig vil FTC føre en onlineliste over virksomheder omfattet af afgørelser truffet i forbindelse med håndhævelsen af principperne i EU-USA-databeskyttelsesrammen ⁽¹⁶⁾.

⁽¹³⁾ Selv om FTC ikke behandler eller mægler i sager om individuelle forbrugerklager, bekræfter FTC, at handelskommissionen vil prioritere henviste sager fra EU's databeskyttelsesmyndigheder under EU-USA-databeskyttelsesrammen. FTC anvender desuden klager i sin Consumer Sentinel-database, som mange andre retshåndhavende organer har adgang til, til at kortlægge tendenser, fastlægge prioriteter for håndhævelsen og identificere potentielle organisationer, der skal undersøges. Privatpersoner i EU kan anvende det samme klagesystem som amerikanske statsborgere til indgivelse af en klage til FTC, og det er tilgængeligt på adressen <https://reportfraud.ftc.gov/>. I forbindelse med individuelle klager over krænkelse af principperne i EU-USA-databeskyttelsesrammen kan det imidlertid være mest hensigtsmæssigt, hvis privatpersoner i EU indgiver deres klager til databeskyttelsesmyndigheden i deres respektive medlemsstater eller til en uafhængig tvistbilæggelsesinstans.

⁽¹⁴⁾ 15 U.S.C. § 45(m), 16 C.F.R. § 1.98. Dette beløb justeres regelmæssigt for inflation.

⁽¹⁵⁾ Sidste år stemte FTC for at strømline processen for undersøgelse af recidivister. Jf. Press Release, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (1.7.2021), findes på <https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities>.

⁽¹⁶⁾ Jf. FTC, Privacy Shield, findes på <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>.

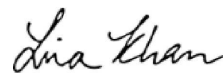
IV. Håndhævelsessamarbejde med EU's databeskyttelsesmyndigheder

FTC anerkender, at EU's databeskyttelsesmyndigheder spiller en vigtig rolle med hensyn til at sikre, at principperne i EU-USA-databeskyttelsesrammen overholdes, og fremmer inddragelsen af og samarbejdet med disse myndigheder. En koordineret tilgang til udfordringerne i forbindelse med den nuværende udvikling på det digitale marked og de dataintensive forretningsmodeller bliver stadig mere kritisk. FTC vil udveksle oplysninger om henvisninger med de henvisende håndhævende myndigheder, herunder status for henvisningerne, i det omfang det er foreneligt med reglerne om — og de begrænsninger, der gælder i forbindelse med — fortrolighed. I lyset af antallet og karakteren af henviste sager vil oplysningerne så vidt muligt omfatte en vurdering af de henviste sager, herunder en redegørelse for de væsentlige problemer, der er blevet rejst, og for eventuelle iværksatte foranstaltninger i forbindelse med lovovertrædelser, der ligger inden for rammerne af FTC's kompetence. FTC vil ligeledes give den henvisende myndighed feedback om typen af modtagne henviste sager for at øge effektiviteten af indsatsen mod ulovlig adfærd. Hvis en henvisende håndhævende myndighed ønsker oplysninger om status for en bestemt henvist sag med henblik på indledning af sin egen håndhævelsesprocedure, vil FTC i sit svar tage hensyn til antallet af henviste sager, der fortsat er under overvejelse, i det omfang det er foreneligt med fortrolighedskrav.

FTC vil ligeledes arbejde tæt sammen med EU's databeskyttelsesmyndigheder om håndhævelsesforanstaltninger. I relevante sager kunne dette omfatte udveksling af oplysninger og efterforskningsbistand i medfør af U.S. SAFE WEB Act, der bemyndiger FTC til at yde bistand til udenlandske retshåndhævende organer, når det udenlandske organ håndhæver love, som forbyder praksis, der i alt væsentligt svarer til praksis, der er forbudt i de love, som FTC håndhæver⁽¹⁷⁾. Som led i denne bistand kan FTC udveksle oplysninger indsamlet i forbindelse med en FTC-undersøgelse, udstede obligatorisk proces på vegne af den databeskyttelsesmyndighed i EU, som foretager sin egen undersøgelse, og indhente mundtlige forklaringer fra vidner eller sagsøgte i forbindelse med databeskyttelsesmyndighedens håndhævelsesprocedure, forudsat at kravene i U.S. SAFE WEB Act overholdes. FTC anvender regelmæssigt denne bemyndigelse til at bistå andre myndigheder verden over i sager om beskyttelse af privatlivets fred og forbrugere.

Ud over samarbejdet med de henvisende databeskyttelsesmyndigheder om sagsspecifikke spørgsmål vil FTC deltage i regelmæssige møder med udpegede repræsentanter fra Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") med henblik på en generel drøftelse af, hvordan samarbejdet om håndhævelse kan forbedres. FTC vil ligeledes deltage i den regelmæssige evaluering af EU-USA-databeskyttelsesrammen sammen med handelsministeriet, Europa-Kommissionen og repræsentanter fra Databeskyttelsesrådet for at drøfte rammens gennemførelse. FTC fremmer endvidere udviklingen af redskaber, som kan forbedre håndhævelsessamarbejdet med EU's databeskyttelsesmyndigheder og med andre databeskyttelsesmyndigheder verden over. FTC bekræfter med glæde sit tilsagn om at håndhæve de kommercielle aspekter af EU-USA-databeskyttelsesrammen. Vi ser vores partnerskab med vores EU-kolleger som en afgørende del af beskyttelsen af privatlivets fred for såvel de amerikanske som de europæiske borgere.

Med venlig hilsen



Lina M. KHAN

Formand, Federal Trade Commission

⁽¹⁷⁾ Ved vurderingen af, om FTC skal anvende sin bemyndigelse under U.S. SAFE WEB Act, overvejer FTC bl.a.: "A) om den anmodende instans har indvilliget i at yde eller vil yde gensidig bistand til FTC, B) om besvarelse af anmodningen vil være til skade for USA's offentlige interesser, og C) om den anmodende instans' undersøgelse eller håndhævelsesprocedure vedrører adfærd eller praksis, der forårsager eller vil kunne forårsage skade på et betydeligt antal personer." 15 U.S.C. § 46(j)(3). Denne bemyndigelse omfatter ikke håndhævelse af konkurrenceregler.

Tillæg A

Håndhævelse af principperne i privatlivsskjoldet og safe harbour-ordningen

	Dossier/FTC-sagsnr.	Sag	Link
1	FTC-sagsnr. 2023062 Sag nr. 3:22-cv-03070 (N.D. Cal.)	USA mod Twitter, Inc.	Twitter
2	FTC-sagsnr. 192 3209	I sagen Residual Pumpkin Entity, LLC, tidligere benævnt CafePress , og PlanetArt, LLC, også benævnt CafePress	CafePress
3	FTC-sagsnr. 192 3133 Dossier nr. C-4747	I sagen Flo Health, Inc.	Flo Health
4	FTC-sagsnr. 192 3050 Dossier nr. C-4723	I sagen Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5	FTC-sagsnr. 192 3092 Dossier nr. C-4709	I sagen T&M Protection, LLC	T&M Protection
6	FTC-sagsnr. 192 3084 Dossier nr. C-4704	I sagen TDARX, Inc.	TDARX
7	FTC-sagsnr. 192 3093 Dossier nr. C-4706	I sagen Global Data Vault, LLC	Global Data
8	FTC-sagsnr. 192 3078 Dossier nr. C-4703	I sagen Incentive Services, Inc.	Incentive Services
9	FTC-sagsnr. 192 3090 Dossier nr. C-4705	I sagen Click Labs, Inc.	Click Labs
10	FTC-sagsnr. 182 3192 Dossier nr. C-4697	I sagen Medable, Inc.	Medable
11	FTC-sagsnr. 182 3189 Dossier nr. 9386	I sagen NTT Global Data Centers Americas, Inc., som retssuccessor til RagingWire Data Centers, Inc.	RagingWire
12	FTC-sagsnr. 182 3196 Dossier nr. C-4702	I sagen Thru, Inc.	Thru
13	FTC-sagsnr. 182 3188 Dossier nr. C-4698	I sagen DCR Workforce, Inc.	DCR Workforce
14	FTC-sagsnr. 182 3194 Dossier nr. C-4700	I sagen LotaData, Inc.	LotaData
15	FTC-sagsnr. 182 3195 Dossier nr. C-4701	I sagen EmpiriStat, Inc.	EmpiriStat

16	FTC-sagsnr. 182 3193 Dossier nr. C-4699	I sagen 214 Technologies, Inc., også benævnt Trueface.ai	Trueface.ai
17	FTC-sagsnr. 182 3107 Dossier nr. 9383	I sagen Cambridge Analytica, LLC	Cambridge Analytica
18	FTC-sagsnr. 182 3152 Dossier nr. C-4685	I sagen SecureTest, Inc.	SecurTest
19	FTC-sagsnr. 182 3144 Dossier nr. C-4664	I sagen VenPath, Inc.	VenPath
20	FTC-sagsnr. 182 3154 Dossier nr. C-4666	I sagen SmartStart Employment Screening, Inc.	SmartStart
21	FTC-sagsnr. 182 3143 Dossier nr. C-4663	I sagen mResourceLLC , også benævnt Loop Works LLC	mResource
22	FTC-sagsnr. 182 3150 Dossier nr. C-4665	I sagen IDmission LLC	IDmission
23	FTC-sagsnr. 182 3100 Dossier nr. C-4659	I sagen ReadyTech Corporation	ReadyTech
24	FTC-sagsnr. 172 3173 Dossier nr. C-4630	I sagen Decusoft, LLC	Decusoft
25	FTC-sagsnr. 172 3171 Dossier nr. C-4628	I sagen Tru Communication, Inc.	Tru
26	FTC-sagsnr. 172 3172 Dossier nr. C-4629	I sagen Md7, LLC	Md7
30	FTC-sagsnr. 152 3198 Dossier nr. C-4543	I sagen Jhayrmaine Daniels (også benævnt California Skate-Line)	Jhayrmaine Daniels
31	FTC-sagsnr. 152 3190 Dossier nr. C-4545	I sagen Dale Jarrett Racing Adventure, Inc.	Dale Jarrett
32	FTC-sagsnr. 152 3141 Dossier nr. C-4540	I sagen Golf Connect, LLC	Golf Connect
33	FTC-sagsnr. 152 3202 Dossier nr. C-4546	I sagen Inbox Group, LLC	Inbox Group
34	Sagsnr. 152 3187 Dossier nr. C-4542	I sagen IOActive, Inc.	IOActive
35	FTC-sagsnr. 152 3140 Dossier nr. C-4549	I sagen Jubilant Clinsys, Inc.	Jubilant
36	FTC-sagsnr. 152 3199 Dossier nr. C-4547	I sagen Just Bagels Manufacturing, Inc.	Just Bagels

37	FTC-sagsnr. 152 3138 Dossier nr. C-4548	I sagen NAICS Association, LLC	NAICS
38	FTC-sagsnr. 152 3201 Dossier nr. C-4544	I sagen One Industries Corp.	One Industries
39	FTC-sagsnr. 152 3137 Dossier nr. C-4550	I sagen Pinger, Inc.	Pinger
40	FTC-sagsnr. 152 3193 Dossier nr. C-4552	I sagen SteriMed Medical Waste Solutions	SteriMed
41	FTC-sagsnr. 152 3184 Dossier nr. C-4541	I sagen Contract Logix, LLC	Contract Logix
42	FTC-sagsnr. 152 3185 Dossier nr. C-4551	I sagen Forensics Consulting Solutions, LLC	Forensics Consulting
43	FTC-sagsnr. 152 3051 Dossier nr. C-4526	I sagen American Int'l Mailing, Inc.	AIM
44	FTC-sagsnr. 152 3015 Dossier nr. C-4525	I sagen TES Franchising, LLC	TES
45	FTC-sagsnr. 142 3036 Dossier nr. C-4459	I sagen American Apparel, Inc.	American Apparel
46	FTC-sagsnr. 142 3026 Dossier nr. C-4469	I sagen Fantage.com, Inc.	Fantage
47	FTC-sagsnr. 142 3017 Dossier nr. C-4461	I sagen Apperian, Inc.	Apperian
48	FTC-sagsnr. 142 3018 Dossier nr. C-4462	I sagen Atlanta Falcons Football Club, LLC	Atlanta Falcons
49	FTC-sagsnr. 142 3019 Dossier nr. C-4463	I sagen Baker Tilly Virchow Krause, LLP	Baker Tilly
50	FTC-sagsnr. 142 3020 Dossier nr. C-4464	I sagen BitTorrent, Inc.	BitTorrent
51	FTC-sagsnr. 142 3022 Dossier nr. C-4465	I sagen Charles River Laboratories, Int'l	Charles River
52	FTC-sagsnr. 142 3023 Dossier nr. C-4466	I sagen DataMotion, Inc.	DataMotion
53	FTC-sagsnr. 142 3024 Dossier nr. C-4467	I sagen DDC Laboratories, Inc. , også benævnt DNA Diagnostics Center	DDC
54	FTC-sagsnr. 142 3028 Dossier nr. C-4470	I sagen Level 3 Communications, LLC	Level 3

55	FTC-sagsnr. 142 3025 Dossier nr. C-4468	I sagen PDB Sports, Ltd. , også benævnt Denver Broncos Football Club, LLP	Broncos
56	FTC-sagsnr. 142 3030 Dossier nr. C-4471	I sagen Reynolds Consumer Products, Inc.	Reynolds
57	FTC-sagsnr. 142 3031 Dossier nr. C-4472	I sagen Receivable Management Services Corporation	Receivable Mgmt
58	FTC-sagsnr. 142 3032 Dossier nr. C-4473	I sagen Tennessee Football, Inc.	Tennessee Football
59	FTC-sagsnr. 102 3058 Dossier nr. C-4369	I sagen Myspace LLC	Myspace
60	FTC-sagsnr. 092 3184 Dossier nr. C-4365	I sagen Facebook, Inc.	Facebook
61	FTC-sagsnr. 092 3081 Civilsag nr. 09-CV-5276 (C.D. Cal.)	FTC mod Javian Karnani, og Balls of Kryptonite, LLC , også benævnt Bite Size Deals, LLC, og Best Priced Brands, LLC	Balls of Kryptonite
62	FTC-sagsnr. 102 3136 Dossier nr. C-4336	I sagen Google, Inc.	Google
63	FTC-sagsnr. 092 3137 Dossier nr. C-4282	I sagen World Innovators, Inc.	World Innovators
64	FTC-sagsnr. 092 3141 Dossier nr. C-4271	I sagen Progressive Gaitways LLC	Progressive Gaitways
65	FTC-sagsnr. 092 3139 Dossier nr. C-4270	I sagen Onyx Graphics, Inc.	Onyx Graphics
66	FTC-sagsnr. 092 3138 Dossier nr. C-4269	I sagen ExpatEdge Partners, LLC	ExpatEdge
67	FTC-sagsnr. 092 3140 Dossier nr. C-4281	I sagen Directors Desk LLC	Directors Desk
68	FTC-sagsnr. 092 3142 Dossier nr. C-4272	I sagen Collectify LLC	Collectify

BILAG V



THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

Den 6. juli 2023

Kommissær Didier Reynders
Europa-Kommissionen
Rue de la Loi / Wetstraat 200
1049 Bruxelles/Brussel
Belgien

Kære kommissær Didier Reynders,

De Forenede Staters transportministerium ("ministeriet") glæder sig over at få lejlighed til at redegøre for sin rolle i håndhævelsen af principperne i EU-USA-databeskyttelsesrammen. EU-USA-databeskyttelsesrammen vil spille en kritisk rolle med hensyn til at fremme beskyttelsen af personoplysninger, der overføres i forbindelse med kommercielle transaktioner, i en stadig mere forbundet verden. Den vil give virksomheder mulighed for at gennemføre vigtige transaktioner i den globale økonomi og samtidig sikre den vigtige beskyttelse af EU-forbrugernes privatliv.

Transportministeriet forpligtede sig første gang offentligt til at håndhæve safe harbour-ordningen mellem USA og EU i et brev til Europa-Kommissionen for over 22 år siden, og dette tilsagn blev gentaget og uddybet i et brev fra 2016 vedrørende EU's og USA's værn om privatlivets fred (EU-USA-privatlivsskjoldet). Ministeriet afgav i disse breve tilsagn om at håndhæve principperne i safe harbour-ordningen mellem USA og EU til beskyttelse af privatlivets fred og derefter principperne i EU-USA-privatlivsskjoldet strengt. Transportministeriet udvider dette tilsagn til principperne i EU-USA-databeskyttelsesrammen, og dette tilsagn understreges i dette brev.

Transportministeriet bekræfter navnlig sine tilsagn på følgende hovedområder: 1) prioritering af undersøgelsen af påståede overtrædelser af principperne i EU-USA-databeskyttelsesrammen, 2) iværksættelse af passende håndhævelsesforanstaltninger mod enheder, der fremsætter falske eller vildledende påstande om deltagelse i EU-USA-databeskyttelsesrammen, og 3) overvågning og offentliggørelse af håndhævelsesafgørelser vedrørende overtrædelser af principperne i EU-USA-databeskyttelsesrammen. Vi redegør nedenfor for de enkelte tilsagn og af hensyn til sammenhængen for den relevante baggrund for transportministeriets rolle i beskyttelsen af forbrugernes privatliv og håndhævelsen af principperne i EU-USA-databeskyttelsesrammen.

1. Baggrund

A. Ministeriets beføjelser inden for beskyttelse af privatlivets fred

Ministeriet er stærkt optaget af at beskytte de oplysninger, som forbrugerne giver flyselskaber og rejsebureauer.

Ministeriets håndhævelsesbeføjelser på dette område har hjemmel i 49 U.S.C. 41712, der forbyder transportører eller rejsebureauer at anvende en illoyal eller vildledende praksis i forbindelse med lufttransportydelse eller salg af lufttransportydelse. Section 41712 er udformet efter Section 5 i Federal Trade Commission (FTC) Act (15 U.S.C. 45).

Ministeriet har for nylig udstedt bestemmelser, der definerer illoyal og vildledende praksis, i overensstemmelse med både ministeriets og FTC's præcedens (14 CFR § 399.79). En praksis er nærmere bestemt "illoyal", hvis den forårsager eller sandsynligvis vil forårsage betydelig skade, som ikke med rimelighed kan undgås, og skaden ikke opvejes af forbrugernes eller de konkurrencemæssige fordele.

En praksis er "vildledende" over for forbrugerne, hvis den kan vildlede en forbruger, der handler fornuftigt under de givne omstændigheder, med hensyn til et væsentligt spørgsmål. Et spørgsmål er væsentligt, hvis det kan have påvirket forbrugerens adfærd eller beslutning vedrørende et produkt eller en tjenesteydelse. Ud over disse generelle principper fortolker transportministeriet specifikt Section 41712 således, at transportører og rejsebureauer ikke må: 1) overtræde principperne i deres politik til beskyttelse af privatlivets fred, 2) overtræde enhver regel udstedt af ministeriet, der identificerer specifik databeskyttelsespraksis som illoyal eller vildledende, 3) overtræde Children's Online Privacy Protection Act (COPPA) eller FTC's regler til gennemførelse af COPPA eller 4) undlade som deltagere i EU-USA-databeskyttelsesrammen at overholde principperne i EU-USA-databeskyttelsesrammen ⁽¹⁾.

Som nævnt ovenfor har ministeriet i henhold til forbundslovgivningen enekompetence til at regulere luftfartsselskabernes databeskyttelsespraksis og deler kompetence med FTC, for så vidt angår rejsebureauernes databeskyttelsespraksis i forbindelse med salg af lufttransporttydelser.

Når først en transportør eller sælger af lufttransporttydelser offentligt har forpligtet sig til at overholde principperne i EU-USA-databeskyttelsesrammen, kan ministeriet gøre brug af sine lovbestemte beføjelser i henhold til Section 41712 for at sikre, at disse principper overholdes. Når en passager afgiver oplysninger til en transportør eller et rejsebureau, der har forpligtet sig til at overholde principperne i EU-USA-databeskyttelsesrammen, vil transportørens eller rejsebureauets manglende overholdelse af disse principper derfor være en overtrædelse af Section 41712.

B. Håndhævelsespraksis

Ministeriets Office of Aviation Consumer Protection ("OACP") ⁽²⁾ undersøger sager og rejser tiltale under 49 U.S.C. 41712. Kontoret håndhæver primært det lovbestemte forbud i Section 41712 mod illoyal og vildledende praksis gennem forhandlinger, udarbejdelse af udkast til forbud (cease and desist orders) og afgørelser om civile sanktioner. Kontoret får primært kendskab til potentielle overtrædelser gennem de klager, der modtages fra borgere, rejsebureauer, luftfartsselskaber og amerikanske og udenlandske regeringsorganer. Forbrugerne kan indgive klager over krænkelse af privatlivets fred mod luftfartsselskaber og rejsebureauer via ministeriets websted ⁽³⁾.

Hvis ikke der indgås et rimeligt og passende forlig i en sag, har OACP kompetence til at indlede en håndhævelsesprocedure med bevisføring for ministeriets forvaltningsdommer (administrative law judge (ALJ)). ALJ er bemyndiget til at udstede forbud og idømme civile sanktioner. Overtrædelser af Section 41712 kan medføre, at der udstedes forbud og idømmes civile sanktioner på op til 37 377 USD for hver overtrædelse af Section 41712.

Ministeriet har ikke beføjelse til at tilkende erstatning eller give økonomisk godtgørelse til individuelle klagere. Ministeriet har dog beføjelse til at godkende forlig, der indgås på baggrund af undersøgelser foretaget af OACP, og som er til direkte gavn for forbrugerne (kontante beløb, vouchere) i form af en udligning af de gebyrer, der ellers skulle betales til de amerikanske myndigheder. Det er sket før og kan ske igen i forbindelse med overtrædelser af principperne i EU-USA-databeskyttelsesrammen, når omstændighederne taler herfor. Hvis et flyselskab gentagne gange overtræder Section 41712, vil der også opstå tvivl om selskabets evne til i det hele taget at overholde loven, hvilket i ekstreme sager vil medføre, at det findes uegnet til at drive erhvervsmæssig virksomhed og dermed mister sin tilladelse hertil.

Ministeriet har indtil videre modtaget forholdsvis få klager over rejsebureauers eller luftfartsselskabers påståede krænkelse af privatlivets fred. Når det sker, undersøges de i overensstemmelse med de principper, der er redegjort for ovenfor.

C. Ministeriets retsbeskyttelse til gavn for EU-forbrugere

I henhold til Section 41712 finder forbuddet mod illoyal eller vildledende praksis i forbindelse med lufttransporttydelser eller salg af lufttransporttydelser anvendelse på amerikanske og udenlandske transportører og rejsebureauer. Ministeriet griber ofte ind over for amerikanske og udenlandske luftfartsselskabers praksis, der både berører udenlandske og amerikanske forbrugere, idet luftfartsselskabernes praksis blev udøvet i forbindelse med transport af passagerer til eller fra USA. Ministeriet anvender og vil fortsat anvende alle tilgængelige retsmidler til at beskytte både udenlandske og amerikanske forbrugere mod regulerede enheders illoyale eller vildledende praksis inden for lufttransport.

⁽¹⁾ <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy>.

⁽²⁾ Tidligere kendt som Office of Aviation Enforcement and Proceedings.

⁽³⁾ <http://www.transportation.gov/airconsumer/privacy-complaints>.

Med hensyn til luftfartsselskaber håndhæver ministeriet ligeledes andre relevante love, hvis bestemmelser også finder anvendelse på ikkeamerikanske forbrugere, f.eks. Children's Online Privacy Protection Act ("COPPA"). I henhold til COPPA skal operatører af websteder og onlinetjenester rettet mod børn eller websteder rettet mod den brede offentlighed, som bevidst indsamler personoplysninger om børn under 13 år, bl.a. underrette forældrene og indhente verificerbart forældresamtykke. USA-baserede websteder og -tjenester, der er omfattet af COPPA og indsamler personoplysninger om udenlandske børn, skal overholde COPPA. Udenlandske websteder og onlinetjenester skal ligeledes overholde COPPA, hvis de henvender sig til børn i USA, eller hvis de bevidst indsamler personoplysninger fra børn i USA. Ministeriet er bemyndiget til at indlede overtrædelsesprocedurer mod amerikanske og udenlandske luftfartsselskaber, der opererer i USA og overtræder COPPA.

II. Håndhævelse af principperne i EU-USA-databeskyttelsesrammen

Hvis et luftfartsselskab eller et rejsebureau vælger at deltage i EU-USA-databeskyttelsesrammen, og ministeriet modtager en klage over luftfartsselskabets eller rejsebureauets påståede overtrædelse af principperne i EU-USA-databeskyttelsesrammen, vil ministeriet træffe følgende foranstaltninger for at håndhæve principperne i databeskyttelsesrammen strengt.

A. Prioritering af undersøgelse af påståede overtrædelser

Ministeriets OACP vil undersøge enhver klage over påståede overtrædelser af principperne i EU-USA-databeskyttelsesrammen, herunder klager fra EU's databeskyttelsesmyndigheder, og træffe håndhævelsesforanstaltninger, hvis der er dokumentation for en overtrædelse.

OACP vil desuden samarbejde med FTC og det amerikanske handelsministerium og give højeste prioritet til sager med påstande om, at de regulerede enheder ikke efterlever deres tilsagn om at beskytte privatlivets fred afgivet under EU-USA-databeskyttelsesrammen.

Når ministeriets OACP modtager en klage med påstand om en overtrædelse af principperne i EU-USA-databeskyttelsesrammen, kan kontoret træffe en række foranstaltninger som led i sin undersøgelse. Kontoret kan f.eks. gennemgå rejsebureauets eller luftfartsselskabets politikker til beskyttelse af privatlivets fred, indhente yderligere oplysninger fra rejsebureauet eller luftfartsselskabet eller fra tredjemand, følge op over for den henvisende instans og vurdere, om der er et overtrædelsesmønster eller et betydeligt antal berørte forbrugere. Derudover vil kontoret vurdere, om sagen vedrører spørgsmål, der henhører under handelsministeriet eller FTC, og om det ville være nyttigt at iværksætte oplysningsforanstaltninger over for forbrugerne og virksomhederne, og eventuelt indlede en håndhævelsesprocedure.

Hvis ministeriet får kendskab til rejsebureauers potentielle overtrædelser af principperne i EU-USA-databeskyttelsesrammen, vil ministeriet koordinere sagen med FTC. Vi vil ligeledes underrette FTC og handelsministeriet om udfaldet af en eventuel håndhævelsesprocedure vedrørende principperne i EU-USA-databeskyttelsesrammen.

B. Håndtering af falske eller vildledende påstande om deltagelse i EU-USA-databeskyttelsesrammen

Ministeriet vil fortsat undersøge overtrædelser af principperne i EU-USA-databeskyttelsesrammen, herunder falske eller vildledende påstande om deltagelse i databeskyttelsesrammen. Vi vil give højeste prioritet til sager henvist fra handelsministeriet vedrørende organisationer, der ifølge handelsministeriet fremstiller sig selv som værende deltagere i EU-USA-databeskyttelsesrammen eller anvender et certificeringsmærke under EU-USA-databeskyttelsesrammen uden tilladelse.

Vi understreger endvidere, at hvis en organisation i sin politik til beskyttelse af privatlivets fred erklærer, at den overholder principperne i EU-USA-databeskyttelsesrammen, fritager det forhold, at organisationen ikke foretager eller opretholder sin selvcertificering over for handelsministeriet, ikke i sig selv organisationen fra ministeriets håndhævelse af de pågældende forpligtelser.

C. Overvågning og offentliggørelse af håndhævelsesafgørelser vedrørende overtrædelser af EU-USA-databeskyttelsesrammen

Ministeriets OACP vil også fortsat overvåge håndhævelsesafgørelser for at sikre, at principperne i EU-USA-databeskyttelsesrammen overholdes. Hvis kontoret udsteder et forbud, der pålægger et luftfartsselskab eller rejsebureau at afholde sig fra fremtidige overtrædelser af principperne i EU-USA-databeskyttelsesrammen og Section 41712, vil kontoret overvåge, om enheden overholder bestemmelserne om forbud. Kontoret vil desuden sikre, at forbud, der udstedes i sager om EU-USA-databeskyttelsesrammen, offentliggøres på dets websted.

Vi ser frem til et fortsat samarbejde med vores føderale partnere og interessenter i EU om EU-USA-databeskyttelsesrammen.

Jeg håber, at disse oplysninger er nyttige, og står naturligvis til rådighed, såfremt De måtte have spørgsmål eller ønske yderligere oplysninger.

Med venlig hilsen



Pete BUTTIGIEG

BILAG VI



U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General

Washington, D.C. 20530

Den 23. juni 2023

Ana Gallego Torres
Generaldirektør for retlige anliggender og forbrugere
Europa-Kommissionen
Rue Montoyer/Montoyerstraat 59
1049 Bruxelles/Brussel
Belgien

Kære generaldirektør Ana Gallego Torres,

Dette brev giver et kort overblik over de vigtigste efterforskningsmetoder, der kan anvendes til at indhente forretningsoplysninger og andre optegnelser fra virksomheder i USA med henblik på strafferetlig håndhævelse eller den offentlige interesse (civilretlige eller reguleringsmæssige formål), herunder disse metoders begrænsninger for adgang ⁽¹⁾. Alle de pålæg, der er beskrevet i dette brev, indebærer ikke forskelsbehandling, da de anvendes til at indhente oplysninger fra virksomheder i USA, herunder virksomheder, som vil foretage selvcertificering under EU-USA-databeskyttelsesrammen, uanset den registreredes nationalitet og opholdssted. Virksomheder, der får udstedt et pålæg i USA, kan desuden anfægte det ved domstolene som anført nedenfor ⁽²⁾.

For så vidt angår offentlige myndigheders beslaglæggelse af oplysninger er det værd at bemærke fjerde amendment til den amerikanske forfatning, hvor det fastslås, at "folkets ret til sikkerhed for deres personer, boliger, papirer og ejendele imod urimelige ransagninger, anholdelser og beslaglæggelser ikke må krænkes, og at ingen kendelse herom må afsiges uden en begrundet mistanke, der er støttet på en udtalelse afgivet under ed eller en højtidelig erklæring og nøje beskriver det sted, der skal ransages, de personer, der skal anholdes, eller de ting, der skal beslaglægges" (den amerikanske forfatning, fjerde amendment). Som fastslået af den amerikanske højesteret i sagen *Berger v. State of New York*, "er det grundlæggende formål med denne forfatningsændring — som anerkendt i utallige af denne domstols afgørelser — at beskytte den enkeltes privatliv og sikkerhed mod embedsmænds vilkårlige indgreb" (388 U.S. 41, 53 (1967)) (citater fra *Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). I henhold til fjerde amendment skal de retshåndhævende myndigheder generelt have en dommerkendelse inden en ransagning i forbindelse med indenlandske strafferetlige efterforskninger, jf. *Katz v. United States*, 389 U.S. 347, 357 (1967). Principperne for udstedelse af en kendelse, såsom begrundet mistanke og særlige krav, finder anvendelse på kendelser om fysiske ransagninger og beslaglæggelser samt på kendelser vedrørende lagret

⁽¹⁾ I dette overblik redegøres ikke for de metoder, som de retshåndhævende myndigheder anvender til nationale sikkerhedsformål i forbindelse med efterforskning af terrorisme og andre efterforskninger vedrørende den nationale sikkerhed, herunder nationale sikkerhedsbreve (National Security Letters (NSL'er) med henblik på indhentning af visse registeroplysninger såsom kreditoplysninger, finansielle oplysninger og elektroniske abonnent- og transaktionsoplysninger, jf. 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v, 18 U.S.C. § 2709, 50 U.S.C. § 3162, og elektronisk overvågning, ransagningskendelser, forretningsoplysninger og anden indsamling af kommunikation i henhold til Foreign Intelligence Surveillance Act, jf. 50 U.S.C. § 1801 et seq.

⁽²⁾ I dette brev redegøres for føderale retshåndhævelses- og reguleringsbeføjelser. Overtrædelser af delstatslovgivningen efterforskes af delstaternes retshåndhævende myndigheder og retsforfølges ved delstatsdomstolene. De retshåndhævende myndigheder på delstatsniveau anvender kendelser og stævninger udstedt i henhold til delstatslovgivningen på stort set samme måde som beskrevet her, men delstaternes pålæg kan omfattes af yderligere beskyttelse i henhold til delstatsforfatninger eller -love, der har forrang for beskyttelsen i den amerikanske forfatning. Beskyttelsen i henhold til delstatslovgivningen skal mindst svare til beskyttelsen i henhold til den amerikanske forfatning, herunder, men ikke begrænset til, fjerde amendment.

elektronisk kommunikationsindhold udstedt i henhold til Stored Communications Act som beskrevet nedenfor. I de tilfælde, hvor der ikke skal udstedes en kendelse, er myndighedernes foranstaltninger betinget af en "rimelighedstest" i henhold til fjerde amendement. Forfatningen sikrer derfor i sig selv, at de amerikanske myndigheder ikke har ubegrænsede eller vilkårlige beføjelser til at beslaglægge personoplysninger ⁽³⁾.

Strafferetlige håndhævende myndigheder

Forbundsanklagerne, der er embedsmænd i det amerikanske justitsministerium, og føderale efterforskningsagenter, herunder agenter i Federal Bureau of Investigation (FBI), et retshåndhævelsesorgan under justitsministeriet, kan anmode virksomheder i USA om at udlevere dokumenter og andre optegnelser til strafferetlige efterforskningsformål 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-anordninger.

Stævninger udstedt af anklagejuryen eller i en retssag (grand jury or trial subpoenas): Stævninger i straffesager anvendes til at understøtte målrettede retshåndhævelse efterforskninger. En stævning udstedt af anklagejuryen er en officiel anmodning fra en anklagejury (normalt på forbundsanklagerens foranledning) om at støtte anklagejuryens efterforskning ved mistanke om en bestemt overtrædelse af straffelovgivningen. Anklagejuryer er domstolens efterforskningsgren og udpeges af en dommer. En stævning kan pålægge en person at vidne under en retssag eller at tilvejebringe eller udlevere forretningsoplysninger, elektronisk lagrede oplysninger eller andre konkrete ting. Oplysningerne skal være relevante for efterforskningen, og pålæg må ikke være urimelige, dvs. overdrevne, undertrykkende eller byrdefulde. En modtager kan anfægte en stævning med henvisning til disse grunde, jf. Fed. R. Crim. P. 17. Under begrænsede omstændigheder kan stævninger i straffesager med påbud om udlevering af dokumenter anvendes, efter at sagen er blevet rejst af anklagejuryen.

Tilladelse til at udstede administrative pålæg (administrative subpoenas): Der kan udstedes administrative pålæg i forbindelse med straffe- og civilretlige undersøgelser. I forbindelse med strafferetlig håndhævelse kan der udstedes administrative pålæg i henhold til en række føderale love om tilvejebringelse eller udlevering af forretningsoplysninger, elektronisk lagrede oplysninger eller andre konkrete ting i sager, der involverer misbrug af sundhedsydelser, børnemishandling, beskyttelse af efterretningstjenester og kontrollerede stoffer og i forbindelse med generalinspektørernes undersøgelser af regeringsorganer. Hvis myndighederne anmoder om at få håndhævet et administrativt pålæg ved domstolene, kan modtageren af det administrative pålæg i lighed med modtageren af en stævning med et pålæg udstedt af en anklagejury gøre gældende, at pålægget er urimeligt, fordi det er overdrevent eller undertrykkende eller byrdefuldt.

Retsafgørelser om installation af pen-register- og trap and trace-anordninger: I henhold til de strafferetlige bestemmelser om pen-register- og trap and trace-anordninger kan de retshåndhævende myndigheder få udstedt en retsafgørelse for at indhente ikkeindholdsmæssige realtidsoplysninger om opkald, routing, adressering og signalering for et telefonnummer eller en e-mailadresse efter fremlæggelse af dokumentation for, at de pågældende oplysninger er relevante for en verserende strafferetlig efterforskning, jf. 18 U.S.C. § 3121-3127. Brug eller installation af en sådan anordning uden lovhjemmel er en føderal forbrydelse.

Electronic Communications Privacy Act (ECPA): Der er en række yderligere bestemmelser, som regulerer myndighedernes adgang til internetudbyderes, teleselskabers og andre eksterne tjenesteudbyderes opbevarede abonnentoplysninger, trafikdata og lagrede kommunikationsindhold, i Title II i ECPA, også benævnt Stored Communications Act (SCA), 18 U.S.C. § 2701-2712. I SCA fastsættes en række lovbestemte rettigheder til beskyttelse af privatlivets fred, der begrænser de retshåndhævende myndigheders adgang til oplysninger fra kunder og abonnenter hos internetudbydere ud over dem, der kræves i forfatningsretten. I henhold til SCA øges niveauet af beskyttelsen af privatlivets fred i forhold til indsamlingens indgribende karakter. Strafferetlige håndhævende myndigheder kan kun få udleveret abonnentoplysninger, IP-adresser og tilknyttede tidsstempler samt faktureringsoplysninger på grundlag af et pålæg. I forbindelse med de fleste andre lagrede,

⁽³⁾ Hvad angår det fjerde amendements principper om beskyttelse af privatlivets fred og sikkerhedsinteresser, der er omhandlet ovenfor, anvender de amerikanske domstole regelmæssigt disse principper på nye typer efterforskningsredskaber i forbindelse med retshåndhævelsen, der muliggøres af den teknologiske udvikling. Højesteret fastslog f.eks. i 2018, at myndighedernes erhvervelse i forbindelse med en retshåndhævelse efterforskning af historiske lokaliseringsoplysninger fra et mobiltelefonselskab gennem en længere periode er en "søgning", der er omfattet af kravet om en kendelse i fjerde amendement. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

ikkeindholdsmæssige oplysninger såsom e-mailhoveder uden emnelinjen skal de retshåndhævende myndigheder fremlægge specifikke forhold for en dommer, som dokumenterer, at de udbedte oplysninger er relevante og væsentlige for en verserende strafferetlig efterforskning. For at få udleveret lagret elektronisk kommunikationsindhold skal strafferetlige håndhævende myndigheder generelt have udstedt et pålæg af en dommer med den begrundelse, at der er begrundet mistanke om, at den pågældende konto indeholder beviser for en forbrydelse. I henhold til SCA kan der desuden pålægges et civilretligt ansvar og strafferetlige sanktioner (*).

Retsafgørelser om overvågning i henhold til føderal lovgivning om aflytning: De retshåndhævende myndigheder kan desuden opfange trådbåren, mundtlig eller elektronisk kommunikation i realtid til strafferetlige efterforskningsformål i medfør af den føderale lovgivning om aflytning, jf. 18 U.S.C. § 2510-2523. Denne tilladelse gives kun på grundlag af en retsafgørelse, hvor en dommer bl.a. vurderer, at der er begrundet mistanke om, at aflytningen eller opfangningen af den elektroniske kommunikation vil tilvejebringe bevis for en føderal forbrydelse eller for opholdsstedet for en person, der er på flugt for at undgå retsforfølgning. I henhold til loven kan der pålægges et civilretligt ansvar og strafferetlige sanktioner for overtrædelser af bestemmelserne om aflytning.

Ransagningskendelse — Fed. R. Crim. P. Rule 41: De retshåndhævende myndigheder kan foretage en fysisk ransagning af lokaler i USA, hvis de bemyndiges hertil af en dommer. De retshåndhævende myndigheder skal således dokumentere over for dommeren, at der er begrundet mistanke om, at der er blevet eller snart vil blive begået en forbrydelse, og at genstande forbundet med forbrydelsen sandsynligvis kan findes på det sted, der er angivet i kendelsen. Kendelser anvendes ofte, når det er nødvendigt, at politiet foretager en fysisk ransagning af et lokale, da der er fare for, at beviser vil blive ødelagt, hvis der udstedes et pålæg eller en anden editionskendelse med pålæg om udlevering. 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. Se *Mapp v. Ohio*, 367 U.S. 643 (1961). Når en dataindehaver skal videregive oplysninger i henhold til en kendelse, kan den pågældende navnlig anfægte kravet om videregivelse som værende urimeligt byrdefuldt. Jf. *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (hvori det fastslås, at "en retfærdig rettergang kræver en høring om denne byrde, før et telefonselskab kan tvinges til at yde" bistand i forbindelse med en ransagningskendelse). *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980) (samme konklusion baseret på rettens tilsynsmyndighed).

Justitsministeriets retningslinjer og politikker: Ud over disse forfatnings-, lov- og regelbaserede begrænsninger for myndighedernes adgang til oplysninger har den amerikanske justitsminister udstedt retningslinjer, der yderligere begrænser de retshåndhævende myndigheders adgang til oplysninger, og som ligeledes indeholder bestemmelser om beskyttelse af privatlivets fred og borgerlige frihedsrettigheder. I den amerikanske justitsministers retningslinjer, Attorney General's Guidelines for Domestic FBI Operations (september 2008) (i det følgende benævnt "AG FBI Guidelines"), som findes på adressen <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, fastsættes der f.eks. begrænsninger for brugen af efterforskningsmetoder til at søge efter oplysninger om efterforskninger, der involverer føderale forbrydelser. I henhold til disse retningslinjer skal FBI anvende de mindst indgribende efterforskningsmetoder under hensyntagen til indvirkningen på privatlivets fred og de borgerlige frihedsrettigheder og den potentielle skade på omdømme. Det fastslås endvidere, at "FBI skal gennemføre sine efterforskninger og andre aktiviteter på en lovlig og rimelig måde, der respekterer frihed og privatlivets fred og undgår unødvendig indtrængen i lovlige menneskers liv". AG FBI Guidelines, s. 5. FBI har integreret disse retningslinjer i FBI Domestic Investigations and Operations Guide (DIOG), som findes på adressen <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29>. Der er tale om en omfattende håndbog, hvor der redegøres i detaljer for begrænsningerne for brugen af efterforskningsmetoder og opstilles retningslinjer, der skal sikre, at borgerlige frihedsrettigheder og privatlivets fred beskyttes i enhver efterforskning. Der er fastlagt yderligere regler og politikker, der begrænser forbundsanklagernes efterforskningsaktiviteter, i Justice Manual, der ligeledes er tilgængelig online på adressen <https://www.justice.gov/jm/justicemanual>.

Civile og regulerende myndigheder (offentlig interesse)

(*) Desuden giver Section 2705(b) i SCA myndighederne mulighed for at indhente en retsafgørelse på grundlag af et dokumenteret behov for beskyttelse mod videregivelse, der forbyder en udbyder af kommunikationstjenester frivilligt at oplyse sine brugere om, at den pågældende har modtaget et pålæg i henhold til SCA. I oktober 2017 udstedte vicejustitsminister Rod Rosenstein et memorandum til justitsministeriets advokater og befuldmægtigede med retningslinjer, som skal sikre, at anmodninger om sådanne sikrende kendelser er tilpasset efterforskningens specifikke forhold og behov, og som fastsætter, at en anmodning generelt højst kan udsætte oplysningspligten i et år. I maj 2022 udsendte vicejustitsminister Lisa Monaco yderligere retningslinjer om emnet, som bl.a. fastsatte interne krav om justitsministeriets godkendelse af anmodninger om forlængelse af en sikrende kendelse ud over den oprindelige etårige periode og krævede, at sikrende kendelser ophæves ved efterforskningens afslutning.

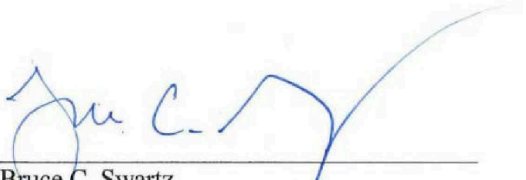
Der er endvidere betydelige begrænsninger for de civile og regulerende myndigheders, dvs. "den offentlige interesses", adgang til oplysninger, som virksomheder i USA ligger inde med. Myndigheder med civilretlige og regulerende opgaver kan udstede pålæg (subpoenas) til virksomheder om udlevering af forretningsoplysninger, elektronisk lagrede oplysninger eller andre konkrete ting (tangible items). Disse myndigheders administrative eller civilretlige beføjelser til at udstede pålæg er begrænsede, ikke kun på grund af deres statutter, men også på grund af den uafhængige domstolsprøvelse af pålæg inden potentiel retshåndhævelse, jf. f.eks. Fed. R. Civ. P. 45. Myndighederne kan kun søge indsigt i oplysninger, der er relevante for anliggender omfattet af deres reguleringskompetence. En modtager af et administrativt pålæg kan endvidere anfægte håndhævelsen af dette pålæg ved domstolene ved at fremlægge bevis for, at den pågældende myndighed ikke har handlet i overensstemmelse med grundlæggende standarder for rimelighed, jf. overfor.

Virksomheder kan anfægte anmodninger om oplysninger fra forvaltningsmyndigheder med hjemmel i andre retsgrundlag, afhængigt af sektoren og karakteren af de opbevarede oplysninger. Finansielle institutioner kan f.eks. anfægte administrative pålæg om udlevering af visse typer oplysninger med den begrundelse, at de er i strid med Bank Secrecy Act og gennemførelsesbestemmelserne hertil, 31 U.S.C. § 5318, 31 C.F.R. kapitel X. Andre virksomheder kan henvise til Fair Credit Reporting Act, 15 U.S.C. § 1681b, eller en lang række andre sektorspecifikke love. Ved misbrug af et organs kompetence til at udstede pålæg kan organet eller embedsmændene personligt drages til ansvar, jf. f.eks. Right to Financial Privacy Act, 12 U.S.C. § 3401-3423. De amerikanske domstole er således et værn mod reguleringsmyndighedernes uretmæssige anmodninger og fører uafhængigt tilsyn med forbundsorganernes foranstaltninger.

Endelig skal forvaltningsmyndighedernes lovbestemte beføjelser til at foretage en fysisk beslaglæggelse af optegnelser fra en virksomhed i USA i forbindelse med en administrativ ransagning opfylde betingelserne i fjerde amendment, jf. See v. City of Seattle, 387 U.S. 541 (1967).

Konklusion

Alle retshåndhævelses- og reguleringsaktiviteter i USA skal være forenelige med gældende ret, herunder den amerikanske forfatning og amerikanske love, regler og bestemmelser. Disse aktiviteter skal ligeledes være i overensstemmelse med gældende politikker, herunder i den amerikanske justitsministers generelle retningslinjer for håndhævelse af forbundslovgivningen. De retlige rammer, der er beskrevet ovenfor, begrænser de amerikanske retshåndhævelses- og reguleringsorganers muligheder for at få udleveret oplysninger fra virksomheder i USA – uanset om oplysningerne vedrører amerikanere eller borgere fra andre lande – og giver endvidere mulighed for domstolsprøvelse af alle anmodninger om oplysninger fra myndighederne i medfør af disse beføjelser.


Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

BILAG VII

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE OFFICE OF GENERAL COUNSEL

WASHINGTON, DC 20511

Den 9. december 2022

Leslie B. Kiernan
General Counsel
U.S. Department of
Commerce 1401 Constitution Ave.,
NW Washington, DC 20230

Kære Leslie B. Kiernan,

Den 7. oktober 2022 undertegnede præsident Biden Executive Order (præsidentielt dekret) 14086, *Enhancing Safeguards for United States Signals Intelligence Activities*, som supplerer de strenge garantier for privatlivets fred og borgerlige frihedsrettigheder, der gælder for amerikanske signalefterretningsaktiviteter. Disse garantier omfatter følgende: krav om, at signalefterretningsaktiviteter skal opfylde opregnede legitime mål, udtrykkeligt forbud mod, at sådanne aktiviteter anvendes med henblik på specifikke forbudte mål, indførelse af nye procedurer for at sikre, at signalefterretningsaktiviteter fremmer disse legitime mål og ikke de forbudte mål, krav om, at signalefterretningsaktiviteter kun udføres, efter at det på grundlag af en rimelig vurdering af alle relevante faktorer er fastslået, at aktiviteterne er nødvendige for at fremme en valideret efterretningsprioritet, og kun i et omfang og på en måde, der står i et rimeligt forhold til den validerede efterretningsprioritet, som de er godkendt til, pålæg om, at efterretningsenhederne ajourfører deres politikker og procedurer, så de afspejler de i det præsidentielle dekret påkrævede signalefterretningsgarantier. Vigtigst er det, at det præsidentielle dekret også indfører en uafhængig og bindende mekanisme, der gør det muligt for enkeltpersoner fra "kvalificerede stater", som udpeget i henhold til det præsidentielle dekret, at søge erstatning, hvis de mener, at de er blevet udsat for ulovlige amerikanske signalefterretningsaktiviteter, herunder aktiviteter, der krænker den beskyttelse, der er omhandlet i det præsidentielle dekret.

Præsident Bidens udstedelse af præsidentielt dekret 14086 markerede kulminationen på mere end et års detaljerede forhandlinger mellem repræsentanter for Europa-Kommissionen (Kommissionen) og USA og angiver de skridt, som USA vil tage for at gennemføre sine forpligtelser i henhold til EU-USA-databeskyttelsesrammen. Det er min opfattelse, at De i overensstemmelse med den samarbejdsånd, der har præget databeskyttelsesrammens tilblivelse, har modtaget to sæt spørgsmål fra Kommissionen om, hvordan efterretningssamfundet vil gennemføre dekretet. Disse spørgsmål vil jeg gerne besvare i dette brev.

Section 702 i Foreign Intelligence Surveillance Act af 1978 (Section 702 i FISA)

Det første sæt spørgsmål vedrører Section 702 i FISA, som gør det muligt at indsamle udenlandske efterretningsoplysninger ved at foretage målrettet overvågning af ikkeamerikanske personer, der med rimelighed kan formodes at befinde sig uden for USA, med påbudt bistand fra udbydere af elektroniske kommunikationstjenester. Spørgsmålene vedrører nærmere bestemt samspillet mellem denne bestemmelse og præsidentielt dekret 14086 samt de øvrige garantier, der finder anvendelse på aktiviteter, der udføres i henhold til Section 702 i FISA.

Indledningsvis kan vi bekræfte, at efterretningstjenesten vil anvende de garantier, der er fastsat i præsidentielt dekret 14086, på aktiviteter, der udføres i henhold til Section 702 i FISA.

Derudover gælder der en lang række andre garantier for regeringens anvendelse af Section 702 i FISA. Alle certificeringer i henhold til Section 702 i FISA skal f.eks. underskrives af både justitsministeren og direktøren for den nationale efterretningstjeneste (DNI), og regeringen skal forelægge alle sådanne certificeringer til godkendelse ved den amerikanske domstol for overvågning af efterretningsvirksomhed i udlandet (FISC), som består af uafhængige dommere, der er ansat i livstidsstillinger, og som sidder i en syvårig periode, som ikke kan forlænges. Certificeringerne identificerer de kategorier af udenlandske efterretningsoplysninger, der skal indsamles, idet disse skal stemme overens med den lovbestemte definition af udenlandske efterretningsoplysninger, ved at foretage målrettet overvågning af ikkeamerikanske personer, der med rimelighed kan formodes at befinde sig uden for USA. Certificeringerne har omfattet oplysninger om international terrorisme og andre spørgsmål såsom erhvervelse af oplysninger om masseødelæggelsesvåben. De årlige certificeringer skal forelægges FISC til godkendelse i en certificeringspakke, der omfatter justitsministerens og DNI's certificeringer, tro og love-erklæringer afgivet af bestemte ledere af efterretningstjenester og målretnings-, minimerings- og søgningsprocedurer, der er bindende for regeringen. Målretningsprocedurerne kræver bl.a., at efterretningstjenesten på grundlag af samtlige omstændigheder med rimelighed vurderer, at det er sandsynligt, at målretningen vil udmønte sig i indsamling af udenlandske efterretningsoplysninger, der er identificeret i en certificering i henhold til Section 702 i FISA.

Ved indsamling af oplysninger i henhold til Section 702 i FISA skal efterretningstjenesterne desuden: fremlægge en skriftlig redegørelse for grundlaget for deres vurdering på tidspunktet for målretningen, hvorefter målet forventes at være i besiddelse af, forventes at modtage eller sandsynligvis vil videregive udenlandske efterretningsoplysninger, der er identificeret i en certificering i henhold til Section 702 i FISA, bekræfte, at målretningsstandarderne som fastsat i målretningsprocedurerne i Section 702 i FISA fortsat er opfyldt, og indstille indsamlingen, hvis standarden ikke længere er opfyldt. Jf. den amerikanske regerings indlæg til den amerikanske domstol for overvågning af efterretningsvirksomhed i udlandet, *2015 Summary of Notable Section 702 Requirements*, s. 2-3 (15.7.2015).

Kravet om, at efterretningssamfundet skriftligt skal registrere og regelmæssigt bekræfte gyldigheden af sin vurdering af, at målene i henhold til Section 702 i FISA opfylder de gældende målretningsstandarder, letter FISC's overvågning af efterretningstjenestens målretningsaktiviteter. Hver enkelt registreret målsætningsvurdering og -begrundelse gennemgås hver anden måned af justitsministeriets advokater for efterretningstilsyn, som udøver dette tilsyn uafhængigt af udenlandske efterretningsaktiviteter. Den afdeling af justitsministeriet, der udøver dette tilsyn, er derefter i henhold til en veletableret FISC-regel ansvarlig for at indberette overtrædelser af de gældende procedurer til FISC. Denne indberetning giver sammen med regelmæssige møder mellem FISC og denne afdeling i justitsministeriet vedrørende tilsynet med målretningen i henhold til Section 702 i FISA FISC mulighed for at håndhæve overholdelsen af målretningsproceduren og de øvrige procedurer i Section 702 i FISA og i øvrigt sikre, at regeringens aktiviteter er lovlige. FISC kan gøre dette på forskellig vis, herunder ved at udstede bindende afhjælpende afgørelser om at fratage regeringen sin beføjelse til at indsamle oplysninger om et bestemt mål eller om at ændre eller udsætte dataindsamling i henhold til Section 702 i FISA. FISC kan endvidere kræve, at regeringen foretager yderligere indberetninger eller briefinger om sin overholdelse af målretningsproceduren og de øvrige procedurer eller kræve, at disse procedurer ændres.

Masseindsamling af signalefterretninger

Det andet sæt spørgsmål vedrører masseindsamling af signalefterretninger, som i præsidentielt dekret 14086 defineres som "tilladt indsamling af store mængder signalefterretninger, der på grund af tekniske eller operationelle forhold foretages uden brug af diskriminanter (f.eks. uden brug af specifikke identifikatorer eller selektorer)".

Med hensyn til disse spørgsmål skal vi indledningsvis bemærke, at masseindsamling hverken er tilladt i henhold til FISA eller de nationale sikkerhedsbreve. For så vidt angår FISA:

- I Title I og III i FISA, der tillader henholdsvis elektronisk overvågning og fysiske ransagninger, stilles der krav om en retsafgørelse (med begrænsede undtagelser såsom nødsituationer), og der stilles krav om, at der altid skal være en begrundet mistanke om, at målet er en fremmed magt eller en agent fra en fremmed magt. Jf. 50 U.S.C. § 1805, 1824.
- USA FREEDOM Act af 2015 ændrede Title IV i FISA, som tillader anvendelsen af pen-register- og trap and trace-anordninger i medfør af en retsafgørelse (undtagen i nødsituationer) til at kræve, at regeringen baserer anmodninger om oplysninger på en "specifik selektor". Jf. 50 U.S.C. § 1842(c)(3).

- Title V i FISA, som tillader, at Federal Bureau of Investigation (FBI) indhenter visse former for forretningsoptegnelser, kræver, at der udstedes en retsafgørelse baseret på en anmodning, i henhold til hvilken "der er specifikke og præcise faktiske forhold, der giver grund til at antage, at den person, som optegnelserne vedrører, er en fremmed magt eller en agent for en fremmed magt". Jf. 50 U.S.C. § 1862(b)(2)(B) ⁽¹⁾.
- Endelig kan der i henhold til Section 702 i FISA "foretages en målrettet overvågning af personer, som med rimelighed kan antages at befinde sig uden for USA, med henblik på indsamling af efterretningsoplysninger". Jf. 50 U.S.C. § 1881a(a). Som rådet for tilsyn med privatlivets fred og borgerlige frihedsrettigheder har bemærket, er regeringens indsamling af data i henhold til Section 702 i FISA således "udelukkende rettet mod enkeltpersoner med henblik på at erhverve kommunikation, der er knyttet til disse personer, fra hvilke regeringen har grund til at forvente, at den vil kunne indhente visse typer udenlandske efterretninger", således at "programmet ikke opererer med masseindsamling af kommunikation". Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, s. 103 (2.7.2014) ⁽²⁾.

Med hensyn til de nationale sikkerhedsbreve indeholder USA FREEDOM Act af 2015 et krav om en "specifik selektor" ved anvendelsen af sådanne breve. Jf. 12 U.S.C. § 3414(a)(2), 15 U.S.C. § 1681u, 15 U.S.C. § 1681v(a), 18 U.S.C. § 2709(b).

Endvidere fastsættes det i præsidentielt dekret 14086, at "målrettet indsamling skal prioriteres", og — når efterretnings-samfundet foretager masseindsamling — at "masseindsamling af signalefterretninger kun er tilladt på grundlag af en afgørelse om, at de oplysninger, der er nødvendige for at fremme en valideret efterretningsprioritet, ikke med rimelighed kan opnås gennem målrettet indsamling". Jf. præsidentielt dekret 14086, § 2(c)(ii)(A).

Præsidentielt dekret 14086 indeholder yderligere garantier i det tilfælde, hvor efterretningssamfundet beslutter, at masseindsamling er i overensstemmelse med disse standarder. Nærmere bestemt stilles der i det præsidentielle dekret krav om, at efterretningstjenesten, når den foretager masseindsamling, "anvender rimelige metoder og tekniske foranstaltninger for at begrænse de indsamlede oplysninger til det, der er nødvendigt for at fremme en valideret efterretningsprioritet, samtidig med at indsamlingen af ikkerekvante oplysninger minimeres". Jf. idem. I dekretet hedder det endvidere, at "signalefterretningsaktiviteter", som omfatter søgning efter signalefterretninger indhentet ved masseindsamling, "kun udføres, efter at det på grundlag af en rimelig vurdering af alle relevante faktorer er fastslået, at aktiviteterne er nødvendige for at fremme en valideret efterretningsprioritet". Jf. idem § 2(a)(ii)(A). Dekretet gennemfører endvidere dette princip ved at fastslå, at efterretningstjenesten kun kan foretage søgninger i masseindsamlede, ikkeminimerede signalefterretninger med henblik på at nå seks tilladte mål, og at sådanne søgninger skal foretages i overensstemmelse med politikker og procedurer, der "tager behørigt hensyn til [søgningernes] indvirkning på privatlivets fred og de borgerlige frihedsrettigheder for alle personer, uanset deres nationalitet og opholdssted". Jf. idem § 2(c)(iii)(D). Endelig indeholder dekretet bestemmelser om håndtering af samt sikkerhed og adgangskontrol i forbindelse med indsamlede oplysninger. Jf. idem § 2(c)(iii)(A) og § 2(c)(iii)(B).

* * * * *

Vi håber, at disse præciseringer er til hjælp. De er velkommen til at kontakte os, hvis De har yderligere spørgsmål om, hvorledes den amerikanske efterretningstjeneste agter at gennemføre præsidentielt dekret 14086.

⁽¹⁾ Fra 2001 til 2020 tillod Title V i FISA, at FBI anmodede FISC om tilladelse til at indsamle "konkrete ting" (tangible things), der var relevante for visse godkendte undersøgelser. Jf. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). Denne formulering, som er forældet og dermed ikke længere en del af gældende lov, tillagde regeringen den beføjelse, hvorefter den engang kunne foretage masseindsamling af telefonmetadata. Selv før bestemmelsen blev forældet, havde USA FREEDOM Act imidlertid allerede ændret den, så der efterfølgende blev stillet krav om, at regeringen skulle basere en anmodning til FISC på en "specifik selektor". Jf. USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § 103 (2015).

⁽²⁾ I Section 703 og 704, som tillader efterretningssamfundet at foretage målrettet overvågning af amerikanske personer, der befinder sig i udlandet, stilles der krav om en retsafgørelse (undtagen i nødsituationer), og der stilles krav om, at der altid skal være en begrundet mistanke om, at målet er en fremmed magt, en agent fra en fremmed magt eller en ansat ved en fremmed magt. Jf. 50 U.S.C. § 1881b, 1881c.

Sincerely,

A handwritten signature in black ink, appearing to read 'C. FONZONE', followed by a horizontal line that ends in a vertical bar.

Christopher C. FONZONE
General Counsel

BILAG VIII

Liste over forkortelser

Følgende forkortelser anvendes i denne afgørelse:

AAA	American Arbitration Association (den amerikanske voldgiftssammenslutning)
Afgørelse	Kommissionens gennemførelsesafgørelse i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om et tilstrækkeligt beskyttelsesniveau for personoplysninger inden for EU-USA-databeskyttelsesrammen
AGG-DOM	Attorney General Guidelines for Domestic FBI Operations (justitsministerens retningslinjer for FBI's indenlandske operationer)
APA	Administrative Procedure Act (lov om administrative procedurer)
CIA	Central Intelligence Agency (den centrale efterretningstjeneste)
CNSS	Committee on National Security Systems (Udvalget for Nationale Sikkerhedssystemer)
DNI	Direktøren for den nationale efterretningstjeneste
DoJ	Department of Justice (det amerikanske justitsministerium)
Domstolen	Den Europæiske Unions Domstol
DPRC	Data Protection Review Court (databeskyttelsesappellretten)
ECOA	Equal Credit Opportunity Act (lov om lige kreditmuligheder)
ECPA	Electronic Communications Privacy Act (lov om databeskyttelse inden for elektronisk kommunikation)
EO 12333	Executive Order 12333 "United States Intelligence Activities" (præsidentielt dekret 12333 om de amerikanske efterretningsaktiviteter)
EO 14086, dekretet	Executive Order 14086 "Enhancing Safeguards for US Signals Intelligence Activities" (præsidentielt dekret 14086 om fremme af garantier i de amerikanske signalefterretningsaktiviteter)
EØS	Det Europæiske Økonomiske Samarbejdsområde
FBI	Federal Bureau of Investigation (forbundspolitiet)
FCRA	Fair Credit Reporting Act (lov om retfærdig kreditrapportering)
FISA	Foreign Intelligence Surveillance Act (lov om overvågning af efterretningsvirksomhed i udlandet)
FISC	Foreign Intelligence Surveillance Court (den amerikanske domstol for overvågning af efterretningsvirksomhed i udlandet)
FISCR	Foreign Intelligence Surveillance Court of Review (den amerikanske appeldomstol for overvågning af efterretningsvirksomhed i udlandet)
FOIA	Freedom of Information Act (lov om informationsfrihed)
Forordning (EU) 2016/679	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)
FRA	Federal Records Act (lov om forbundsregistret)
FTC	Federal Trade Commission (den amerikanske konkurrencemyndighed)

HIPAA	Health Insurance Portability and Accountability Act (lov om portabilitet og ansvarlighed vedrørende sundhedsforsikring)
ICDR	International Centre for Dispute Resolution (internationalt center for tvistbilæggelse)
IOB	Intelligence Oversight Board (tilsynsmyndigheden for efterretningsvirksomhed)
Justitsministerens forordning	Forordning om Data Protection Review Court udstedt af den amerikanske justitsminister
NIST	National Institute of Standards and Technology (det nationale institut for standarder og teknologi)
NSA	National Security Agency (den nationale sikkerhedsmyndighed)
NSL	National Security Letter(s) (nationale sikkerhedsbrev(e))
ODNI	Office of the Director of National Intelligence (kontoret for direktøren for den nationale efterretningstjeneste)
ODNI CLPO, CLPO	Civil Liberties Protection Officer of the Director of National Intelligence (den ansvarlige for beskyttelse af borgerlige frihedsrettigheder under direktøren for den nationale efterretningstjeneste)
OMB	Office of Management and Budget (forvaltnings- og budgetkontoret)
OPCL	Office of Privacy and Civil Liberties of the Department of Justice (justitsministeriets kontor for privatlivets fred og borgerlige frihedsrettigheder)
PCLOB	Privacy and Civil Liberties Oversight Board (Rådet for Tilsyn med Privatlivets Fred og Borgerlige Rettigheder)
PIAB	President's Intelligence Advisory Board (presidentens rådgivande styrelse for efterretningsvirksomhed)
PPD 28	Presidential Policy Directive 28 (præsidentielt direktiv 28)
Principperne	Principperne i EU-USA-databeskyttelsesrammen
SAOP	Senior Agency Official for Privacy (øverste embedsmand for privatlivets fred)
Unionen	Den Europæiske Union
USA	De Forenede Stater