

II

(Ikke-lovgivningsmæssige retsakter)

AFGØRELSER

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2016/1250

af 12. juli 2016

i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred

(meddelt under nummer C(2016) 4176)

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ⁽¹⁾, særlig artikel 25, stk. 6,

efter høring af Den Europæiske Tilsynsførende for Databeskyttelse ⁽²⁾, og

1. INDLEDNING

- (1) I direktiv 95/46/EF fastsættes reglerne for overførsel af personoplysninger fra medlemsstaterne til tredjelande, i det omfang overførslen falder inden for direktivets anvendelsesområde.
- (2) Det fastslås i artikel 1 i direktiv 95/46/EF og af anden og tiende betragtning hertil, at direktivet ikke alene har til formål at sikre en effektiv og fuldstændig beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især den grundlæggende ret til respekt for privatlivet i forbindelse med behandling af personoplysninger, men også et højt beskyttelsesniveau for disse grundlæggende rettigheder og frihedsrettigheder ⁽³⁾.
- (3) Betydningen af såvel den grundlæggende ret til respekt for privatlivet, der er sikret ved artikel 7, som den grundlæggende ret til beskyttelse af personoplysninger, der er sikret ved artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder, er desuden fremhævet i Domstolens retspraksis ⁽⁴⁾.
- (4) Medlemsstaterne skal i henhold til artikel 25, stk. 1, i direktiv 95/46/EF fastsætte bestemmelser om, at overførsel af personoplysninger til et tredjeland kun må finde sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, og hvis den pågældende medlemsstats lovgivning til gennemførelse af direktivets andre bestemmelser overholdes forud for overførslen. Kommissionen kan fastslå, at et tredjeland sikrer et sådant tilstrækkeligt beskyttelsesniveau på grundlag af dets nationale lovgivning eller dets internationale forpligtelser med henblik på at beskytte den enkeltes grundlæggende rettigheder. I så fald kan der overføres personoplysninger fra medlemsstaterne, uden at det er nødvendigt, at der stilles yderligere garantier, forudsat at de nationale bestemmelser, der vedtages til gennemførelse af direktivets øvrige bestemmelser, overholdes.

⁽¹⁾ EFT L 281 af 23.11.1995, s. 31.

⁽²⁾ Se udtalelse 4/2016 om udkastet til afgørelse om tilstrækkeligheden af EU's og USA's værn om privatlivets fred, som blev offentliggjort den 30. maj 2016.

⁽³⁾ Sag C-362/14, Maximillian Schrems mod Data Protection Commissioner («Schrems»), EU:C:2015:650, præmis 39.

⁽⁴⁾ Sag C-553/07, Rijkeboer, EU:C:2009:293, præmis 47, forenede sager C-293/12 og C-594/12, Digital Rights Ireland m.fl., EU:C:2014:238, præmis 53, sag C-131/12, Google Spain og Google, EU:C:2014:317, præmis 53, 66 og 74.

- (5) I henhold til artikel 25, stk. 2, i direktiv 95/46/EF skal vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, ske på grundlag af samtlige de forhold, der har indflydelse på en overførsel eller en type overførsel af oplysninger, herunder de retsregler — almindelige regler eller sektorregler — der er i kraft i det pågældende tredjeland.
- (6) Det fremgår af Kommissionens beslutning 2000/520/EF ⁽⁵⁾, at »safe harbour-principperne«, der finder anvendelse i overensstemmelse med de normgivende såkaldte »hyppige spørgsmål« fra det amerikanske handelsministerium, på grundlag af artikel 25, stk. 2, i direktiv 95/46/EF, formodes at sikre et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til foretagender i USA.
- (7) I sine meddelelser COM(2013) 846 final ⁽⁶⁾ og COM(2013) 847 final ⁽⁷⁾ af 27. november 2013 anførte Kommissionen, at grundlaget for safe harbour-ordningen skal tages op til fornyet overvejelse og styrkes i betragtning af en række faktorer, herunder den eksponentielle stigning i datastrømme og deres afgørende betydning for den transatlantiske økonomi, den hurtige vækst i antallet af amerikanske virksomheder, der følger safe harbour-ordningen, og nye oplysninger om omfanget og udbredelsen af visse amerikanske efterretningsprogrammer, der rejser nye spørgsmål om det beskyttelsesniveau, som safe harbour-ordningen kan sikre. Kommissionen konstaterede desuden en række mangler i safe harbour-ordningen.
- (8) Baseret på dokumentation, som er indsamlet af Kommissionen, bl.a. som led i arbejdet i EU-USA-kontaktgruppen vedrørende beskyttelse af privatlivets fred ⁽⁸⁾ og oplysninger om amerikanske efterretningsprogrammer, som er blevet fremlagt i EU-USA-ad hoc-arbejdsgruppen ⁽⁹⁾, udarbejdede Kommissionen 13 anbefalinger vedrørende en gennemgang af safe harbour-ordningen. Disse anbefalinger fokuserede på styrkelse af de materielle principper om beskyttelse af privatlivets fred, øget gennemsigtighed i amerikanske selvcertificerede virksomheders privatlivspolitikker, bedre tilsyn, overvågning og håndhævelse fra de amerikanske myndigheders side af virksomhedernes overholdelse af principperne, økonomisk overkommelige tvistbilæggelsesmekanismer og behovet for at sikre, at den nationale sikkerhedsundtagelse i beslutning 2000/520/EF kun anvendes, når det er strengt nødvendigt eller proportionalt.
- (9) I sin dom af 6. oktober 2015 i sag C-362/14, Maximilian Schrems mod Data Protection Commissioner ⁽¹⁰⁾, erklærede Domstolen beslutning 2000/520/EF ugyldig. Uden at undersøge indholdet af safe harbour-principperne om beskyttelse af privatlivets fred bemærkede Domstolen, at Kommissionen ikke havde anført i nævnte beslutning, at USA faktisk »sikrer« et tilstrækkeligt beskyttelsesniveau på grundlag af landets nationale lovgivning eller dets internationale forpligtelser ⁽¹¹⁾.
- (10) Domstolen forklarede i denne forbindelse, at udtrykket »et tilstrækkeligt beskyttelsesniveau«, der er indeholdt i artikel 25, stk. 6, i direktiv 95/46/EF, ganske vist ikke indebærer et beskyttelsesniveau, som er identisk med det niveau, der er sikret i EU's retsorden, men at det imidlertid skal forstås således, at det opstiller et krav om, at tredjelandet sikrer et beskyttelsesniveau for de grundlæggende rettigheder og frihedsrettighederne, som »i det væsentlige svarer til« det niveau, der er sikret i EU i medfør af direktiv 95/46/EF sammenholdt med chartret om grundlæggende rettigheder. Selv om de midler, som tredjelandet anvender i denne henseende, kan være forskellige fra de midler, som anvendes inden for EU, skal disse midler ikke desto mindre i praksis vise sig at være effektive ⁽¹²⁾.
- (11) Domstolen kritiserede, at beslutning 2000/520/EF ikke indeholdt nogen konstateringer om, hvorvidt der i USA foreligger regler af statslig karakter, hvorved det tilsigtes at begrænse eventuelle indgreb i de grundlæggende rettigheder hos de personer, hvis oplysninger bliver overført fra EU til USA, hvilke indgreb de statslige enheder i dette land er beføjede til at foretage, når der herved forfølges legitime mål, såsom statens sikkerhed, eller om hvorvidt der foreligger en effektiv domstolsbeskyttelse mod indgreb af denne art ⁽¹³⁾.

⁽⁵⁾ Kommissionens beslutning 2000/520/EF af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbour-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium (EFT L 215 af 28.8.2000, s. 7).

⁽⁶⁾ Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om genopbygning af tilliden til datastrømmene mellem EU og USA, COM(2013) 846 final af 27.11.2013.

⁽⁷⁾ Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om, hvordan safe harbour-ordningen fungerer for så vidt angår EU-borgerne og virksomhederne i EU, COM(2013) 847 final af 27.11.2013.

⁽⁸⁾ Se f.eks. Rådet for Den Europæiske Union, endelig rapport fra EU-USA-Kontaktgruppen på Højt Plan om Informationsdeling og Beskyttelse af Privatlivets Fred og Personoplysninger, notat 9831/08 af 28. maj 2008, tilgængeligt på internettet på adressen: <http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf>.

⁽⁹⁾ Rapport om resultaterne af EU's fælles formandskab for ad hoc-gruppen mellem EU og USA om databeskyttelse af 27.11.2013, tilgængelig på internettet på adressen: <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>.

⁽¹⁰⁾ Se fodnote 3.

⁽¹¹⁾ Schrems-dommen, præmis 97.

⁽¹²⁾ Schrems-dommen, præmis 73-74.

⁽¹³⁾ Schrems-dommen, præmis 88-89.

- (12) I 2014 havde Kommissionen indledt drøftelser med de amerikanske myndigheder om en styrkelse af safe harbour-ordningen i overensstemmelse med de 13 anbefalinger i meddelelsen COM(2013) 847 final. Efter Domstolens dom i Schrems-sagen blev disse drøftelser intensiveret med henblik på en mulig ny afgørelse om et tilstrækkeligt beskyttelsesniveau, der opfylder kravene i artikel 25 i direktiv 95/46/EF som fortolket af Domstolen. De dokumenter, der er knyttet til nærværende afgørelse, og som ligeledes vil blive offentliggjort i USA's Federal Register, er resultatet af disse drøftelser. Principperne om beskyttelse af privatlivets fred (bilag II) og de officielle udredninger og tilsagn afgivet af forskellige amerikanske myndigheder i bilag I og III-VII udgør »EU's og USA's værn om privatlivets fred«.
- (13) Kommissionen har foretaget en grundig analyse af amerikansk ret og praksis, herunder af disse officielle udredninger og tilsagn. På grundlag af overvejelserne i betragtning 136-140 konkluderer Kommissionen, at USA sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres under EU's og USA's værn om privatlivets fred fra EU til selvcertificerede foretagender i USA.

2. EU'S OG USA'S VÆRN OM PRIVATLIVETS FRED

- (14) EU's og USA's værn om privatlivets fred er baseret på et selvcertificeringssystem, hvorved amerikanske foretagender forpligter sig til at overholde en række principper om beskyttelse af privatlivets fred — principperne i ordningen for EU's og USA's værn om privatlivets fred, herunder de supplerende principper (herefter samlet benævnt: »principperne«) — opstillet af det amerikanske handelsministerium og indeholdt i bilag II til denne afgørelse. Det finder anvendelse for såvel dataansvarlige som databehandlere (mandatarer) med den præcisering, at databehandlere 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 rettigheder i henhold til principperne ⁽¹⁴⁾.
- (15) Uden at dette berører pligten til at overholde de nationale bestemmelser, der er vedtaget i henhold til direktiv 95/46/EF, medfører denne afgørelse tilladelse til at foretage overførsler fra en dataansvarlig eller databehandler i EU til foretagender i USA, der har anmeldt selvcertificering om tilslutning til principperne til det amerikanske handelsministerium og har forpligtet sig til at overholde dem. Principperne finder alene anvendelse for det amerikanske foretagendes behandling af personoplysninger for så vidt som disse foretagenders behandling ikke er omfattet af EU-lovgivningen ⁽¹⁵⁾. Værnet om privatlivets fred berører ikke anvendelsen af EU-lovgivningen vedrørende behandling af personoplysninger i medlemsstaterne ⁽¹⁶⁾.

⁽¹⁴⁾ Se bilag II, afsnit III, punkt 10.a. I overensstemmelse med definitionen i afsnit I, punkt 8.c, bestemmer den dataansvarlige i EU formålet med samt metoderne til behandling af personoplysningerne. Det skal desuden tydeligt fremgå af aftalen med mandatarer, om videreoverførsel er tilladt (jf. afsnit III, punkt 10.a.ii.2).

⁽¹⁵⁾ Det gælder ligeledes for overførslen fra EU af oplysninger om menneskelige ressourcer i forbindelse med ansættelsesforhold. Selv om principperne understreger, at EU-foretagendet er hovedansvarligt (jf. bilag II, afsnit III, punkt 9.d.i), præciseres det også, at foretagendets adfærd er underlagt de gældende regler i EU og/eller den pågældende medlemsstat og ikke principperne. Jf. bilag II, afsnit III, punkt 9.a.i, 9.b.ii, 9.c.i og 9.d.i.

⁽¹⁶⁾ Det gælder også behandling under anvendelse af udstyr, der befinder sig i EU, men anvendes af et foretagende, der er etableret uden for EU (jf. artikel 4, stk. 1, litra c), i direktiv 95/46/EF). Fra den 25. maj 2018 finder den generelle forordning om databeskyttelse anvendelse for behandling af persondata, i) som foretages som led i aktiviteter, der udføres af et foretagende eller en dataansvarlig eller databehandler, der er etableret i Unionen (selv om behandlingen finder sted i USA), eller ii) om registrerede, der er i Unionen, som foretages af en dataansvarlig eller databehandler, der ikke er etableret i Unionen, hvis behandlingsaktiviteterne vedrører a) udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet, eller b) overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen. Jf. artikel 3, stk. 1 og 2, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

- (16) Beskyttelsen af personoplysninger under værnet om privatlivets fred gælder alle registrerede i EU ⁽¹⁷⁾, hvis personoplysninger er overført fra Unionen til foretagender i USA, der har anmeldt deres selvcertificering om tilslutning til principperne til det amerikanske handelsministerium.
- (17) Principperne finder anvendelse straks efter certificering. Der gælder dog en undtagelse for princippet om ansvar for videreoverførsel, i de tilfælde hvor et foretagende, der har anmeldt selvcertificering om tilslutning til værnet om privatlivets fred, allerede har forretningsforbindelser med tredjeparter. Da det kan tage tid at bringe disse eksisterende forretningsforbindelser i overensstemmelse med bestemmelserne under princippet om ansvar for videreoverførsel, vil foretagendet være forpligtet til at gøre dette hurtigst muligt og under alle omstændigheder senest ni måneder efter selvcertificering (forudsat at dette sker inden for de første to måneder efter iværksættelsen af værnet om privatlivets fred). I denne overgangsperiode skal foretagendet anvende principperne om oplysningspligt og valgfrihed (og således give den EU-registrerede mulighed for at modsætte sig anvendelse) og, hvis personoplysningerne overføres til en tredjepart, der fungerer som mandatar, sikre, at sidstnævnte som minimum yder det samme niveau af beskyttelse som krævet efter principperne ⁽¹⁸⁾. Denne overgangsperiode sikrer en rimelig og passende balance mellem den grundlæggende ret til beskyttelse af dataoplysninger og virksomhedernes legitime behov for tilstrækkelig tid til at tilpasse sig de nye rammer, især når dette berører deres eksisterende forretningsforbindelser med tredjeparter.
- (18) Ordningen vil blive forvaltet og overvåget af det amerikanske handelsministerium på grundlag af ministeriets tilsagn i udredningerne fra den amerikanske handelsminister (bilag I til denne afgørelse). Med hensyn til håndhævelsen af principperne har Federal Trade Commission (FTC) (den føderale handelskommission) og det amerikanske transportministerium udarbejdet udredninger, der er indeholdt i bilag IV og V til denne afgørelse).

2.1. Principper om beskyttelse af privatlivets fred

- (19) Som led i deres selvcertificering under EU's og USA's værn om privatlivets fred skal foretagender forpligte sig til at overholde principperne ⁽¹⁹⁾.
- (20) I henhold til *princippet om oplysningspligt* skal foretagender give oplysninger til registrerede om en række centrale elementer vedrørende behandlingen af deres personoplysninger (f.eks. type af indsamlede oplysninger, formål med behandlingen, retten til indsigt og valgfrihed, betingelser for videreoverførsel og ansvar). Der findes yderligere garantier, hvorved foretagender navnlig skal offentliggøre deres privatlivspolitik (som afspejler principperne) og angive link til handelsministeriets websted (med yderligere oplysninger om selvcertificering, de registreredes rettigheder og tilgængelige klageinstanser), listen over deltagere i værnet om privatlivets (omhandlet i betragtning 30) og webstedet for relevant udenretslig tvistbilæggesinstans.
- (21) I henhold til *princippet om dataintegritet og formålsbegrænsning* skal personoplysninger begrænses til oplysninger, der er relevante for formålet med behandlingen og er pålidelige, nøjagtige, fuldstændige og ajourførte. Et foretagende må 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. Foretagender skal sikre, at personoplysningerne er pålidelige, nøjagtige, fuldstændige og ajourførte.

⁽¹⁷⁾ 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. EU's bestemmelser om databeskyttelse, herunder direktiv 95/46/EF, er indeholdt i EØS-aftalen og er blevet indarbejdet i bilag XI til aftalen. Det Blandede EØS-Udvalg skal træffe beslutning om indarbejdelsen af denne afgørelse i EØS-aftalen. Så snart denne afgørelse finder anvendelse for Island, Liechtenstein og Norge, vil EU's og USA's værn om privatlivets fred også dække disse tre lande, og alle henvisninger til EU og dets medlemsstater i pakken for værnet om privatlivets fred skal læses som omfattende Island, Liechtenstein og Norge.

⁽¹⁸⁾ Jf. bilag II, afsnit III, punkt 6.e.

⁽¹⁹⁾ Særlige regler om yderligere garantier finder anvendelse på oplysninger om menneskelige ressourcer, der indsamles inden for rammerne af et ansættelsesforhold, jf. det supplerende princip om »oplysninger om menneskelige ressourcer« (se bilag II, afsnit III, punkt 9). Arbejdsgivere bør f.eks. respektere de ansattes ønsker om hemmeligholdelse af personoplysninger ved at give begrænset indsigt i personoplysninger, gøre visse oplysninger anonyme, eller anvende koder eller pseudonymer. Særligt skal foretagender samarbejde med og følge anbefalingerne fra databeskyttelsesmyndighederne i EU vedrørende sådanne oplysninger.

- (22) Hvis et nyt (ændret) formål er væsentligt forskelligt men stadig foreneligt med det oprindelige formål, giver *princippet om valgfrihed* den registrerede ret til at modsætte sig anvendelsen af oplysningerne. *Princippet om valgfrihed* træder ikke i stedet for det udtrykkelige forbud mod uforenelig behandling ⁽²⁰⁾. Ved direkte markedsføring gælder der særlige bestemmelser, der generelt giver mulighed for til enhver tid at vælge ikke at lade sine personoplysninger anvende (opt out) ⁽²¹⁾. I tilfælde af følsomme oplysninger skal de pågældende foretagender normalt indhente den registreredes udtrykkelige samtykke (opt in).
- (23) I henhold til *princippet om dataintegritet og formålsbegrænsning* må personlige oplysninger dog alene opbevares i en form, der giver mulighed for at identificere eller gøre en person identificerbar (dvs. i form af personoplysninger), for så vidt som det tjener de(t) formål, hvortil de oprindeligt blev indsamlet eller efterfølgende godkendt. Denne pligt forhindrer ikke foretagender, der indgår i værnet om privatlivets fred, i at fortsætte med behandlingen af personoplysninger i længere perioder, men dog kun så længe og i det omfang en sådan behandling i rimeligt omfang tjener et af følgende formål: arkivering i samfundets interesse, journalistik, kunst og litteratur, videnskabelig og historisk forskning samt statistisk analyse. En længere opbevaring af personoplysninger til et af disse formål vil være underlagt garantierne i principperne.
- (24) I henhold til *princippet om sikkerhed* skal foretagender, der opretter, vedligeholder, anvender eller spreder personoplysninger træffe »rimelige og passende« sikkerhedsforanstaltninger under hensyntagen til de risici, som behandlingen indebærer, og de pågældende oplysningers karakter. I forbindelse med udlicitering af databehandling skal foretagender indgå en aftale med den underkontraherede databehandler, der sikrer det samme niveau af beskyttelse som i principperne, og sørge for, at den gennemføres korrekt.
- (25) I henhold til *princippet om indsigt* ⁽²²⁾ har registrerede ret til uden begrundelse og mod betaling af et rimeligt gebyr at få oplyst, om et foretagende behandler personoplysninger om dem, og til at få udleveret oplysningerne inden for en rimelig tid. Denne ret kan kun begrænses i ekstraordinære tilfælde; enhver nægtelse eller begrænsning af retten til indsigt skal være nødvendig og behørigt begrundet, og foretagendet skal dokumentere, at disse krav er opfyldt. Registrerede skal have mulighed for at rette, ændre eller slette ukorrekte oplysninger eller oplysninger behandlet i strid med principperne. På de områder, hvor foretagender ofte anvender automatiseret behandling af personoplysninger til at træffe beslutninger vedrørende en fysisk person (f.eks. långivning, realkreditlån, ansættelse), indeholder amerikansk ret særlige garantier vedrørende negative beslutninger ⁽²³⁾. Disse retsakter 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. Reglerne indeholder garantier i formodentlig meget begrænsede tilfælde, hvor de automatiserede beslutninger træffes af foretagender, der indgår i værnet om privatlivets fred ⁽²⁴⁾. I betragtning af, at automatiseret behandling (herunder profilering) i stigende grad anvendes som grundlag for beslutninger vedrørende fysiske personer i den moderne digitale økonomi, er dette ikke desto mindre et område, der skal overvåges nøje. Med henblik på at lette denne overvågning er man nået til enighed med de amerikanske myndigheder om at afholde drøftelser om automatiserede beslutninger, herunder at drøfte ligheder og forskelle i EU's og USA's praksis, som led i den første årlige evaluering samt, efter behov, ved efterfølgende evalueringer.

⁽²⁰⁾ Det gælder alle overførsler af oplysninger inden for rammerne af værnet om privatlivets fred, også oplysninger der er indsamlet i forbindelse med ansættelsesforhold. Et selvcertificeret foretagende i USA kan i princippet benytte oplysninger om menneskelige ressourcer til andre, ikke-ansættelsesrelaterede formål (f.eks. i forbindelse med markedsføring), men det skal overholde forbuddet mod uforenelig behandling og en sådan brug må udelukkende ske i overensstemmelse med *principperne om oplysningspligt og valgfrihed*. Forbuddet for det amerikanske foretagende 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.

⁽²¹⁾ Jf. bilag II, afsnit III, punkt 12.

⁽²²⁾ Se også det supplerende princip om »Indsigt« (bilag II, afsnit III, punkt 8).

⁽²³⁾ Se bl.a. Equal Credit Opportunity Act (ECOA, 15 U.S.C. 1691 et seq.), Fair Credit Reporting Act (FCRA, 15 USC § 1681 et seq.) eller Fair Housing Act (FHA, 42 U.S.C. 3601 et seq.).

⁽²⁴⁾ Ved overførsel af personoplysninger, der er blevet indsamlet i EU, vil aftaleforholdet med den registrerede (kunden) i de fleste tilfælde være indgået af — og derfor vil enhver beslutning baseret på automatiseret behandling typisk være truffet af — den dataansvarlige i EU, som skal overholde EU's bestemmelser om databeskyttelse. Det omfatter også de tilfælde, hvor behandlingen foretages af et foretagende, der indgår i værnet om privatlivets fred, og der fungerer som mandatar for den dataansvarlige i EU.

- (26) I henhold til *princippet om klageadgang, håndhævelse og ansvar* ⁽²⁵⁾ skal de deltagende foretagender sørge for robuste mekanismer til at sikre overholdelsen af de øvrige principper og klageadgang for registrerede i EU, hvis personoplysninger er blevet behandlet i strid med principperne, herunder effektive retsmidler. Når et foretagende frivilligt har besluttet at foretage selvcertificering ⁽²⁶⁾ under EU's og USA's værn om privatlivets fred, skal det overholde principperne til fulde. For fortsat at kunne modtage personoplysninger fra EU inden for rammerne af værnet om privatlivets fred skal disse foretagender årligt recertificere deres deltagelse. Foretagender skal desuden træffe foranstaltninger til at kontrollere ⁽²⁷⁾, at deres offentliggjorte privatlivspolitik 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 foretagendets privatlivspolitik, og at overholdelsen kontrolleres regelmæssigt og objektivt, eller gennem ekstern kontrol af overholdelsen, der kan omfatte revision eller stikprøvekontrol. Foretagendet skal også indføre en effektiv klagemekanisme til behandling af eventuelle klager (se også betragtning 43) og være omfattet af de undersøgelses- og håndhælsesbeføjelser, der er tillagt FTC, det amerikanske transportministerium eller et andet kompetent organ, der vil sikre overholdelsen af principperne.
- (27) Der gælder særlige regler for såkaldte »videreoverførsler«, dvs. overførsler af personoplysninger fra et foretagende til en tredjepart (dataansvarlig eller databehandler), uanset om denne befinder sig i USA eller i et tredjeland uden for USA (og EU). Formålet med disse regler er at sikre, at den garanterede beskyttelse af EU-registreredes personoplysninger ikke undergraves og ikke kan omgås ved at overføre dem til tredjeparter. Det er særlig relevant i mere komplekse behandlingskæder, som er typiske for vor tids digitale økonomi.
- (28) I henhold til *princippet om ansvar for videreoverførsel* ⁽²⁸⁾ kan videreoverførsel alene finde sted i) til begrænsede og bestemte formål, ii) på grundlag af en aftale (eller tilsvarende arrangement i en koncern ⁽²⁹⁾) og iii) udelukkende, hvis denne aftale sikrer samme niveau af beskyttelse som principperne, som indeholder krav om, at anvendelsen af principperne kun kan begrænses, for så vidt som det er nødvendigt af hensyn til national sikkerhed, retshåndhævelse og andre almene interesser ⁽³⁰⁾. Dette bør ses i sammenhæng med *princippet om oplysningspligt* og, i tilfælde af videreoverførsel til en dataansvarlig tredjepart ⁽³¹⁾, *princippet om valgfrihed*, ifølge hvilke den registrerede skal oplyses om (bl.a.) typen/identiteten af en eventuel tredjepartsmodtager, formålet med videreoverførslen samt om det valg, vedkommende kan træffe om at modsætte sig (opt out) eller, i forbindelse med følsomme oplysninger, at give sit udtrykkelige samtykke (opt in) til videreoverførslen. Med hensyn til *princippet om dataintegritet og formålsbegrænsning* indebærer forpligtelsen til at yde samme niveau af beskyttelse som under principperne, at tredjeparten udelukkende må råde over de personoplysninger, der er blevet overført til denne til formål, der ikke er i strid med de formål, hvortil oplysningerne oprindeligt blev indsamlet eller efterfølgende godkendt af den registrerede.
- (29) 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. Under alle omstændigheder skal det fastslås i aftalen med den modtagende tredjepart, at denne underretter foretagendet i værnet om privatlivets fred, hvis den beslutter, at den ikke længere

⁽²⁵⁾ Se også det supplerende princip om »Bilæggelse af tvister og håndhævelse« (bilag II, afsnit III, punkt 11).

⁽²⁶⁾ Se også det supplerende princip om »Selvcertificering« (bilag II, afsnit III, punkt 6).

⁽²⁷⁾ Se også det supplerende princip om »Kontrol (verifikation)« (bilag II, afsnit III, punkt 7).

⁽²⁸⁾ Se også det supplerende princip om »Obligatoriske aftaler om videreoverførsel« (bilag II, afsnit III, punkt 10).

⁽²⁹⁾ Se også det supplerende princip om »Obligatoriske aftaler om videreoverførsel« (bilag II, afsnit III, punkt 10.b). Selv om dette princip giver mulighed for overførsler, der også er baseret på ikke-kontraktlige 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 det selvcertificerede foretagende i USA fortsat vil skulle overholde principperne, vil det have et stærkt incitament til at benytte instrumenter, som rent faktisk fungerer godt i praksis.

⁽³⁰⁾ Jf. bilag II, afsnit I, punkt 12.

⁽³¹⁾ Registrerede har ikke ret til at modsætte sig, hvis personoplysningerne overføres til en tredjepart, der fungerer som mandatar og udfører opgaver på vegne af det amerikanske foretagende og i henhold til dets anvisninger. Det kræver dog, at der er indgået en aftale med mandataren, og at det amerikanske foretagende bærer ansvaret for at garantere den beskyttelse, der skal ydes i henhold til principperne, ved at udnytte dets anvisningsbeføjelser.

kan opfylde denne pligt. Når en tredjepart træffer en sådan beslutning, skal den pågældende tredjepart ophøre med at behandle oplysningerne eller træffe andre rimelige og passende skridt for at rette op på situationen ⁽³²⁾. I tilfælde af problemer med overholdelsen i udliciterings- eller behandlingskæden skal foretagendet i værnet om privatlivets fred, som fungerer som dataansvarlig for personoplysningerne, bevise, at det ikke er skyld i den begivenhed, der medførte skaden, og i modsat fald påtage sig ansvaret, jf. *princippet om klageadgang, håndhævelse og ansvar*. Der gælder yderligere garantier i tilfælde af en videreoverførsel til en tredjepart, der fungerer som mandatar ⁽³³⁾.

2.2. Gennemsigtighed og forvaltning af samt tilsyn med EU's og USA's værn om privatlivets fred

- (30) EU's og USA's værn om privatlivets fred indeholder tilsyns- og håndhævelsesmekanismer for at kontrollere og sikre, at selvcertificerede foretagender i USA overholder principperne, og at der tages hånd om eventuel manglende overholdelse. Disse mekanismer er indeholdt i principperne (bilag II) og de tilsagn, der er afgivet af det amerikanske handelsministerium (bilag I), FTC (bilag IV) og det amerikanske transportministerium (bilag V).
- (31) For at sikre en korrekt anvendelse af EU's og USA's værn om privatlivets fred skal interesserede parter, f.eks. registrerede, dataeksportører og de nationale databeskyttelsesmyndigheder kunne identificere de foretagender, der har tilsluttet sig principperne. Handelsministeriet har til dette formål påtaget sig at føre og offentliggøre en liste over foretagender, der på grundlag af selvcertificering har tilsluttet sig principperne, og som er underlagt mindst en af de håndhævelsesmyndigheder, der er nævnt i bilag I og II til denne afgørelse («listen over deltagere i værnet om privatlivets fred») ⁽³⁴⁾. Handelsministeriet vil ajourføre listen på grundlag af et foretagendes årlige anmeldelser om recertificering, og når et foretagende trækker sig ud af eller udelukkes fra EU's og USA's værn om privatlivets fred. Ministeriet vil ligeledes føre og offentliggøre en officiel fortegnelse over foretagender, der er blevet fjernet fra listen, og i hvert enkelt tilfælde angive årsagen hertil. Endelig vil ministeriet angive et link til listen over FTC-håndhævelsessager relateret til værnet om privatlivets fred på FTC's websted.
- (32) Handelsministeriet offentliggør både listen over deltagere i værnet om privatlivets fred og anmeldelserne om recertificering på et særligt websted. De selvcertificerede foretagender skal til gengæld meddele deres webadresser til handelsministeriet med henblik på optagelse på listen. Hvis et foretagendes privatlivspolitik er tilgængeligt online, skal det desuden indeholde et link til webstedet for værnet om privatlivets fred samt et link til webstedet og klageformularer for den uafhængige klageinstans, der kan behandle åbne klager. Det amerikanske handelsministerium vil i forbindelse med et foretagendes certificering eller recertificering af sin deltagelse i ordningen systematisk kontrollere, om foretagendets privatlivspolitik er i overensstemmelse med principperne.
- (33) Foretagender, der vedvarende overtræder principperne, vil blive fjernet fra listen over deltagere i værnet om privatlivets fred, og de skal tilbagesende eller slette modtagne personoplysninger under EU's og USA's værn om privatlivets fred. I andre tilfælde af fjernelse, f.eks. frivillig udtræden eller manglende recertificering, kan foretagendet beholde disse oplysninger, 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). I dette tilfælde skal et foretagende udpege et kontaktpunkt i foretagendet for alle spørgsmål relateret til værnet om privatlivets fred.
- (34) Handelsministeriet vil desuden overvåge foretagender, der ikke længere deltager i EU's og USA's værn om privatlivets fred, enten fordi de frivilligt har trukket sig ud, eller fordi deres certificering er udløbet, for at kontrollere, om de agter at tilbagesende, slette eller beholde ⁽³⁵⁾ de personoplysninger, som de tidligere har

⁽³²⁾ 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 foretagendet i værnet om privatlivets fred — som har ansvaret for behandlingen og giver anvisninger til mandataren — som skal træffe disse foranstaltninger.

⁽³³⁾ I dette tilfælde skal det amerikanske foretagende også træffe rimelige og passende foranstaltninger til i) at sikre, at mandataren behandler de overførte personoplysninger i overensstemmelse med foretagendets pligter i henhold til principperne, og ii) at standse og bringe orden i uautoriseret behandling efter eventuel meddelelse herom.

⁽³⁴⁾ Bilag I og II indeholder oplysninger om varetagelsen af listen over deltagere i værnet om privatlivets fred (afsnit I, punkt 2, afsnit I, punkt 4, afsnit III, punkt 6.d og afsnit III, punkt 11.g).

⁽³⁵⁾ Se bl.a. bilag II, afsnit I, punkt 3, afsnit III, punkt 6.f og afsnit III, punkt 11.g.i.

modtaget under ordningen. Hvis de beholder oplysningerne, skal foretagenderne fortsætte med at anvende principperne. Hvis handelsministeriet har fjernet foretagender fra listen over deltagere i værnet på grund af vedvarende overtrædelse af principperne, vil ministeriet sikre, at disse foretagender tilbagesender eller sletter de personoplysninger, som de modtog under ordningen.

- (35) Hvis et foretagende af den ene eller anden årsag forlader EU's og USA's værn om privatlivets fred, skal det fjerne alle offentlige udtalelser, der lader formode, at foretagendet fortsat deltager i EU's og USA's værn om privatlivets fred eller er berettiget til at drage fordel heraf, navnlig alle henvisninger til EU's og USA's værn om privatlivets fred i den offentliggjorte privatlivspolitik. Handelsministeriet vil holde udkig efter og sætte ind over for falske påstande om deltagelse i ordningen, herunder påstande fremsat af tidligere deltagere ⁽³⁶⁾. Et foretagende, der afgiver urigtige oplysninger til offentligheden vedrørende dets 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 indbringes i henhold til False Statements Act (18 U.S.C. § 1001) ⁽³⁷⁾.
- (36) Handelsministeriet vil ex officio føre tilsyn med falske påstande om deltagelse i værnet om privatlivets fred eller uretmæssig brug af certificeringsmærket for værnet om privatlivets fred, og databeskyttelsesmyndighederne kan henvise foretagender til et særligt kontaktpunkt i ministeriet med henblik på kontrol. Hvis et foretagende har trukket sig ud af EU's og USA's værn om privatlivets fred, ikke foretager en recertificering eller fjernes fra listen over deltagere i værnet om privatlivets fred, vil handelsministeriet løbende kontrollere, at foretagendet har slettet alle henvisninger til værnet om privatlivets fred i sin offentliggjorte privatlivspolitik, der lader formode, at foretagendet fortsat deltager heri, og — hvis foretagendet fortsætter med at fremsætte falske påstande — henvise sagen til FTC, transportministeriet eller en anden kompetent myndighed med henblik på eventuelle foranstaltninger. Ministeriet vil ligeledes fremsende spørgeskemaer til foretagender, hvis selvcertificeringer er udløbet, eller som frivilligt har trukket sig ud af EU's og USA's værn om privatlivets fred, for at kontrollere, om foretagendet agter at tilbagesende eller slette personoplysningerne eller fortsat vil anvende principperne om beskyttelse af privatlivets fred på de personoplysninger, som de modtog, mens de deltog i værnet om privatlivets fred, og hvis de beholder personoplysningerne, kontrollere, hvem der fremover fungerer som kontaktpunkt for spørgsmål relateret til værnet om privatlivets fred.
- (37) Handelsministeriet vil løbende foretage ex officio-kontrol ⁽³⁸⁾ af selvcertificerede foretagenders overholdelse, herunder gennem fremsendelse af detaljerede spørgeskemaer. Ministeriet vil ligeledes systematisk foretage kontrol, hver gang det modtager en specifik (begrundet) klage, hvis et foretagende ikke svarer tilfredsstillende på dets forespørgsler, eller hvis der er troværdig dokumentation for, at et foretagende muligvis ikke overholder principperne. Når det er relevant, vil handelsministeriet desuden konsultere databeskyttelsesmyndighederne i forbindelse med sådanne kontroller.

2.3. Klageadgang og -håndtering samt fuldbyrdelse

- (38) I henhold til *princippet om klageadgang, håndhævelse og ansvar* inden for rammerne af EU's og USA's værn om privatlivets fred skal foretagender give fysiske personer, der er genstand for manglende overholdelse, mulighed for regres, dvs. give registrerede i EU mulighed for at indgive klager vedrørende selvcertificerede amerikanske foretagenders manglende overholdelse og om nødvendigt få disse klager afgjort ved en afgørelse om effektive afhjælpende foranstaltninger.
- (39) Som led i deres selvcertificering skal foretagender opfylde kravene i princippet om klageadgang, håndhævelse og ansvar 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.
- (40) Foretagender kan vælge at benytte uafhængige klageinstanser i enten EU eller i USA. Det omfatter også muligheden for frivilligt at forpligte sig til at samarbejde med databeskyttelsesmyndighederne i EU. Denne valgmulighed findes dog ikke, når foretagenderne behandler oplysninger om menneskelige ressourcer, da det

⁽³⁶⁾ Se afsnittet om »Søgning efter og håndtering af falske påstande om deltagelse i værnet« i bilag I.

⁽³⁷⁾ Se bilag II, afsnit III, punkt 6.h og afsnit III, punkt 11.f.

⁽³⁸⁾ Se bilag I.

i dette tilfælde er 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 inkorporerer principperne. Sidstnævnte skal omfatte effektive fuldbyrdelsesmekanismer i overensstemmelse med kravene i princippet om klageadgang, håndhævelse og ansvar. Foretagender har pligt til at løse eventuelle problemer vedrørende manglende overensstemmelse. De skal ligeledes præcisere, at de er underlagt de undersøgelses- og håndhævelsesbeføjelser, der er tillagt FTC, transportministeriet eller ethvert andet godkendt kompetent organ.

- (41) Ordningen for værnet om privatlivets fred giver således de registrerede en række muligheder for at udøve deres rettigheder, indgive klager vedrørende selvcertificerede amerikanske foretagenders manglende overholdelse og om nødvendigt at få klagerne afgjort gennem en afgørelse med effektive afhjælpende foranstaltninger. Fysiske personer kan indbringe en klage direkte til et foretagende, til en uafhængig tvistbilæggesinstans, der er udpeget af foretagendet, til de nationale databeskyttelsesmyndigheder eller til FTC.
- (42) Hvis deres klager ikke afgøres ved hjælp af disse klage- eller håndhævelsesmekanismer, kan fysiske personer indbringe sagen til tvungen voldgift for panelet i værnet om privatlivets fred (bilag 1 til bilag II 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. Det anbefales dog at følge den logiske rækkefølge, der er beskrevet nedenfor.
- (43) For det første kan registrerede i EU rette klager vedrørende manglende overholdelse af principperne direkte til det *selvcertificerede amerikanske foretagende*. Foretagendet skal indføre en effektiv klagemekanisme til behandling af disse klager for at fremme en løsning. Et foretagendes privatlivspolitik skal derfor indeholde klare oplysninger til fysiske personer om det kontaktpunkt i eller uden for foretagendet, der behandler klagerne (herunder ethvert relevant organ i EU, som kan besvare forespørgsler eller klager), og oplysninger om de uafhængige klageinstanser.
- (44) Ved modtagelsen af en klage fra en fysisk person, enten direkte fra personen eller via handelsministeriet, som har fået sagen henvist fra en databeskyttelsesmyndighed, skal foretagendet fremsende et svar til den registrerede i EU inden for 45 dage. Dette svar skal indeholde en vurdering af klagens berettigelse og oplysninger om, hvordan foretagendet vil løse problemet. Foretagenderne skal ligeledes straks besvare henvendelser og andre anmodninger om oplysninger fra handelsministeriet eller en databeskyttelsesmyndighed ⁽³⁹⁾ (hvis foretagendet har forpligtet sig til at samarbejde med databeskyttelsesmyndighederne) vedrørende deres tilslutning til principperne. Foretagenderne skal føre protokol over implementeringen af deres privatlivspolitik og på anmodning herom stille dem til rådighed for en uafhængig klageinstans eller FTC (eller den amerikanske myndighed, der har kompetence til at undersøge sager om illoyal eller vildledende praksis) i forbindelse med en undersøgelse eller en klage vedrørende manglende overholdelse.
- (45) For det andet kan fysiske personer ligeledes indgive klagen direkte til den *uafhængige tvistbilæggesinstans* (enten i USA eller i EU), der er udpeget af et foretagende til at undersøge og afgøre individuelle klager (medmindre klagerne tydeligt er ubegrundede eller useriøse) og sikre egnet gratis klageadgang for fysiske personer. De sanktioner og afhjælpende foranstaltninger, der pålægges af denne instans, skal være af en sådan karakter, at foretagenderne tilskyndes til at overholde principperne, og de bør sikre, at foretagendet 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. De uafhængige tvistbilæggesinstanser, der udpeges af et foretagende, skal angive relevante oplysninger om EU's og USA's værn om privatlivets fred og om de tjenester, de tilvejebringer i tilknytning hertil, på deres offentlige websteder. De skal hvert år offentliggøre en årlig rapport med en samlet statistik over disse tjenester ⁽⁴⁰⁾.

⁽³⁹⁾ Den myndighed, der er blevet udpeget af panelet af databeskyttelsesmyndigheder, til at behandle sagerne i overensstemmelse med det supplerende princip om »Databeskyttelsesmyndighedernes rolle« (bilag II, afsnit III, punkt 5).

⁽⁴⁰⁾ Den årlige rapport skal indeholde oplysninger om: 1) det samlede antal klager relateret til værnet om privatlivets fred 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.

- (46) Handelsministeriet vil som led i sin kontrol af overholdelsen ligeledes kontrollere, om selvcertificerede amerikanske foretagender rent faktisk har ladet sig registrere ved den uafhængige klageinstans, som de påstår at have registreret sig ved. Både foretagenderne og den ansvarlige uafhængige klageinstans skal straks besvare forespørgsler og anmodninger fra handelsministeriet om oplysninger vedrørende værnet om privatlivets fred.
- (47) I de tilfælde hvor foretagendet 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 sager om illoyal eller vildledende praksis) eller til en kompetent domstol ⁽⁴¹⁾. Hvis et foretagende nægter at følge et selvregulerende organs, et uafhængigt tvistbilægelsesorgans eller et statsligt organs endelige afgørelse, eller hvis et sådant organ fastslår, at et foretagende regelmæssigt overtræder principperne, vil dette blive betragtet som en vedvarende overtrædelse med det resultat, at handelsministeriet, efter at have givet det pågældende foretagende 30 dages varsel og mulighed for at fremsætte bemærkninger, fjerner foretagendet fra listen over deltagere i værnet om privatlivets fred ⁽⁴²⁾. Hvis foretagendet efter at være blevet fjernet fra listen fastholder påstande om deltagelse i værnet om privatlivets fred, henviser ministeriet det til FTC eller en anden retshåndhævende myndighed ⁽⁴³⁾.
- (48) For det tredje kan en fysisk person også indgive en klage til en national *databeskyttelsesmyndighed*. Foretagender 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 det pågældende foretagende frivilligt har underlagt sig databeskyttelsesmyndighedernes tilsyn. Foretagenderne 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.
- (49) Databeskyttelsesmyndighedernes anbefalinger vil blive formidlet gennem et uformelt panel af databeskyttelsesmyndigheder etableret på EU-niveau ⁽⁴⁴⁾, som vil bidrage til at sikre en ensartet og sammenhængende tilgang til en given klage. Anbefalingerne vil blive afgivet, når begge parter i sagen har haft passende mulighed for at fremsætte bemærkninger og fremlægge eventuel dokumentation, som de finder relevant. Panelet vil afgive sine anbefalinger så hurtigt som muligt under hensyntagen til kravet om behørig behandling og som hovedregel senest 60 dage efter modtagelse af klagen. Hvis et foretagende ikke har rettet sig efter en anbefaling senest 25 dage efter anbefalingens afgivelse og ikke har givet en tilfredsstillende forklaring på denne forsinkelse, vil panelet meddele, at det agter at indbringe sagen for FTC (eller et andet kompetent amerikansk retshåndhævende organ) eller 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). I det andet tilfælde vil panelet underrette handelsministeriet, der vil betragte foretagendets afslag om at efterkomme panelets anbefalinger som en vedvarende overtrædelse, der indebærer, at foretagendet fjernes fra listen over deltagere i værnet om privatlivets fred.
- (50) Hvis den databeskyttelsesmyndighed, som har modtaget klagen, ikke har truffet eller har truffet utilstrækkelige foranstaltninger vedrørende en klage, har den enkelte klager mulighed for at indbringe sagen for de nationale domstole i den pågældende medlemsstat.
- (51) Fysiske personer kan også indgive klager til databeskyttelsesmyndighederne, selv om foretagendet ikke har udpeget panelet som tvistbilægelsesinstans. I disse tilfælde kan databeskyttelsesmyndigheden henvise klagen til enten handelsministeriet eller til FTC. For at fremme og styrke samarbejdet om spørgsmål relateret til individuelle klager og manglende overholdelse fra foretagender i værnet om privatlivets fred vil handelsministeriet udpege et særligt kontaktpunkt, der skal agere bindeled og hjælpe med at besvare forespørgsler om et foretagendes overholdelse af principperne ⁽⁴⁵⁾. FTC har ligeledes forpligtet sig til at udpege et særligt kontaktpunkt ⁽⁴⁶⁾ og yde databeskyttelsesmyndighederne efterforskningsbistand i henhold til USA's SAFE WEB Act ⁽⁴⁷⁾.

⁽⁴¹⁾ Jf. bilag II, afsnit III, punkt 11.e.

⁽⁴²⁾ Jf. bilag II, afsnit III, punkt 11.g og særligt punkt ii. og iii.

⁽⁴³⁾ Se afsnittet om »Søgning efter og håndtering af falske påstande om deltagelse i værnet« i bilag I.

⁽⁴⁴⁾ Databeskyttelsesmyndighederne bør fastlægge forretningsordenen for det uformelle panel på grundlag af deres kompetence til at tilrettelægge deres arbejde og samarbejde med hinanden.

⁽⁴⁵⁾ Se afsnittene om »Øget samarbejde med databeskyttelsesmyndighederne« og »Fremme af afgørelser af klager om manglende overholdelse« i bilag I samt bilag II, afsnit II, punkt 7.e.

⁽⁴⁶⁾ Jf. bilag IV, s. 6.

⁽⁴⁷⁾ *ibid.*

- (52) For det fjerde har handelsministeriet forpligtet sig til at modtage, gennemgå og gøre sit yderste for at behandle klager om et foretagendes manglende overholdelse af principperne. Handelsministeriet har i den forbindelse indført særlige procedurer, som databeskyttelsesmyndighederne skal følge ved henvisning af klager til et specifikt kontaktpunkt, sporing af klagerne og opfølgning over for foretagenderne for at fremme en løsning. For at fremskynde behandlingen af individuelle klager vil kontaktpunktet tage direkte kontakt til den pågældende databeskyttelsesmyndighed i tilfælde af problemer med overholdelsen og navnlig underrette myndigheden om status for klagerne senest 90 dage efter henvisningen. Dette giver registrerede mulighed for at indgive klager over amerikanske selvcertificerede foretagender, der ikke overholder principperne, direkte til deres nationale databeskyttelsesmyndighed og få dem kanaliseret til handelsministeriet, der er den amerikanske myndighed, som forvalter EU's og USA's værn om privatlivets fred. Handelsministeriet har ligeledes forpligtet sig til at forelægge en rapport, hvor de klager, ministeriet modtager hvert år, analyseres i aggregeret form, i forbindelse med den årlige evaluering af EU's og USA's værn om privatlivets fred ⁽⁴⁸⁾.
- (53) Hvis handelsministeriet på grundlag af sin ex officio-kontrol, klager eller andre oplysninger konkluderer, at et foretagende vedvarende overtræder principperne, vil ministeriet fjerne det fra listen over deltagere i værnet om privatlivets fred. Hvis et foretagende nægter at rette sig efter den endelige afgørelse truffet af en uafhængig selvregulerende tvistbilægelsesinstans 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.
- (54) For det femte skal et foretagende i værnet om privatlivets fred være underlagt de undersøgelses- og håndhævelsesbeføjelser, der er tillagt de amerikanske myndigheder, særligt *Federal Trade Commission* ⁽⁴⁹⁾, som vil garantere overholdelsen af principperne. FTC vil prioritere sager om manglende overholdelse af principperne om privatlivets fred, der henvises fra uafhængige tvistbilægelsesinstanser eller selvregulerende instanser, handelsministeriet og databeskyttelsesmyndighederne (der handler på eget initiativ eller på grundlag af klager) for at bestemme, om Section 5 i *Federal Trade Commission Act* er blevet overtrådt ⁽⁵⁰⁾. 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. FTC vil derudover tage imod klager direkte fra fysiske personer og på eget initiativ foretage undersøgelser relateret til værnet om privatlivets fred, navnlig som led i sine mere generelle undersøgelser af forhold vedrørende beskyttelse af privatlivets fred.
- (55) FTC kan håndhæve overholdelsen gennem administrative afgørelser («consent orders» — forligsafgørelser) og vil systematisk overvåge overholdelsen af disse afgørelser. Hvis et foretagende ikke efterlever afgørelsen, kan FTC henvise sagen til den kompetente domstol med henblik på idømmelse af civilretlige sanktioner eller andre afhjælpende foranstaltninger, herunder for enhver skade som følge af den ulovlige adfærd. FTC kan alternativt anmode en føderal domstol om at udstede et foreløbigt eller endeligt forbud eller påbud eller andre afhjælpende foranstaltninger. Enhver forligsafgørelse, der udstedes til et foretagende i værnet om privatlivets fred, vil indeholde bestemmelser om selvrapportering ⁽⁵¹⁾, og foretagenderne vil blive anmodet om at offentliggøre alle afsnit relateret til værnet om privatlivets fred i alle overholdelses- eller vurderingsrapporter forelagt FTC. Endelig vil FTC føre en onlineliste over foretagender omfattet FTC- eller retsafgørelser i sager om værnet om privatlivets fred.
- (56) 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 værnet om privatlivets fred« med henblik på tvungen voldgift. Foretagender skal informere de registrerede om muligheden for, på visse betingelser, at indbringe sagen til tvungen voldgift, og de er forpligtede til at reagere, når en registreret benytter sig af denne mulighed ved at rette henvendelse til det berørte foretagende ⁽⁵²⁾.

⁽⁴⁸⁾ Jf. afsnittet om »Fremme af afgørelser af klager om manglende overholdelse« i bilag I.

⁽⁴⁹⁾ Et foretagende i værnet om privatlivets fred skal offentligt erklære sin tilslutning til principperne, offentliggøre sin privatlivspolitik 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.

⁽⁵⁰⁾ FTC er ifølge egne oplysninger ikke bemyndiget til at foretage kontrol på stedet inden for beskyttelse af privatlivets fred. Det har dog kompetence til at tvinge foretagender til at fremsende dokumenter og vidneudsagn (jf. Section 20 i FTC Act) og kan benytte sig af retssystemet til at få håndhævet dette i tilfælde af manglende overholdelse.

⁽⁵¹⁾ Foretagender 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.

⁽⁵²⁾ Jf. bilag II, afsnit II, punkt 1.xi og afsnit III, punkt 7.c.

- (57) Voldgiftspanelet vil bestå af en pulje af mindst 20 voldgiftsmænd udpeget af det amerikanske handelsministerium og Kommissionen på grundlag af disses 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 voldgiftsmænd fra denne pulje ⁽⁵³⁾. Voldgiftsproceduren vil være underlagt almindelige voldgiftsregler, der skal fastlægges af handelsministeriet og Kommissionen. Disse regler vil supplere de allerede eksisterende regler, der indeholder flere elementer til at give registrerede i EU større mulighed for at anvende denne mekanisme, bl.a. i) kan den registrerede få hjælp af sin nationale databeskyttelsesmyndighed til at fremsætte en klage for panelet, ii) den registrerede i EU har mulighed for at deltage i voldgiftsbehandlingen, som foregår i USA, via video- eller telekonference uden ekstra omkostninger for den registrerede, iii) voldgiftsproceduren vil 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 ⁽⁵⁴⁾ 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 foretagenderne i værnet om privatlivets fred, som skal dække støtteberettigede voldgiftsomkostninger op til maksimumsbeløb, der skal fastlægges af de amerikanske myndigheder i samråd med Kommissionen.
- (58) Panelet i værnet om privatlivets fred har beføjelse til at give rimelig individuel ikkepengemæssig oprejsning ⁽⁵⁵⁾ («individual-specific, non-monetary equitable relief») for at afhjælpe overtrædelsen af principperne. Selv om panelet vil tage højde for andre afhjælpende foranstaltninger, der allerede er iværksat gennem andre mekanismer i værnet om privatlivets fred, 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 vil give registrerede i EU mulighed for at kræve sagen afgjort ved voldgift, hver gang de kompetente amerikanske myndigheders (f.eks. FTC) tiltag eller mangel på tiltag 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 det selvcertificerede amerikanske foretagende, nemlig i de sager, hvor foretagendet 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 et foretagende ikke overholder principperne.
- (59) For det syvende kan der i tilfælde af et foretagendes manglende overholdelse af principperne og af dens privatlivspolitik findes andre muligheder for retslig prøvelse i de enkelte amerikanske staters lovgivning, som indeholder bestemmelser om retsmidler under erstatningsretten og i tilfælde af svigagtig afgivelse af urigtige oplysninger, illoyal eller vildledende praksis eller kontraktbrud.
- (60) Hvis en databeskyttelsesmyndighed modtager en klage fra en registreret i EU og finder, at overførslen af en persons personoplysninger til et foretagende i USA sker i strid med EU's regler om databeskyttelse, herunder også når dataeksportøren i EU har grund til at tro, at foretagendet ikke overholder principperne, kan den også udøve sine beføjelser i forhold til dataeksportøren og om nødvendigt beordre suspension af dataoverførslen.
- (61) På grundlag af oplysningerne i dette afsnit finder Kommissionen, at de principper, som det amerikanske handelsministerium har opstillet, i deres helhed sikrer et niveau af beskyttelse af personoplysninger, der i det væsentlige svarer til det niveau, der er garanteret ved de grundlæggende principper i direktiv 95/46/EF.
- (62) Den effektive anvendelse af principperne er desuden garanteret ved gennemsigtighedskrav og handelsministeriets forvaltning og kontrol af værnet om privatlivets fred.
- (63) Kommissionen mener desuden, at mekanismerne for tilsyn og klageadgang i værnet om privatlivets fred gør det muligt at identificere overtrædelser af principperne begået af foretagender i værnet om privatlivets fred og straffe disse i praksis og sikre registrerede retsmidler med henblik på at få adgang til personoplysninger, som vedrører de pågældende, eller til at få sådanne oplysninger berigtiget eller slettet.

⁽⁵³⁾ Parterne skal aftale antallet af voldgiftsmænd i panelet.

⁽⁵⁴⁾ Panelet kan imidlertid beslutte, at en dækning af omkostningerne i den specifikke voldgiftssag ville føre til uberettigede eller uforholdsmæssige omkostninger.

⁽⁵⁵⁾ 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.

3. DE AMERIKANSKE MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER OVERFØRT UNDER EU'S OG USA'S VÆRN OM PRIVATLIVETS FRED

- (64) Som anført i bilag II, afsnit I, punkt 5, er overholdelsen af principperne begrænset til et niveau, der er tilstrækkeligt til at opfylde kravene med hensyn til den nationale sikkerhed, den offentlige interesse eller retshåndhævelse.
- (65) Kommissionen har vurderet begrænsningerne og garantierne i amerikansk ret for de amerikanske myndigheds adgang til og brug af personoplysninger overført under EU's og USA's værn om privatlivets fred med henblik på beskyttelsen af den nationale sikkerhed, retshåndhævelse og andre offentlige interesser. Den amerikanske regering har desuden gennem Office of the Director of National Intelligence (ODNI) ⁽⁵⁶⁾ forelagt detaljerede udredninger og tilsagn for Kommissionen, som findes i bilag VI til denne afgørelse. Ved brev fra den amerikanske udenrigsminister knyttet som bilag III til denne afgørelse har den amerikanske regering ligeledes forpligtet sig til at indføre en ny tilsynsmekanisme for nationale sikkerhedsforanstaltninger, nemlig ombudsmanden i værnet om privatlivets fred, der er uafhængig af de amerikanske efterretningstjenester. Endelig beskrives i bilag VII til denne afgørelse de gældende begrænsninger og garantier for de offentlige myndigheds adgang til og brug af oplysninger med henblik på retshåndhævelse og andre offentlige interesser i en udredning fra det amerikanske justitsministerium. For at øge gennemsigtigheden og afspejle den retlige karakter af disse forpligtelser vil de enkelte dokumenter, der er anført i og knyttet til denne afgørelse, blive offentliggjort i USA's Federal Register.
- (66) Nedenfor redegøres der nærmere for Kommissionens konklusioner om begrænsningerne for de amerikanske offentlige myndigheds adgang til og brug af personoplysninger overført fra EU til USA og om adgangen til en effektiv domstolsbeskyttelse.

3.1. De amerikanske myndigheds adgang til og brug af personoplysninger til nationale sikkerhedsformål

- (67) Kommissionens analyse viser, at amerikansk ret indeholder en række klare begrænsninger for adgangen til og brugen af personoplysninger, der er overført under EU's og USA's værn om privatlivets fred til nationale sikkerhedsformål, samt tilsyns- og klagemekanismer, der giver tilstrækkelige garantier for, at disse oplysninger beskyttes effektivt mod risikoen for ulovlig adgang og risikoen for misbrug ⁽⁵⁷⁾. Siden 2013, hvor Kommissionen offentliggjorde sine to meddelelser (jf. betragtning 7), er dette retsgrundlag blevet betydeligt styrket som anført nedenfor.

3.1.1. Begrænsninger

- (68) I henhold til den amerikanske forfatning skal præsidenten som øverstbefalende og regeringsleder beskytte den nationale sikkerhed og, hvad angår udenlandsk efterretningsvirksomhed, føre den amerikanske udenrigspolitik ⁽⁵⁸⁾. Selv om den amerikanske kongres har beføjelse til at pålægge begrænsninger og har gjort dette i mange henseender, kan præsidenten inden for disse grænser styre de amerikanske efterretningstjenesters aktiviteter, navnlig gennem præsidentielle dekretter (executive orders) eller præsidentielle direktiver (presidential directives). Det gælder naturligvis også på de områder, hvor der ikke er nogen retningslinjer fra kongressen. De to centrale retlige instrumenter på dette område i øjeblikket er et præsidentielt dekret, Executive Order 12333 (»E.O. 12333«) ⁽⁵⁹⁾, og et præsidentielt direktiv, Presidential Policy Directive 28.

⁽⁵⁶⁾ Director of National Intelligence (DNI) står i spidsen for de amerikanske efterretningstjenester og er hovedrådgiver for præsidenten og USA's nationale sikkerhedsråd — National Security Council. Se Intelligence Reform and Terrorism Prevention Act fra 2004, Pub. L. 108-458 af 17.12.2004. ODNI fastsætter bl.a. kravene til og forvalter og styrer de amerikanske efterretningstjenesters opgaver, indsamling, analyse, produktion og formidling af nationale efterretninger, herunder gennem opstilling af retningslinjer for adgang til og brug og udveksling af oplysninger eller efterretninger. Se Sec. 1.3 (a), (b) i E.O. 12333.

⁽⁵⁷⁾ Jf. Schrems-dommen, præmis 91.

⁽⁵⁸⁾ Artikel II i den amerikanske forfatning. Se også indledningen til PPD-28.

⁽⁵⁹⁾ E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8.12.1981). For så vidt som det præsidentielle dekret er offentligt tilgængeligt, definerer det efterretningsindsatsens formål, retning, opgaver og ansvarsområder (herunder de forskellige efterretningsenheders rolle) og fastlægger de generelle parametre for udøvelsen af efterretningsaktiviteter (navnlig nødvendigheden af at fastlægge specifikke procedureregler). I henhold til Sec. 3.2 i E.O. 12333 udsteder præsidenten, med støtte fra National Security Council, og DNI de nødvendige direktiver, procedurer og retningslinjer til gennemførelse af dekretet.

(69) I Presidential Policy Directive 28 (»PPD-28«), udstedt den 17. januar 2014, pålægges en række begrænsninger for »signalefterretningsaktiviteter«⁽⁶⁰⁾. Dette præsidentielle direktiv er bindende for de amerikanske efterretningsmyndigheder⁽⁶¹⁾ og vil fortsat være i kraft efter et regeringsskifte i USA⁽⁶²⁾. PPD-28 er særlig relevant for ikke-amerikanske personer, herunder registrerede i EU. Bl.a. fastslås følgende:

- a) indsamlingen af signalefterretninger skal være hjemlet i lov eller præsidentiel bemyndigelse og skal foretages i overensstemmelse med den amerikanske forfatning (navnlig det fjerde amendment) og amerikansk ret
- b) alle mennesker bør behandles med værdighed og respekt, uanset deres nationalitet eller bopæl
- c) alle mennesker har legitime interesser i beskyttelsen af privatlivets fred ved behandlingen af deres personoplysninger
- d) hensynet til privatlivets fred og borgerlige rettigheder skal integreres i planlægningen af amerikanske signalefterretningsaktiviteter
- e) amerikanske signalefterretningsaktiviteter skal derfor omfatte tilstrækkelige garantier for alle personers personoplysninger uanset deres nationalitet eller bopæl.

(70) Ifølge PPD-28 må signalefterretninger kun indsamles til udenlandske efterretnings- eller kontraspionageformål, der understøtter nationale eller ministerielle opgaver, og de må ikke indsamles til noget andet formål (f.eks. for at give amerikanske virksomheder en konkurrencefordel). ODNI forklarer i den forbindelse, at efterretningsenhederne »skal stille krav om, at indsamlingen så vidt muligt rettes mod specifikke udenlandske efterretningsmål eller -emner ved brug af diskriminanter (f.eks. specifikke faciliteter, selektorer og identifikatorer)«⁽⁶³⁾. I udredningerne gives der endvidere sikkerhed for, at afgørelser om indsamling af efterretninger ikke overlades til de enkelte efterretningsfolk, men er underlagt de politikker og procedurer, som de forskellige amerikanske efterretningsenheder (agenturer) skal indføre som led i gennemførelsen af PPD-28⁽⁶⁴⁾. Søgningen efter og fastlæggelsen af passende selektorer sker derfor inden for rammerne af den overordnede »National Intelligence Priorities Framework« (NIPF), som sikrer, at efterretningsprioriteterne fastlægges af politiske beslutningstagere på højt niveau, og at de gennemgås regelmæssigt, således at de tilpasses de reelle nationale sikkerhedstrusler og mulige risici, herunder risiciene for krænkelse af privatlivets fred⁽⁶⁵⁾. På denne baggrund søger agenturerne efter og identificerer specifikke selektorer, som forventes at resultere i indsamlingen af udenlandske efterretninger i overensstemmelse med prioriteterne⁽⁶⁶⁾. Selektorerne skal gennemgås jævnlige for at undersøge, om de stadig tilvejebringer værdifulde efterretninger, som er i overensstemmelse med prioriteterne⁽⁶⁷⁾.

⁽⁶⁰⁾ I henhold til E.O. 12333 er direktøren for National Security Agency ((NSA) — Director of the National Security Agency — den funktionelle leder af signalefterretning og styrer en fælles organisation for signalefterretningsaktiviteter.

⁽⁶¹⁾ For en definition af de amerikanske efterretningstjenester (»Intelligence Community«) se Sec. 3.5 (h) i E.O. 12333 sammenholdt med n. 1 i PPD-28.

⁽⁶²⁾ Se memorandum fra det amerikanske justitsministeriums rådgivende kontor — Office of Legal Counsel — til præsident Clinton, 29.1.2000. Ifølge denne juridiske udtalelse har præsidentielle direktiver »samme materielle retsvirkning som et præsidentielt dekret«.

⁽⁶³⁾ ODNI's udredninger (bilag VI), s. 3.

⁽⁶⁴⁾ Jf. Sec. 4(b),(c) i PPD-28. Ifølge offentligt tilgængelige oplysninger blev de seks formål bekræftet ved gennemgangen i 2015. Se ODNI, Signals Intelligence Reform, 2016 Progress Report.

⁽⁶⁵⁾ ODNI's udredninger (bilag VI), s. 6 (med henvisning til Intelligence Community Directive 204). Se også Sec. 3 i PPD-28.

⁽⁶⁶⁾ ODNI's udredninger (bilag VI), s. 6. Se f.eks. NSA's Civil Liberties and Privacy Office (NSA CLPO), NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities i henhold til Executive Order 12333, 7.10.2014. Se også ODNI Status Report 2014. Med hensyn til anmodninger om indsigt under Sec. 702 i FISA er søgninger omfattet af FISC-godkendte minimeringsprocedurer. Se NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014.

⁽⁶⁷⁾ Se Signals Intelligence Reform, 2015 Anniversary Report. Se også ODNI's udredninger (bilag VI), s. 6, 8-9 og 11.

- (71) Kravene i PPD-28 om, at indsamlingen altid ⁽⁶⁸⁾ skal være »så målrettet som muligt«, og at de amerikanske efterretningstjenester skal prioritere andre tilgængelige oplysninger og hensigtsmæssige og mulige alternativer ⁽⁶⁹⁾ er desuden udtryk for en generel regel om at prioritere målrettet indsamling frem for masseindsamling. Ifølge ODNI's udredninger sikrer den navnlig, at masseindsamlingen hverken er »omfattende« eller »vilkårlig«, og at undtagelsen ikke bliver reglen ⁽⁷⁰⁾.
- (72) Selv om det anføres i PPD-28, at efterretningsenhederne i visse situationer kan være nødsaget til at foretage masseindsamling af signalefterretninger, f.eks. for at identificere og evaluere nye trusler eller trusler under udvikling, pålægges enhederne at prioritere alternativer, der gør det muligt at målrette indsamlingen af signalefterretninger ⁽⁷¹⁾. Heraf følger, at der alene foretages masseindsamling, når målrettet indsamling ved anvendelse af diskriminanter — dvs. en identifikator, der er knyttet til et bestemt mål (f.eks. målets e-mailadresse eller telefonnummer) — ikke er mulig »på grund af tekniske eller praktiske forhold« ⁽⁷²⁾. Det gælder både den måde, hvorpå signalefterretningerne indsamles, og det der rent faktisk indsamles ⁽⁷³⁾.
- (73) Selv når efterretningstjenesterne ikke kan bruge specifikke identifikatorer til at målrette indsamlingen søger ODNI ifølge dens udredninger at indsnævre indsamlingen »så vidt muligt«. Med henblik herpå bruger den »filtre og andre tekniske redskaber til at målrette indsamlingen de faciliteter, der kan formodes at indeholde kommunikation af relevans for udenlandske efterretningsaktiviteter« (og dermed opfylder de amerikanske beslutningstageres krav i henhold til den procedure, der er beskrevet i betragtning 70). Masseindsamling gøres således målrettet på to måder: For det første vil den altid vedrøre specifikke mål for den udenlandske efterretningsvirksomhed (f.eks. at indhente signalefterretninger om en terrorgruppes aktiviteter i en bestemt region) og være rettet mod indsamling af kommunikation i relation hertil. Ifølge ODNI's udredninger kommer dette til udtryk ved, at »amerikanske signalefterretningsaktiviteter kun vedrører en meget lille del af kommunikationen på internettet« ⁽⁷³⁾. For det andet fremgår det af ODNI's udredninger, at filtrene og de øvrige tekniske redskaber vil være udformet således, at indsamlingen bliver »så målrettet som muligt« for at sikre, at andelen af »ikke-relevante oplysninger« blive så lille som muligt.
- (74) Selv når USA vurderer, at det er nødvendigt at foretage masseindsamling af signalefterretninger på de betingelser, der er anført i betragtning 70-73, begrænser PPD-28 anvendelsen af disse oplysninger til en specifik liste med seks nationale sikkerhedsformål for at beskytte alle personers privatliv og borgerlige rettigheder uanset nationalitet og bopæl ⁽⁷⁴⁾. De tilladte formål omfatter foranstaltninger til sporing og imødegåelse af trusler fra spionage, terrorisme og masseødelæggelsesvåben mod de væbnede styrker, trusler mod cybersikkerheden eller

⁽⁶⁸⁾ Se fodnote 63.

⁽⁶⁹⁾ Det bør ligeledes bemærkes, at de forskellige efterretningsenheder i henhold til Sec. 2.4 i E.O. 12333 »anvender de mindst indgribende indsamlingsteknikker i USA«. Hvad angår begrænsningerne med hensyn til at erstatte masseindsamling med målrettet indsamling henvises til resultaterne af National Research Council's undersøgelse som anført af Den Europæiske Unions Agentur for Grundlæggende Rettigheder i rapporten Surveillance by intelligence services: Fundamental Rights Safeguards and Remedies in the EU (2015), s. 18.

⁽⁷⁰⁾ ODNI's udredninger (bilag VI), s. 4.

⁽⁷¹⁾ Se også Sec. 5(d) i PPD-28, hvor det fastslås, at direktøren for National Intelligence (Director of National Intelligence) i samarbejde med lederne af de relevante efterretningsenheder og Office of Science and Technology Policy skal forelægge »en rapport med en vurdering af muligheden for at udvikle software, som gør det nemmere for de amerikanske efterretningstjenester at foretage målrettet indsamling af oplysninger i stedet for masseindsamling«. Ifølge offentligt tilgængelige oplysninger konkluderede rapporten, at »der ikke findes noget softwarebaseret alternativ, der fuldt ud erstatter masseindsamling ved sporingen af en række nationale sikkerhedstrusler«. Se Signals Intelligence Reform, 2015 Anniversary Report.

⁽⁷²⁾ Se fodnote 63.

⁽⁷³⁾ ODNI's udredninger (bilag VI). Dette er især en løsning på de betænkeligheder, som de nationale databeskyttelsesmyndigheder gav udtryk for i deres udtalelse til udkastet til afgørelsen om et tilstrækkeligt beskyttelsesniveau. Se Artikel 29 — Gruppen vedrørende Databeskyttelse, udtalelse 01/2016 om udkastet til afgørelse om tilstrækkeligheden af EU's og USA's værn om privatlivets fred (vedtaget den 13.4.2016), s. 38 sammenholdt med n. 47.

⁽⁷⁴⁾ Jf. Sec. 2 i PPD-28.

militærpersonel samt transnationale kriminelle trusler relateret til de fem andre formål, og de vil blive gennemgået mindst en gang årligt. Ifølge udredningerne fra den amerikanske regering har efterretningstjenesterne styrket deres analysepraksis og standarder for søgning efter ikkeevaluerede signalefterretninger for at opfylde disse krav. Anvendelsen af målrettede søgninger »sikrer, at analytikerne kun får forelagt de oplysninger, der formodes at have en potentiel efterretningsværdi, til analyse«⁽⁷⁵⁾.

- (75) Disse begrænsninger er særlig relevante for personoplysninger overført under EU's og USA's værn om privatlivets fred, navnlig hvis indsamlingen af personoplysninger skal finde sted uden for USA, herunder under transit på de transatlantiske kabler fra EU til USA. Som de amerikanske myndigheder har bekræftet i ODNI's udredninger, finder de heri anførte begrænsninger og garantier — herunder i PPD-28 — anvendelse på denne indsamling⁽⁷⁶⁾.
- (76) Selv om disse principper ikke er formuleret ved brug af disse juridiske begreber, afspejler de det væsentligste indhold af principperne om nødvendighed og proportionalitet. Måltrettet indsamling er klart prioriteret, hvorimod masseindsamling er begrænset til (særlige) situationer, hvor måltrettet indsamling ikke er mulig af tekniske eller operationelle årsager. Selv når *masseindsamling* ikke kan undgås, er videre »anvendelse« af disse oplysninger gennem adgang *strengt begrænset* til specifikke legitime nationale sikkerhedsformål⁽⁷⁷⁾.
- (77) Da direktivet er udstedt af præsidenten som regeringsleder, er disse krav bindende for alle amerikanske efterretningstjenester, og de er blevet udbygget i agenturernes regler og procedurer, der omsætter de generelle principper til specifikke retningslinjer for daglige aktiviteter. Selv om den amerikanske kongres ikke er bundet af PPD-28, har den ligeledes truffet foranstaltninger til at sikre, at indsamling af og adgang til personoplysninger i USA er måltrettet og ikke foretages »på generaliseret vis«.
- (78) Ifølge de foreliggende oplysninger, herunder udredningerne fra den amerikanske regering, må amerikanske efterretningsagenturer, når oplysningerne er blevet overført til selvcertificerede foretagender i USA under EU's og USA's værn om privatlivets fred, kun søge personoplysninger⁽⁷⁸⁾, hvis deres anmodning er i overensstemmelse med Foreign Intelligence Surveillance Act (FISA), eller hvis anmodningen foretages af Federal Bureau of Investigation (FBI) på grundlag af et såkaldt »National Security Letter« (NSL) (nationalt sikkerhedsbrev)⁽⁷⁹⁾. Der er en række retsgrundlag i FISA, som kan anvendes til at indsamle (og efterfølgende behandle) personoplysninger for

⁽⁷⁵⁾ ODNI's udredninger (bilag VI), s. 4. Se også Intelligence Community Directive 203.

⁽⁷⁶⁾ ODNI's udredninger (bilag VI), s. 2. De anførte begrænsninger i E.O. 12333 (f.eks. kravet om, at indsamlede oplysninger skal være i overensstemmelse med de prioriteringer, som præsidenten har fastlagt) finder ligeledes anvendelse.

⁽⁷⁷⁾ Jf. Schrems-dommen, præmis 93.

⁽⁷⁸⁾ FBI's indsamling af oplysninger kan desuden ligeledes være baseret på retshåndhævelsestilladelser (se punkt 3.2 i denne afgørelse).

⁽⁷⁹⁾ Der redegøres nærmere for anvendelsen af NSL i ODNI's udredninger (bilag VI), s. 13-14, sammenholdt med n. 38. Som anført heri kan FBI kun anvende NSL'er til at anmode om ikke-indholdsmæssige oplysninger af relevans for en godkendt national sikkerhedsundersøgelse med henblik på beskyttelse mod international terrorisme eller hemmelige efterretningsaktiviteter. Med hensyn til dataoverførsler under EU's og USA's værn om privatlivets fred er den mest relevante lovbestemte tilladelse tilsyneladende Electronic Communications Privacy Act (18 U.S.C. § 2709), hvori det fastslås, at der i enhver anmodning om abonnent- eller transaktionsoplysninger skal anvendes en »term, der specifikt identificerer en person, en enhed, et telefonnummer eller en konto«.

registrerede i EU overført under EU's og USA's værn om privatlivets fred. Foruden Sec. 104 i FISA ⁽⁸⁰⁾ vedrørende individualiseret elektronisk overvågning og Sec. 402 i FISA ⁽⁸¹⁾ om installation af pen-register- eller trap and trace-anordninger er de to centrale instrumenter Sec. 501 i FISA (ex-Section 215 U.S. PATRIOT ACT) og Section 702 i FISA ⁽⁸²⁾.

- (79) I den forbindelse forbyder USA FREEDOM Act, som trådte i kraft den 2. juni 2015, masseindsamling af oplysninger baseret på Sec. 402 i FISA (pen-register og trap and trace-tilladelse), Sec. 501 i FISA (tidligere Sec 215 i U.S. PATRIOT Act) ⁽⁸³⁾ og anvendelsen af NSL, idet der i stedet anvendes specifikke selektorer ⁽⁸⁴⁾.
- (80) Selv om FISA indeholder yderligere lovbestemte tilladelser til at udføre nationale efterretningsaktiviteter, herunder signalefterretning, viser Kommissionens vurdering, at disse tilladelser i forbindelse med overførsel af personoplysninger under EU's og USA's værn om privatlivets fred ligeledes begrænser offentlige indgreb til målrettet indsamling og adgang.
- (81) Dette er klart for traditionel individualiseret elektronisk overvågning i henhold til Sec. 104 i FISA ⁽⁸⁵⁾. I henhold til Sec. 702 i FISA, der udgør retsgrundlaget for to af de amerikanske efterretningsagenturers vigtige efterretningsprogrammer (Prism og Upstream), skal søgninger foretages målrettet ved brug af individuelle selektorer, der identificerer specifikke kommunikationsfaciliteter såsom målets e-mailadresse eller telefonnummer, men ikke nøgleord eller endog navnene på de pågældende personer ⁽⁸⁶⁾. Som påpeget af Privacy and Civil Liberties

⁽⁸⁰⁾ United States Code, afsnit 50, § 1804. I dette retsgrundlag stilles der krav om en »erklæring om de faktiske forhold og omstændigheder, som den anmodende part gør gældende for at begrunde sin antagelse om, at (A) målet for den elektroniske overvågning er en fremmed magt eller en agent fra en fremmed magt«, og sidstnævnte kan omfatte ikke-amerikanske personer involveret i international terrorisme eller international spredning af masseødelæggelsesvåben (herunder forberedende foranstaltninger) (50 U.S.C. § 1801 (b)(1)). Der er imidlertid kun en teoretisk forbindelse til personoplysninger overført under EU's og USA's værn om privatlivets fred, da redegørelsen for sagens kendsgerninger også skal begrunde antagelsen om, at »de enkelte faciliteter eller steder, der skal overvåges elektronisk, anvendes eller snart vil blive anvendt af en fremmed magt eller en agent fra en fremmed magt«. For at opnå denne tilladelse skal der under alle omstændigheder indgives en anmodning til FISC, der bl.a. vil vurdere, om der på grundlag af de forelagte faktiske forhold er begrundet mistanke (»probable cause«) om, at dette reelt er tilfældet.

⁽⁸¹⁾ U.S.C. afsnit 50 § 1842 sammenholdt med § 1841(2), og Sec. 3127 i Titel 18. 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). Der skal i denne forbindelse indgives en anmodning til FISC (eller en amerikansk undersøgelsesdommer) om en retsafgørelse og anvendes specifikke selektorer i henhold til § 1841(4), 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.

⁽⁸²⁾ Selv om FBI i henhold til Sec. 501 i FISA (ex-Sec. 215 U.S. PATRIOT ACT) har bemyndigelse til at anmode om en retsafgørelse om udlevering af »materielle genstande« (navnlig telefonmetadata, men også forretningsoplysninger) til udenlandske efterretningsformål, kan amerikanske efterretningsselementer i henhold til Sec. 702 i FISA søge indsigt i oplysninger, herunder i indholdet af internetkommunikation, fra USA, men som vedrører ikke-amerikanske personer uden for USA.

⁽⁸³⁾ I henhold til denne bestemmelse kan FBI anmode om materielle ting — »tangible things« — (f.eks. optegnelser, papirer, dokumenter) ved at dokumentere over for den amerikanske domstol for overvågning af efterretningsvirksomhed i udlandet, Foreign Intelligence Surveillance Court (FISC), at der er rimelige grunde til at antage, at de er relevante for en specifik FBI-undersøgelse. Ved søgningen skal FBI anvende FISC-godkendte selektorer, hvor der er en begrundet og klar mistanke (»reasonable, articulable suspicion«) om, at disse termer er relateret til en eller flere fremmede magter eller deres agenter involveret i international terrorisme eller forberedelse heraf. Jf. PCLOB, Sec. 215 Report, s. 59. Jf. NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016, s. 4-6.

⁽⁸⁴⁾ ODNI's udredninger (bilag VI), s. 13 (n. 38).

⁽⁸⁵⁾ Se fodnote 81.

⁽⁸⁶⁾ Jf. PCLOB Sec. 702 Report, s. 32-33, med yderligere henvisninger. Ifølge NSA's kontor for beskyttelse af privatlivets fred skal NSA 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. Se NSA CLPO, NSA's Implementation of Foreign Intelligence Act Sec. 702, 16.4.2014.

Oversight Board (PCLOB) (rådet for tilsyn med privatlivets fred og borgerlige rettigheder) er overvågning i henhold til Sec. 702 således »udelukkende rettet mod specifikke [ikke-amerikanske] personer, som er blevet individuelt identificeret«⁽⁸⁷⁾. På grund af en udløbsklausul skal Sec. 702 i FISA revideres i 2017, og Kommissionen skal på dette tidspunkt revurdere de garantier, som registrerede i EU har.

- (82) Den amerikanske regering har i sine udredninger desuden specifikt forsikret Europa-Kommissionen om, at de amerikanske efterretningstjenester »ikke foretager vilkårlig overvågning af nogen, herunder almindelige europæiske borgere«⁽⁸⁸⁾. Med hensyn til personoplysninger indsamlet i USA understøttes denne erklæring af empirisk dokumentation, der viser, at *anmodninger om indsigt* gennem NSL og i henhold til FISA, både hver for sig og samlet, kun vedrører et forholdsvis lille antal mål sammenlignet med den generelle datastrøm på internettet⁽⁸⁹⁾.
- (83) Med hensyn til *indsigt* i indsamlede data og *datasikkerhed* skal indsigt i henhold til PPD-28 »begrænses til autoriseret personale, der har brug for oplysningerne for at varetage deres opgaver«, og personoplysninger skal »behandles og lagres under forhold, der giver tilstrækkelig beskyttelse og hindrer personer uden tilladelse i at få indsigt i overensstemmelse med de gældende garantier for følsomme oplysninger«. Det amerikanske efterretningspersonale skal oplyses om principperne i PPD-28 på passende og tilstrækkelig vis⁽⁹⁰⁾.
- (84) Med hensyn til *lagring* og yderligere *formidling* af personoplysninger fra registrerede i EU, der er indsamlet af de amerikanske efterretningsmyndigheder, anføres det i PPD-28, at alle personer (herunder ikke-amerikanske personer) bør behandles med værdighed og respekt, at alle personer har legitime interesser i beskyttelsen af privatlivets fred ved behandlingen af deres personoplysninger, og at efterretningsenhederne derfor skal indføre politikker, der giver tilstrækkelige garantier for sådanne oplysninger og »i rimeligt omfang er udformet med henblik på at minimere formidlingen og opbevaringen heraf«⁽⁹¹⁾.

⁽⁸⁷⁾ Jf. PCLOB, Sec. 702 Report, s. 111. Se også ODNI's udredninger (bilag VI), s. 9 (»Indsamling i henhold til Sec. 702 i [FISA] er ikke« omfattende og vilkårlig», men er snævert fokuseret på indsamling af udenlandske efterretninger fra individuelt identificerede legitime mål») og s. 13, n. 36 (med henvisning til en FISC-udtalelse fra 2014), NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. Selv i forbindelse med Upstream må NSA kun anmode om opfangning af elektronisk kommunikation til, fra eller om udvalgte selektorer.

⁽⁸⁸⁾ ODNI's udredninger (bilag VI), s. 18. Se også s. 6, hvor det anføres, at de anvendte procedurer »viser, at der er en klar vilje til at forhindre vilkårlig indsamling af signalefterretninger og til at gennemføre princippet om rimelighed på højeste regeringsniveau«.

⁽⁸⁹⁾ Se Statistical Transparency Report Regarding Use of National Security Authorities, 22.4.2015. For yderligere oplysninger om den generelle datastrøm på internettet henvises f.eks. til rapporten fra EU's Agentur for Grundlæggende Rettigheder »Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU« (2015), s. 15-16. Hvad angår Upstream-programmet tegnede det ifølge en afklassificeret FISC-udtalelse fra 2011 sig kun for 10 % af den elektroniske kommunikation opfanget efter Sec. 702 i FISA, Prism-programmet tegnede sig for 90 %. Se FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), n. 21 (tilgængelig på adressen: <http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>).

⁽⁹⁰⁾ Jf. Sec. 4(a)(ii) i PPD-28. Se også ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive af 28. juli 2014, s. 5, hvori det anføres, at »efterretningsenhedernes politikker skal styrke eksisterende analysepraksis og -standarder med krav om, at analytikerne skal strukturere deres søgninger eller andre søgetermer og -teknikker for at identificere efterretningsoplysninger, der er relevante for en gyldig efterretnings- og retshåndhævelsesopgave, rette søgninger om personer mod de kategorier af efterretningsoplysninger, der er relevante i efterretnings- og retshåndhævelsesøjemed, og minimere gennemgangen af personoplysninger, der ikke er relevante i efterretnings- og retshåndhævelsesøjemed«. Se f.eks. CIA, Signals Intelligence Activities, s. 5, FBI, Presidential Policy Directive 28 Policies and Procedures, s. 3. Ifølge Progress Report on the Signals Intelligence Reform fra 2016 har en række efterretningsenheder (herunder FBI, CIA og NSA) truffet foranstaltninger med henblik på at oplyse deres personale om kravene i PPD-28 ved at udvikle nye eller ændre eksisterende uddannelsespolitikker.

⁽⁹¹⁾ Ifølge ODNI's udredninger finder disse begrænsninger anvendelse, uanset om oplysningerne er blevet masseindsamlet eller indsamlet på målrettet vis, og uafhængigt af personens nationalitet.

- (85) Den amerikanske regering har forklaret, at dette krav om rimelighed betyder, at efterretningsenhederne ikke skal gennemføre »enhver foranstaltning, der er teoretisk mulig«, men at de skal »veje deres foranstaltninger til beskyttelse af legitime hensyn til privatlivets fred og borgerlige rettigheder op mod de praktiske krav til signalefterretningsaktiviteter«⁽⁹²⁾. Ikke-amerikanske personer vil i denne forbindelse blive behandlet på samme måde som amerikanske borgere i henhold til procedurer godkendt af den amerikanske justitsminister (Attorney General)⁽⁹³⁾.
- (86) I henhold til disse bestemmelser må oplysninger generelt kun opbevares i højst fem år, medmindre der er en særlig bestemmelse i lovgivningen, eller medmindre direktøren for National Intelligence efter grundig evaluering af beskyttelsen af privatlivets fred og under hensyntagen til de holdninger, som ODNI's Civil Liberties Protection Officer samt databeskyttelsesansvarlige (privacy and civil liberties officers) i de forskellige agenturer giver udtryk for, bestemmer, at fortsat opbevaring er i den nationale sikkerheds interesse⁽⁹⁴⁾. Formidlingen er begrænset til tilfælde, hvor oplysningerne er relevante for det underliggende formål med indsamlingen og således opfylder godkendte udenlandske efterretnings- eller retshåndhævelsesformål⁽⁹⁵⁾.
- (87) Ifølge den amerikanske regerings garantier må personoplysninger ikke formidles udelukkende med den begrundelse, at den pågældende er udlænding, og »signalefterretninger om en udlændings rutinemæssige aktiviteter vil ikke blive betragtet som udenlandske efterretninger, der kan formidles eller opbevares permanent alene af denne årsag, medmindre de på anden vis opfylder et godkendt behov for udenlandske efterretninger«⁽⁹⁶⁾.
- (88) Kommissionen konkluderer på baggrund af ovenstående, at USA har indført regler, hvorved det tilsigtes at begrænse de eventuelle indgreb af hensyn til den nationale sikkerhed i de grundlæggende rettigheder hos de personer, hvis oplysninger overføres fra EU til USA under EU's og USA's værn om privatlivets fred, til det strengt nødvendige med henblik på at nå det tilsigtede mål.
- (89) Som ovenstående analyse har vist, sikrer amerikansk ret, at overvågningsforanstaltningerne kun vil blive anvendt til indsamling af udenlandske efterretningsoplysninger, hvilket er et legitimt politisk mål⁽⁹⁷⁾, og at de vil være så

⁽⁹²⁾ Se ODNI's udredninger (bilag VI).

⁽⁹³⁾ Se Sec. 4(a)(i) i PPD-28 sammenholdt med Sec. 2.3 i E.O. 12333.

⁽⁹⁴⁾ Sec. 4(a)(i) i PPD-28, ODNI's udredninger (bilag VI), s. 7. Hvad angår personoplysninger indsamlet i henhold til Sec. 702 i FISA, fastslås det f.eks. i NSA's FISC-godkendte minimeringsprocedurer, at metadata og ikkeevalueret indhold for Prism generelt kun må opbevares i fem år, hvorimod Upstream-data kun må opbevares i to år. NSA overholder disse opbevaringsgrænser ved hjælp af en automatiseret proces, hvor indsamlede data slettes ved udløbet af opbevaringsperioden. Se NSA Sec. 702 i FISA, Minimization Procedures, Sec. 7 sammenholdt med Sec. 6(a)(1), NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act, Sec. 702, 16.4.2014. Opbevaring i henhold til Sec. 501 i FISA (ex-Sec. 215 U.S. PATRIOT ACT) er begrænset til fem år, medmindre personoplysningerne er omfattet af en behørigt godkendt formidling af udenlandske efterretningsoplysninger, eller medmindre det amerikanske justitsministerium skriftligt meddeler NSA, at oplysningerne skal opbevares i en verserende eller forventet retssag. Se NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016.

⁽⁹⁵⁾ I henhold til Sec. 501 i FISA (ex-Sec. 215 U.S. PATRIOT ACT) må personoplysninger navnlig kun formidles i forbindelse med terrorbekæmpelse eller som bevis for en forbrydelse, og i henhold til Sec. 702 i FISA kun til godkendte udenlandske efterretnings- eller retshåndhævelsesformål. Jf. NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act, Sec. 702, 16.4.2014. Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016. Se også NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014.

⁽⁹⁶⁾ ODNI's udredninger (bilag VI), s. 7 (med henvisning til Intelligence Community Directive (ICD) 203).

⁽⁹⁷⁾ Domstolen har slået fast, at national sikkerhed udgør et legitimt politisk mål. Se Schrems, præmis 88. Se også dommen i Digital Rights Ireland m.fl., præmis 42-44 og 51, hvori Domstolen fastslår, at bekæmpelse af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, i vid udstrækning kan være afhængig af anvendelsen af moderne efterforskningsmetoder. Dertil kommer, at efterretningsaktiviteter, i modsætning til strafferetlige efterforskninger, som typisk vedrører den retrospektive fastsættelse af ansvar og skyld for tidligere adfærd, ofte fokuserer på forebyggelse af trusler mod national sikkerhed, før skaden sker. Sådanne efterforskninger skal følgelig ofte omfatte en bredere vifte af mulige aktører (»mål«) og et større geografisk område. Jf. ECHR, *Weber and Saravia v. Germany*, afgørelse af 29.6.2006, begæring nr. 54934/00, præmis 105-118 (om såkaldt »strategisk overvågning«).

måltrettede som muligt. Navnlig vil masseindsamling kun undtagelsesvist blive godkendt i tilfælde, hvor måltrettet indsamling ikke er mulig, og skal ledsages af ekstra garantier, som minimerer mængden af indsamlede oplysninger og den efterfølgende adgang hertil (som skal målrette og kun godkendes til specifikke formål).

- (90) Efter Kommissionens opfattelse passer dette med den standard, som Domstolen har sat i Schrems-dommen, ifølge hvilken den lovgivning, som indebærer et indgreb i de ved chartrets artikel 7 og 8 sikrede grundlæggende rettigheder, skal indføre »minimumsgarantier«⁽⁹⁸⁾ og »på generel vis tillader opbevaring af samtlige personoplysninger fra samtlige de personer, hvis oplysninger er blevet overført fra Unionen til USA, uden at der bliver foretaget nogen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål, og uden at der bliver fastsat noget objektivt kriterium, som gør det muligt at afgrænse de offentlige myndigheders adgang til oplysningerne og deres senere anvendelse heraf med henblik på veldefinerede formål, der er strengt begrænsede, og som kan begrunde det indgreb, som såvel adgangen til disse oplysninger som anvendelsen heraf indebærer, er således ikke begrænset til det strengt nødvendige«⁽⁹⁹⁾. Der vil heller ikke være ubegrænset indsamling og opbevaring af oplysninger for alle personer uden nogen begrænsninger eller ubegrænset adgang. Derudover udelukkes det i de udredninger, som Kommissionen har modtaget, herunder garantierne om, at USA's signalefterretningsaktiviteter kun vedrører en meget lille del af kommunikationen på internettet, at der vil være tale om en »generel«⁽¹⁰⁰⁾ adgang til indholdet af den elektroniske kommunikation⁽¹⁰¹⁾.

3.1.2. Effektiv retsbeskyttelse

- (91) Kommissionen har både vurderet de eksisterende mekanismer i USA for tilsyn med de amerikanske efterretningsmyndigheders indgreb i personoplysninger overført til USA og de individuelle klagemuligheder, som registrerede i EU har.

Tilsyn

- (92) Den amerikanske efterretningstjeneste er genstand for adskillige kontrol- og tilsynsordninger, som hører under statsmagtens tre grene. Der er tale om interne og eksterne organer under den udøvende magt, et antal kongresudvalg og enheder, der har til opgave at føre retsligt tilsyn med aktiviteter under Foreign Intelligence Surveillance Act.
- (93) For det første er de amerikanske myndigheders efterretningsaktiviteter underlagt et omfattende tilsyn fra den udøvende magts side.
- (94) I henhold til PPD-28, afsnit 4(a)(iv), skal efterretningsenhedernes politikker og procedurer »omfatte passende foranstaltninger, der letter tilsynet med gennemførelsen af garantier for beskyttelse af personoplysninger«, og disse foranstaltninger bør omfatte regelmæssig revision⁽¹⁰¹⁾.

⁽⁹⁸⁾ Schrems, præmis 91, med yderligere henvisninger.

⁽⁹⁹⁾ Schrems, præmis 93.

⁽¹⁰⁰⁾ Jf. Schrems, præmis 94.

⁽¹⁰¹⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, s. 7. Se f.eks. CIA, Signals Intelligence Activities, s. 6 (Responsibilities). FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4), NSA, PPD-28 Sec. 4, Procedures, 12.1.2015, Sec. 8.1, 8.6(c).

- (95) Der er i denne forbindelse indført flere lag, herunder databeskyttelsesansvarlige (privacy and civil liberties officers), generalinspektører (inspectors general), ODNI's Civil Liberties and Privacy Office, PCLOB og President's Intelligence Oversight Board. Disse tilsynsfunktioner understøttes af kontrolmedarbejdere i alle agenturerne ⁽¹⁰²⁾.
- (96) Som anført af den amerikanske regering ⁽¹⁰³⁾ er der udpeget databeskyttelsesansvarlige (civil liberties or privacy officers) med tilsynsfunktioner i forskellige ministerier med efterretningsopgaver og i efterretningsagenturer ⁽¹⁰⁴⁾. Selv om disse databeskyttelsesansvarliges specifikke beføjelser kan variere afhængigt af lovhjemlen, omfatter de typisk tilsynet med procedurer for at sikre, at det pågældende ministerium/agentur tager tilstrækkeligt hensyn til beskyttelsen af privatlivets fred og borgerlige rettigheder, og at der er indført passende procedurer for behandling af klager fra fysiske personer, der mener, at deres privatliv eller borgerlige rettigheder er blevet krænket (og i nogle tilfælde har de selv beføjelse til at undersøge klager ⁽¹⁰⁵⁾, f.eks. ODNI). Lederen af ministeriet/agenturet skal sikre, at den databeskyttelsesansvarlige modtager alle de oplysninger og får adgang til alt det materiale, der er nødvendigt for at udføre dennes opgaver. Databeskyttelsesansvarlige rapporterer regelmæssigt til den amerikanske kongres og PCLOB, herunder om antallet og karakteren af de klager, som ministeriet/agenturet har modtaget, med en oversigt over afgørelserne i disse klagesager, de gennemførte undersøgelser og forespørgsler og resultaterne af deres aktiviteter ⁽¹⁰⁶⁾. Ifølge den vurdering, som de nationale databeskyttelsesmyndigheder har foretaget, kan de databeskyttelsesansvarliges interne tilsyn betragtes som »forholdsvis robust«, om end de set fra deres synspunkt ikke har den nødvendige uafhængighed ⁽¹⁰⁷⁾.
- (97) Hver efterretningsenhed har desuden sin egen generalinspektør med ansvar for tilsyn med bl.a. udenlandske efterretningsaktiviteter ⁽¹⁰⁸⁾. ODNI har således sit eget Office of the Inspector General (generalinspektørens kontor) med brede beføjelser til at føre tilsyn med alle amerikanske efterretningstjenester og til at undersøge klager eller oplysninger om påstande om ulovlig praksis eller magtmisbrug i forbindelse med ODNI's og/eller efterretningstjenesternes programmer og aktiviteter ⁽¹⁰⁹⁾. Generalinspektører er lovmæssigt uafhængige ⁽¹¹⁰⁾ enheder med ansvar for revisioner og undersøgelser af de programmer og operationer, det pågældendeagentur gennemfører til nationale efterretningsformål, herunder af misbrug og lovovertrædelser ⁽¹¹¹⁾. De er bemyndiget til at få adgang til alle optegnelser, rapporter, revisioner, evalueringer, dokumenter, papirer, anbefalinger eller andet

⁽¹⁰²⁾ NSA beskæftiger f.eks. over 300 kontrolmedarbejdere i kontroldirektoratet. Se ODNI's udredninger (bilag VI), s. 7.

⁽¹⁰³⁾ Se ombudsmandsmekanismen (bilag III), punkt 6, b), nr. i)-iii).

⁽¹⁰⁴⁾ Jf. United States Code, afsnit 42, paragraf 2000ee-1. Herunder udenrigsministeriet (Department of State), justitsministeriet (Department of Justice) (herunder FBI), ministeriet for national sikkerhed (Department of Homeland Security), forsvarsministeriet (Department of Defense), NSA, CIA og ODNI.

⁽¹⁰⁵⁾ Ifølge den amerikanske regering vil ODNI's Civil Liberties and Privacy Office, når det modtager en klage, også koordinere de amerikanske efterretningstjenesters videre behandling af klagen med andre efterretningsenheder. Se ombudsmandsmekanismen (bilag III), punkt 6, b), nr. ii).

⁽¹⁰⁶⁾ See United States Code, afsnit 42, paragraf 2000ee-1 (f)(1),(2).

⁽¹⁰⁷⁾ Artikel 29-Gruppen vedrørende Databeskyttelse, udtalelse 01/2016 om udkastet til afgørelse om tilstrækkeligheden af EU's og USA's værn om privatlivets fred (vedtaget den 13. april 2016), s. 41.

⁽¹⁰⁸⁾ ODNI's udredninger (bilag VI), s. 7. Se f.eks. NSA, PPD-28 Sec. 4, Procedures, 12.1.2015, Sec. 8.1, CIA, Signals Intelligence Activities, s. 7 (Responsibilities).

⁽¹⁰⁹⁾ Denne generalinspektør (en funktion, der blev oprettet i oktober 2010) udnævnes af præsidenten med Senatets godkendelse og kan afsættes af præsidenten, men ikke af DNI.

⁽¹¹⁰⁾ 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 og fuldføre en revision eller efterforskning, hvis det anses for nødvendigt for at beskytte vigtige nationale (sikkerheds)interesser. Den amerikanske kongres skal imidlertid orienteres om udøvelse af denne myndighed og kan på dette grundlag holde den pågældende chef ansvarlig. Se f.eks. Inspector General Act fra 1978, paragraf 8 (forsvarsministeriets generalinspektør), paragraf 8E (justitsministeriets generalinspektør), paragraf 8G (d)(2)(A),(B) (NSA's generalinspektør), 50. United States Code, paragraf 403q (b) (CIA's generalinspektør), Intelligence Authorization Act For Fiscal Year 2010, Sec. 405(f) (generalinspektør for efterretningstjenesterne). Ifølge de nationale databeskyttelsesmyndigheders vurdering er det sandsynligt, at generalinspektørerne »opfylder kriterierne for organisatorisk uafhængighed som defineret af EU-Domstolen og Den Europæiske Menneskerettighedsdomstol (ECHR), i det mindste fra tidspunkt, hvor den nye udnævnelsesproces gælder for alle.« Se Artikel 29-Gruppen vedrørende Databeskyttelse, udtalelse 01/2016 om udkastet til afgørelse om tilstrækkeligheden af EU's og USA's værn om privatlivets fred (vedtaget den 13. april 2016), s. 40.

⁽¹¹¹⁾ Se ODNI's udredninger (bilag VI), s. 7. Se også Inspector General Act fra 1978, som ændret, Pub. L. 113-126 af 7.7.2014.

relevant materiale, om nødvendigt på grundlag af en »subpoena« (pålæg), og kan indhente vidneudsagn ⁽¹¹²⁾. Selv om generalinspektørerne kun kan fremsætte ikkebindende anbefalinger om korrigerende foranstaltninger, offentliggøres deres rapporter, herunder om opfølgende foranstaltninger (eller mangel herpå), og de fremsendes desuden til den amerikanske kongres, der på dette grundlag kan udøve sin tilsynsfunktion ⁽¹¹³⁾.

- (98) *Privacy and Civil Liberties Oversight Board* (PCLOB), som er et uafhængigt eksekutivt råd ⁽¹¹⁴⁾ bestående af fem medlemmer fra de to partier ⁽¹¹⁵⁾ og udnævnt af præsidenten for en fast seksårig periode med senatets godkendelse, har en række ansvarsområder relateret til terrorbekæmpelsespolitikker og deres gennemførelse med henblik på at beskytte privatlivets fred og borgerlige rettigheder. Rådet kan i forbindelse med sin revision af efterretningstjenestens handlinger få adgang til alle agenturnes relevante optegnelser, rapporter, revisioner, evalueringer, dokumenter, papirer og anbefalinger, herunder klassificerede informationer, gennemføre interview og indhente vidneudsagn. Det modtager rapporter fra databeskyttelsesansvarlige i en række føderale ministerier og agenturer ⁽¹¹⁶⁾, det kan udstede anbefalinger til dem og rapporterer regelmæssigt til forskellige kongresudvalg og præsidenten ⁽¹¹⁷⁾. PCLOB har ligeledes til opgave at udarbejde en rapport inden for sit mandat med en vurdering af gennemførelsen af PPD-28.
- (99) Endelig suppleres ovennævnte tilsynsmekanismer af *Intelligence Oversight Board* nedsat under President's Intelligence Advisory Board, der fører tilsyn med de amerikanske efterretningsmyndigheders overholdelse af forfatningen og alle gældende bestemmelser.
- (100) For at lette tilsynet opfordres efterretningsenheder til at udforme informationssystemer, der gør det muligt at overvåge, registrere og gennemgå søgninger eller andre forespørgsler om personoplysninger. ⁽¹¹⁸⁾ Tilsyns- og kontrolorganer vil jævnligt kontrollere efterretningsenhedernes praksis for beskyttelse af personoplysninger indeholdt i signalefterretninger og deres overholdelse af disse procedurer ⁽¹¹⁹⁾.
- (101) Disse tilsynsfunktioner er ligeledes understøttet af omfattende krav om rapportering af manglende overholdelse. Agenturnes procedurer skal navnlig sikre, at alvorlige tilfælde af manglende overholdelse, der involverer personoplysninger, uanset for hvem og uanset nationalitet, indsamlet gennem signalefterretning, straks indberettes til lederen af efterretningsenheden, som herefter underretter direktøren for National Intelligence, der i henhold til PPD-28 beslutter, om der skal træffes korrigerende foranstaltninger ⁽¹²⁰⁾. I henhold til E.O. 12333 skal alle efterretningsenheder indberette tilfælde af manglende overholdelse til Intelligence Oversight Board ⁽¹²¹⁾. Disse mekanismer sikrer, at dette spørgsmål behandles på højeste niveau i efterretningstjenesterne. Hvis en

⁽¹¹²⁾ Se Inspector General Act fra 1978, paragraf 6.

⁽¹¹³⁾ Se ODNI's udredninger (bilag VI), s. 7. Se også Inspector General Act fra 1978, paragraf 4(5). I henhold til Sec. 405(b)(3),(4) i Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259 af 7.10.2010 skal generalinspektøren for efterretningstjenesterne holde DNI og den amerikanske kongres orienteret om behovet og status for korrigerende foranstaltninger.

⁽¹¹⁴⁾ Ifølge de nationale databeskyttelsesmyndigheders vurdering har PCLOB tidligere vist sig uafhængig. Se Artikel 29-Gruppen vedrørende Databeskyttelse, udtalelse 01/2016 om udkastet til afgørelse om tilstrækkeligheden af EU's og USA's værn om privatlivets fred (vedtaget den 13. april 2016), s. 42.

⁽¹¹⁵⁾ PCLOB har omkring 20 fastansatte medarbejdere. Se <https://www.pclob.gov/about-us/staff.html>.

⁽¹¹⁶⁾ Disse omfatter som minimum justitsministeriet (Department of Justice), forsvarsministeriet (Department of Defense), ministeriet for national sikkerhed (Department of Homeland Security), direktøren for National Intelligence (DNI) og direktøren for Central Intelligence Agency (CIA) samt andre ministerier, agenturer eller enheder inden for den udøvende magt, som PCLOB betragter som relevante i denne sammenhæng.

⁽¹¹⁷⁾ Jf. United States Code, afsnit 42, paragraf 2000ee. Se også ombudsmandsmekanismen (bilag III), punkt 6, b), nr. iv). PCLOB skal bl.a. rapportere, når et agentur under den udøvende magt nægter at følge PCLOB's råd.

⁽¹¹⁸⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, s. 7.

⁽¹¹⁹⁾ Idem s. 8. Se ligeledes ODNI's udredninger (bilag VI), s. 9.

⁽¹²⁰⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, s. 7. Se f.eks. NSA, PPD-28 Sec. 4 Procedures, 12.1.2015, Sec. 7.3, 8.7(c),(d); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4), CIA, Signals Intelligence Activities, s. 6 (Compliance) og s. 8 (Responsibilities).

⁽¹²¹⁾ Se E.O. 12333, Sec. 1.6(c).

ikke-amerikansk person er involveret, beslutter direktøren for National Intelligence i samråd med den amerikanske udenrigsminister og lederen af det indberettende ministerium/agentur, om der bør tages skridt til at underrette den relevante udenlandske regering, hvis det er foreneligt med beskyttelsen af kilder og metoder og personer i De Forenede Staters tjeneste ⁽¹²²⁾.

- (102) Ud over disse tilsynsmekanismer i den udøvende magt fører den amerikanske kongres, navnlig Repræsentanternes Hus og Senatets efterretnings- og retsudvalg — House and Senate Intelligence and Judiciary Committees — tilsyn med alle amerikanske udenlandske efterretningsaktiviteter, herunder amerikansk signalefterretning. 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« ⁽¹²³⁾. Det anføres ligeledes, at »præsidenten sikrer, at enhver ulovlig efterretningsaktivitet og enhver gennemført eller planlagt korrigerende foranstaltning over for denne ulovlige aktivitet straks indberettes til kongressens efterretningsudvalg« ⁽¹²⁴⁾. Udvalgsmedlemmerne har både adgang til klassificerede informationer og efterretningsmetoder og -programmer ⁽¹²⁵⁾.
- (103) Senere love har udvidet og finjusteret rapporteringskravene, både til efterretningsenhederne, de relevante generalinspektører og den amerikanske justitsminister. I henhold til FISA skal den amerikanske justitsminister f. eks. »orientere« Repræsentanternes Hus og Senatets efterretnings- og retsudvalg »fuldt ud« om regeringens aktiviteter i henhold til bestemte paragraffer i FISA ⁽¹²⁶⁾. Der stilles ligeledes krav om at give kongresudvalgene kopier af »alle afgørelser, kendelser eller udtalelser fra Foreign Intelligence Surveillance Court eller Foreign Intelligence Surveillance Court of Review, som indeholder en væsentlig forståelse eller fortolkning« af FISA-bestemmelser. Med hensyn til overvågning i henhold til afsnit 702 i FISA udøves tilsynet navnlig 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 afsnit 702 i FISA med tilhørende dokumenter, herunder navnlig justitsministeriets og ODNI's overholdelsesrapporter og en redegørelse for eventuelle tilfælde af manglende overholdelse ⁽¹²⁷⁾, og en særskilt halvårlig vurdering fra den amerikanske justitsminister og DNI, der dokumenterer overholdelsen af målretnings- og minimeringsprocedurerne, herunder overholdelse af de procedurer, der skal sikre, at oplysninger indsamles til godkendte udenlandske efterretningsformål ⁽¹²⁸⁾. Den amerikanske kongres modtager ligeledes rapporter fra generalinspektørerne, der har beføjelse til at evaluere agenturernes overholdelse af målretnings- og minimeringsprocedurerne og den amerikanske justitsministers retningslinjer.
- (104) I henhold til USA FREEDOM Act fra 2015 skal den amerikanske regering hvert år bl.a. oplyse kongressen (og offentligheden) om det antal FISA-kendelser og -direktiver, der er anmodet om og udstedt, og om det skønnede antal overvågede amerikanske og ikke-amerikanske personer ⁽¹²⁹⁾. I loven stilles der ligeledes yderligere krav om offentliggørelse af antallet af udstedte NSL'er, også her vedrørende både amerikanske og ikke-amerikanske

⁽¹²²⁾ PPD-28, Sec. 4(a)(iv).

⁽¹²³⁾ Se afsnit 501(a)(1) (United States Code, afsnit 50, paragraf 413(a)(1)). Denne bestemmelse indeholder generelle krav vedrørende kongressens tilsyn med nationale sikkerhedsanliggender.

⁽¹²⁴⁾ Se afsnit 501(b) (United States Code, afsnit 50, paragraf 413(b)).

⁽¹²⁵⁾ Jf. afsnit 501(d) (United States Code, afsnit 50, paragraf 413(d)).

⁽¹²⁶⁾ Jf. United States Code, afsnit 50, paragraf 1808, 1846, 1862, 1871 og 1881f.

⁽¹²⁷⁾ Jf. United States Code, afsnit 50, paragraf 1881f.

⁽¹²⁸⁾ Jf. United States Code, afsnit 50, paragraf 1881 a(l)(1).

⁽¹²⁹⁾ Se USA FREEDOM Act fra 2015, Pub. L. No. 114-23, Sec. 602(a). I henhold til Sec. 402 skal »direktøren for National Intelligence 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 Sec. 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«.

personer (og modtagerne af FISA-kendelser og -certificeringer og NSL-anmodninger får mulighed for at udarbejde gennemsigthedsrapporter på visse betingelser) ⁽¹³⁰⁾.

- (105) De amerikanske offentlige myndigheders efterretningsaktiviteter i henhold til FISA er undergivet FISA-domstolens (FISC) ⁽¹³¹⁾ prøvelsesret, og foranstaltningerne skal i nogle tilfælde forhåndsgodkendes af domstolen, der er en uafhængig domstol ⁽¹³²⁾, hvis afgørelser kan indbringes for Foreign Intelligence Court of Review (FISCR) ⁽¹³³⁾ og i sidste ende for Supreme Court of the United States (De Forenede Staters højesteret) ⁽¹³⁴⁾. For at opnå en forhåndsgodkendelse skal de anmodende myndigheder (FBI, NSA, CIA osv.) indsende et udkast af anmodningen til jurister i det amerikanske justitsministeriums departement for national sikkerhed, som vil undersøge det og om nødvendigt anmode om yderligere oplysninger ⁽¹³⁵⁾. Når anmodningen er udarbejdet, skal den godkendes af justitsministeren (Attorney General), vicejustitsministeren (Deputy Attorney General) eller den assisterende justitsminister for national sikkerhed (Assistant Attorney General for National Security) ⁽¹³⁶⁾. Justitsministeriet vil herefter forelægge anmodningen for FISC, som vil vurdere anmodningen og træffe en foreløbig afgørelse om det videre forløb ⁽¹³⁷⁾. I forbindelse med høringer har FISC beføjelse til at indhente vidneudsagn, herunder ekspertrådgivning ⁽¹³⁸⁾.

- (106) FISC (og FISCR) understøttes af et fast panel bestående af fem eksperter i national sikkerhed og borgerlige rettigheder ⁽¹³⁹⁾. 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 mening udgør en ny eller væsentlig fortolkning af lovbestemmelser, medmindre domstolen finder, at en sådan udnævnelse ikke er hensigtsmæssig ⁽¹⁴⁰⁾. Dette skal navnlig sikre, at hensynet til privatlivets fred afspejles behørigt i domstolens vurdering. Domstolen kan ligeledes udpege en person eller et foretagende til at optræde som amicus curiae, herunder bistå med teknisk ekspertise, når den finder det hensigtsmæssigt, eller på begæring tillade personer eller foretagender at indgive amicus curiae-indlæg ⁽¹⁴¹⁾.

⁽¹³⁰⁾ USA FREEDOM Act, Sec. 602(a), 603(a).

⁽¹³¹⁾ I forbindelse med visse typer overvågning kan en amerikansk dommer (magistrate judge) officielt udnævnt af USA's højesteretspræsident (Chief Justice of the United States) have beføjelse til at behandle anmodninger og afsige kendelser.

⁽¹³²⁾ FISC består af 11 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 7-årige embedsperioder. I henhold til FISA skal dommerne hentes fra mindst syv forskellige amerikanske retskredse. Se Sec. 103 i FISA (United States Code, Sec. 50, paragraf 1803 (a)), PCLOB, Sec. 215 Report, s. 174-187. Dommerne bistås af erfarne dommerfuldmægtige, der udgør domstolens retspersonale og udarbejder juridiske analyser af anmodninger om indsamling. Se PCLOB, Sec. 215 Report, s. 178. Brev fra Reggie B. Walton, retspræsident for U.S. Foreign Intelligence Surveillance Court, til Patrick J. Leahy, formand for retsudvalget i det amerikanske senat (den 29. juli 2013), («Walton-brevet»), s. 2-3.

⁽¹³³⁾ FISCR består af tre dommere udnævnt af USA's højesteretspræsident og hentet fra amerikanske distriktsdomstole eller appeldomstole, og de sidder i en forskudt 7-årig embedsperiode. Se Sec. 103 i FISA (United States Code, afsnit 50, paragraf 1803 (b)).

⁽¹³⁴⁾ Se United States Code, afsnit 50, paragraf 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

⁽¹³⁵⁾ F.eks. yderligere faktuelle oplysninger om målet for overvågningen, tekniske oplysninger om overvågningsmetoden eller garantier for, hvordan de indhentede oplysninger vil blive anvendt og formidlet. Se PCLOB, Sec. 215 Report, s. 177.

⁽¹³⁶⁾ United States Code, afsnit 50, paragraf 1804(a), 1801 (g).

⁽¹³⁷⁾ FISC kan godkende anmodningen om yderligere oplysninger, afgøre, om det er nødvendigt at gennemføre en høring eller eventuelt angive, at anmodningen muligvis vil blive afslået. Regeringen vil udarbejde sin endelige anmodning på baggrund af denne foreløbige vurdering. Den endelige anmodning kan indeholde væsentlige ændringer af den oprindelige anmodning foretaget på grundlag af dommerens foreløbige bemærkninger. Selv om FISC godkender en stor procentdel af de endelige anmodninger, indeholder en betydelig del af disse væsentlige ændringer af den oprindelige anmodning, f.eks. 24 % af anmodningerne godkendt i perioden juli til september 2013. Se PCLOB, Sec. 215 Report, s. 179. Walton-brevet, s. 3.

⁽¹³⁸⁾ PCLOB, Sec. 215 Report, s.179, nr. 619.

⁽¹³⁹⁾ United States Code, afsnit 50, paragraf 1803 (i)(1),(3)(A). Denne nye lovgivning gennemførte PCLOB's anbefalinger om at etablere en pulje af eksperter inden for beskyttelse af privatlivets fred og borgerlige rettigheder, som kan optræde som amicus curiae, med det formål at give domstolen retlige argumenter til fremme af privatlivets fred og borgerlige rettigheder. Se PCLOB, Sec. 215 Report, s. 183-187.

⁽¹⁴⁰⁾ United States Code, afsnit 50, paragraf 1803 (i)(2)(A). Ifølge ODNI er sådanne udnævnelser allerede sket. Se Signals Intelligence Reform, 2016 Progress Report.

⁽¹⁴¹⁾ United States Code, afsnit 50, paragraf 1803 (i)(2)(B).

- (107) Med hensyn til de to lovbestemte tilladelser til at foretage overvågning i henhold til FISA, der har størst betydning for dataoverførsler under EU's og USA's værn om privatlivets fred, er FISC's tilsyn forskelligt.

- (108) I henhold til afsnit 501 i FISA ⁽¹⁴²⁾, der tillader indsamlingen af konkrete ting — »tangible things» — (herunder bøger, optegnelser, papirer, dokumenter og andre oplysninger), skal anmodningen til FISC indeholde en redegørelse for sagens kendsgerninger, der viser, at der er rimelige grunde til at antage, at de konkrete ting, der ønskes indsamlet, er relevante for en godkendt undersøgelse (ikke en trusselsvurdering) med henblik på indsamling af udenlandske efterretninger om ikke-amerikanske personer eller beskyttelse mod international terrorisme eller hemmelige efterretningsaktiviteter. Anmodningen skal desuden indeholde oplysninger om de minimeringsprocedurer, som den amerikanske justitsminister har indført for opbevaring og formidling af de indsamlede efterretninger. ⁽¹⁴³⁾

- (109) I henhold til afsnit 702 i FISA ⁽¹⁴⁴⁾ tillader FISC derimod ikke individuelle overvågningsforanstaltninger, men overvågningsprogrammer (f.eks. Prism, Upstream) på grundlag af årlige certificeringer udformet af den amerikanske justitsminister og direktøren for National Intelligence. I henhold til afsnit 702 i FISA kan der foretages en målrettet overvågning af personer, som med rimelighed kan antages at befinde sig uden for USA, med henblik på indsamling af efterretningsoplysninger ⁽¹⁴⁵⁾. NSA foretager denne målrettede overvågning i to trin: NSA-analytikere vil først identificere ikke-amerikanske personer uden for USA, hvor en overvågning ifølge analytikernes vurdering vil resultere i indsamling af relevante udenlandske efterretningsoplysninger som præciseret i certificeringen. Når disse individualiserede personer er blevet identificeret og den målrettede overvågning godkendt på grundlag af en omfattende evalueringsmekanisme i NSA ⁽¹⁴⁶⁾, vil de selektorer, der identificerer de kommunikationsfaciliteter (f.eks. e-mailadresser), som anvendes af målne, derefter blive udvalgt (dvs. udviklet og anvendt) ⁽¹⁴⁷⁾. Som anført indeholder de certificeringer, der skal godkendes af FISC, ingen oplysninger om de enkelte personer, der skal overvåges, men identificerer derimod kategorier af udenlandske efterretningsoplysninger ⁽¹⁴⁸⁾. Selv om FISC — på grundlag af en begrundet mistanke eller enhver anden standard — vurderer, at fysiske personer ikke er velegnede mål for indsamling af udenlandske efterretningsoplysninger ⁽¹⁴⁹⁾, kan der stadig indsamles oplysninger, såfremt »et væsentligt formål med indsamlingen er at indhente udenlandske efterretningsoplysninger» ⁽¹⁵⁰⁾. I henhold til afsnit 702 i FISA kan NSA kun indsamle kommunikation fra ikke-amerikanske personer uden for USA, hvis det med rimelighed kan antages, at et bestemt kommunikationsmiddel anvendes til at kommunikere udenlandske efterretningsoplysninger (f.eks. vedrørende international terrorisme, nuklear spredning eller fjendtlige cyberaktiviteter). Sådanne afgørelser er omfattet af domstolsprøvelse ⁽¹⁵¹⁾. Certificeringer skal ligeledes omfatte målretnings- og minimeringsprocedurer ⁽¹⁵²⁾. Den amerikanske justitsminister og direktøren for National Intelligence kontrollerer overholdelsen, og agenturerne skal indberette

⁽¹⁴²⁾ United States Code, afsnit 50, paragraf 1861.

⁽¹⁴³⁾ United States Code, afsnit 50, paragraf 1861(b).

⁽¹⁴⁴⁾ United States Code, afsnit 50, paragraf 1881.

⁽¹⁴⁵⁾ United States Code, afsnit 50, paragraf 1881a (a).

⁽¹⁴⁶⁾ PCLOB, Sec. 702 Report, s. 46.

⁽¹⁴⁷⁾ United States Code, afsnit 50, paragraf 1881a (h).

⁽¹⁴⁸⁾ United States Code, afsnit 50, paragraf 1881a (g). Ifølge PCLOB har disse kategorier indtil videre primært vedrørt international terrorisme og spørgsmål såsom erhvervelse af masseødelæggelsesvåben. Se PCLOB, Sec. 702 Report, s. 25.

⁽¹⁴⁹⁾ PCLOB, Sec. 702 Report, s. 27.

⁽¹⁵⁰⁾ United States Code, afsnit 50, paragraf 1881a.

⁽¹⁵¹⁾ »Liberty and Security in a Changing World«, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12.12.2013, s. 152.

⁽¹⁵²⁾ United States Code, afsnit 50, paragraf 1881a (i).

eventuelle tilfælde af manglende overholdelse til FISC ⁽¹⁵³⁾ (samt til den amerikanske kongres og President's Intelligence Oversight Board), som kan ændre tilladelsen på dette grundlag ⁽¹⁵⁴⁾.

- (110) For at øge effektiviteten af FISC's tilsyn har den amerikanske administration desuden indvilliget i at følge en anbefaling fra PCLOB om at fremsende dokumentation for afsnit 702-afgørelser om målrettet overvågning til FISC, herunder en stikprøve af overvågningsmål, således at FISC kan vurdere, hvordan kravet om et udenlandsk efterretningsformål opfyldes i praksis ⁽¹⁵⁵⁾. Den amerikanske administration har samtidig accepteret og truffet foranstaltninger til at revidere NSA's målretningsprocedurer, således at agenturet nemmere kan dokumentere de udenlandske efterretningsformål, der ligger bag afgørelser om målrettet overvågning ⁽¹⁵⁶⁾.

Individuel klageadgang

- (111) I henhold til amerikansk ret har registrerede i EU en række klagemuligheder, hvis de er usikre på, om deres personoplysninger er blevet behandlet (indsamlet, vurderet osv.) af amerikanske efterretningsenheder, og i så fald om de gældende begrænsninger i amerikansk ret er blevet overholdt. Disse vedrører navnligt tre områder: indgreb i henhold til FISA, embedsmænds ulovlige, forsætlige adgang til personoplysninger og indsigt i oplysninger i henhold til den amerikanske offentlighedslov, Freedom of Information Act (FOIA) ⁽¹⁵⁷⁾.
- (112) Foreign Intelligence Surveillance Act indeholder for det første en række retsmidler, der kan anvendes til at klage over ulovlig elektronisk overvågning, og som ligeledes kan anvendes af ikke-amerikanske personer ⁽¹⁵⁸⁾. Dette omfatter fysiske personers mulighed for at anlægge private søgsmål for økonomisk erstatning mod USA, når den pågældendes personoplysninger ulovligt og forsætligt er blevet anvendt eller videregivet ⁽¹⁵⁹⁾, muligheden for at sagsøge embedsmænd personligt («i lovens navn») for økonomisk erstatning ⁽¹⁶⁰⁾, og muligheden for at gøre indsigelse mod overvågningens lovlighed (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 ⁽¹⁶¹⁾.
- (113) Den amerikanske regering har for det andet oplyst Kommissionen om en række yderligere muligheder, som registrerede i EU kan anvende til at sagsøge embedsmænd for ulovlig statslig adgang til eller brug af

⁽¹⁵³⁾ I henhold til regel 13(b) i FISC's procedureregler skal regeringen straks efter konstateringen af, at en tilladelse eller godkendelse givet af domstolen er blevet gennemført i strid med domstolens tilladelse eller godkendelse og med gældende ret, skriftligt underrette domstolen herom. Regeringen skal ligeledes skriftligt underrette domstolen om de faktiske forhold og omstændigheder, der er relevante for denne manglende overholdelse. Regeringen vil typisk indsende en endelig skriftlig meddelelse i henhold til regel 13, a), når den får klarhed over de relevante kendsgerninger og den uautoriserede indsamling er blevet destrueret. Se Walton-brevet, s. 10.

⁽¹⁵⁴⁾ United States Code, afsnit 50, paragraf 1881 (l). Se også PCLOB, Sec. 702 Report, s. 66-76. NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act, Sec. 702, 16.4.2014. Indsamlingen af personoplysninger til efterretningsformål i henhold til Sec. 702 i FISA er underlagt internt og eksternt tilsyn fra den udøvende magts side. Det interne tilsyn omfatter bl.a. interne overholdelsesprogrammer, der anvendes til at evaluere og føre tilsyn med overholdelsen af målretnings- og minimeringsprocedurer, rapportering af tilfælde af manglende overholdelse både internt og eksternt til ODNI, justitsministeriet, den amerikanske kongres og FISC og fremsendelse af årlige evalueringer til disse organer. Det eksterne tilsyn består primært af kontrol af målretnings- og minimeringsprocedurer, der foretages af ODNI, justitsministeriet og generalinspektørerne, som herefter aflægger rapport til den amerikanske kongres og FISC, herunder om tilfælde af manglende overholdelse. Alvorlige tilfælde af manglende overholdelse skal straks indberettes til FISC, mens andre tilfælde indberettes i kvartalsrapporter. Se PCLOB, Sec. 702 Report, s. 66-77.

⁽¹⁵⁵⁾ PCLOB, Recommendations Assessment Report, 29.1.2015, s. 20.

⁽¹⁵⁶⁾ PCLOB, Recommendations Assessment Report, 29.1.2015, s. 16.

⁽¹⁵⁷⁾ Ifølge Sec. 10 i Classified Information Procedures Act skal den amerikanske regering i forbindelse med enhver retsforfølgning, hvor den amerikanske regering skal dokumentere, at materiale udgør klassificerede informationer (f.eks. fordi det skal beskyttes mod uautoriseret videregivelse af nationale sikkerhedshensyn), desuden underrette sagsøgte om, hvilke dele af materialet, som den amerikanske regering med rimelighed forventer at anvende til at dokumentere de klassificerede informationer, som lovovertrædelsen omfatter.

⁽¹⁵⁸⁾ For det følgende se ODNI's udredninger (bilag VI), s. 16.

⁽¹⁵⁹⁾ United States Code, afsnit 18, paragraf 2712.

⁽¹⁶⁰⁾ United States Code, afsnit 50, paragraf 1810.

⁽¹⁶¹⁾ United States Code, afsnit 50, paragraf 1806.

personoplysninger, herunder til påståede nationale sikkerhedsformål (Computer Fraud Abuse Act ⁽¹⁶²⁾, Electronic Communications Privacy Act ⁽¹⁶³⁾, og Right to Financial Privacy Act ⁽¹⁶⁴⁾). Alle disse klagemuligheder vedrører specifikke oplysninger, mål og/eller typer af adgang (f.eks. fjernadgang via computer via internettet) og kan anvendes i visse tilfælde (f.eks. forsætlig adfærd, handlinger, der ligger uden for udførelsen af et hverv, lidt skade) ⁽¹⁶⁵⁾. En mere generel klageadgang findes i Administrative Procedure Act (United States Code, afsnit 5, paragraf 702), ifølge hvilken »enhver person, mod hvem der er begået juridisk uret på grund af et agenturs foranstaltninger, eller som er blevet krænkede eller forurettet herved« kan begære retslig prøvelse. Det omfatter muligheden for at anmode domstolen om at »erklære agenturets foranstaltninger, konstateringer og konklusioner for ulovlige og annullere dem, hvis de er vilkårlige, ustadige eller udtryk for magtmisbrug eller på anden vis ikke i overensstemmelse med loven« ⁽¹⁶⁶⁾.

- (114) Den amerikanske regering har endelig understreget, at ikke-amerikanske personer kan henholde sig til FOIA som et middel til at søge indsigt i de amerikanske forbundsorganers eksisterende optegnelser, herunder om de pågældendes personoplysninger ⁽¹⁶⁷⁾. I lyset af FOIA's anvendelsesområde giver loven ikke den enkelte mulighed for at gøre indsigelse mod indgreb i personoplysninger som sådan, selv om den i princippet giver dem mulighed for at få adgang til relevante oplysninger, der opbevares af nationale efterretningsagenturer. Selv på dette område er mulighederne tilsyneladende begrænsede, da 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 ⁽¹⁶⁸⁾. Når dette er sagt, kan nationale efterretningsagenturers anvendelse af disse undtagelser påklages af den registrerede, som både kan anmode om administrativ og retlig prøvelse.
- (115) Selv om personer, herunder registrerede i EU, således har en række klagemuligheder, når de har været genstand for ulovlig (elektronisk) overvågning af hensyn til den nationale sikkerhed, står det ligeledes klart, at i hvert fald nogle af de retsgrundlag, som de amerikanske efterretningsmyndigheder kan anvende (f.eks. E.O. 12333), ikke er omfattet. Selv når ikke-amerikanske personer i princippet har klageadgang, f.eks. i forbindelse med overvågning i henhold til FISA, er de tilgængelige klagemuligheder desuden begrænsede ⁽¹⁶⁹⁾, og søgsmål fra registrerede (herunder amerikanere) vil blive afvist, hvis de ikke kan dokumentere deres søgsmålskompetence (»standing« ⁽¹⁷⁰⁾), hvilket begrænser adgangen til almindelige domstole ⁽¹⁷¹⁾.
- (116) For at give alle registrerede i EU en yderligere klagemulighed har den amerikanske regering besluttet at oprette en ny mekanisme, ombudsmanden i værnet om privatlivets fred, som anført i brevet fra den amerikanske udenrigsminister til Kommissionen, der er indeholdt i bilag III til denne afgørelse. Denne mekanisme er baseret på udpegningen i medfør af PPD-28 af en seniorkoordinator (på viceministerniveau) i det amerikanske udenrigsministerium som kontaktpunkt for udenlandske regeringer, der bl.a. kan rejse bekymringer over amerikanske signalefterretningsaktiviteter, men mekanismen er langt mere vidtrækkende end den oprindelige idé.

⁽¹⁶²⁾ United States Code, afsnit 18, paragraf 1030.

⁽¹⁶³⁾ United States Code, afsnit 18, paragraf 2701-2712.

⁽¹⁶⁴⁾ United States Code, afsnit 12, paragraf 3417.

⁽¹⁶⁵⁾ ODN's udredninger (bilag VI), s. 17.

⁽¹⁶⁶⁾ United States Code, afsnit 5, paragraf 706 (2)(A).

⁽¹⁶⁷⁾ United States Code, afsnit 5, paragraf 552. Der findes tilsvarende love på delstatsniveau.

⁽¹⁶⁸⁾ I dette tilfælde vil den pågældende normalt kun modtage et standardsvar, hvor agenturet afslår at bekræfte eller benægte, at der foreligger optegnelser. Se *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

⁽¹⁶⁹⁾ Se ODN's udredninger (bilag VI), s. 16. Ifølge det oplyste er de tilgængelige klagemuligheder betinget af, at der er lidt skade (United States Code, afsnit 18, paragraf 2712; United States Code, afsnit 50, paragraf 1810), eller dokumentation for, at regeringen agter at bruge eller videregive oplysninger indhentet ved eller udledt af elektronisk overvågning af den pågældende mod denne i forbindelse med retslige eller administrative procedurer i USA (United States Code, afsnit 50, paragraf 1806). Domstolen har imidlertid gentagne gange understreget, at det ved afgørelsen af, om der foreligger et indgreb i den grundlæggende ret til respekt for privatlivet, ikke har nogen betydning, om indgrebet har medført eventuelle ubehageligheder for den berørte. Se Schrems, præmis 89, med yderligere henvisninger.

⁽¹⁷⁰⁾ Dette kriterium for antagelighed er baseret på kravet om retstvist (»case or controversy«) i artikel III i den amerikanske forfatning.

⁽¹⁷¹⁾ Se *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). Med hensyn til anvendelsen af NSL skal krav om beskyttelse af oplysninger i henhold til USA FREEDOM Act (Sec. 502(f)-503) evalueres regelmæssigt, og modtagere af NSL'er skal underrettes, når et krav om beskyttelse af oplysninger ikke længere er begrundet i faktiske forhold (se ODN's udredninger (bilag VI), s. 13). Dette sikrer imidlertid ikke, at den registrerede i EU underrettes om, at den pågældende har været mål for en undersøgelse.

- (117) I henhold til tilsagnene fra den amerikanske regering vil ombudsmandsmekanismen sikre, at individuelle klager bliver ordentligt undersøgt, og at de enkelte modtager en uafhængig bekræftelse af, at den amerikanske lovgivning er blevet overholdt, eller at den manglende overholdelse er blevet afhjulpnet i tilfælde af en overtrædelse af lovgivningen ⁽¹⁷²⁾. Mekanismen omfatter »ombudsmanden i værnet om privatlivets fred«, dvs. viceministeren og yderligere personale såvel som tilsynsorganer, der er kompetente til at føre tilsyn med de forskellige dele af efterretningstjenesten, hvis samarbejde er nødvendigt for, at ombudsmanden i værnet om privatlivets fred kan håndtere klager. Navnlig i tilfælde, hvor en persons klage vedrører foreneligheden af overvågningen med amerikansk lovgivning, vil ombudsmanden i værnet om privatlivets fred kunne støtte sig til uafhængige tilsynsorganer med undersøgelsesbeføjelser (såsom generalinspektører eller PCLOB). I hvert enkelt tilfælde sørger den amerikanske udenrigsminister for, at ombudsmanden har midlerne til at sikre, at svaret på de individuelle anmodninger er baseret på alle de nødvendige oplysninger.
- (118) Ombudsmandsmekanismen garanterer via denne sammensatte struktur uafhængigt tilsyn og individuel klageadgang. Derudover sikrer samarbejdet med de øvrige tilsynsorganer adgang til den nødvendige ekspertise. Ved at pålægge ombudsmanden i værnet om privatlivets fred en forpligtelse til at bekræfte overholdelse eller afhjælpning af manglende overholdelse, afspejler mekanismen den amerikanske regerings generelle tilsagn om at behandle klager fra EU-borgere.
- (119) For det første vil ombudsmanden i værnet om privatlivets fred modtage og besvare individuelle klager, hvilket ikke er tilfældet for en ren mellemstatslig mekanisme. Disse klager kan fremsendes til de organer i medlemsstaterne, der fører tilsyn med nationale sikkerhedstjenester og/eller offentlige myndigheders behandling af personoplysninger, som vil fremsende dem til et centraliseret EU-organ, hvorfra de vil blive kanaliseret videre til ombudsmanden i værnet om privatlivets fred ⁽¹⁷³⁾. Dette vil rent faktisk være til fordel for fysiske personer i EU, der kan henvende sig til et nationalt organ tæt på og på deres eget sprog. Et sådant organ skal bistå den registrerede med udarbejdelsen af en anmodning til ombudsmanden i værnet om privatlivets fred, der indeholder de grundlæggende oplysninger og således kan betragtes som »fuldstændig«. Den enkelte skal ikke dokumentere, at den amerikanske regering rent faktisk har fået adgang til vedkommendes personoplysninger gennem signalefterretningsaktiviteter.
- (120) For det andet forpligter den amerikanske regering sig til at sikre, at ombudsmanden i værnet om privatlivets fred i udførelsen af sine opgaver vil kunne regne med et samarbejde med andre uafhængige organer for tilsyn med og kontrol af overholdelsen i amerikansk ret. Dette vil til tider involvere nationale efterretningsmyndigheder, navnlig i tilfælde hvor anmodningen kan tolkes som en anmodning om indsigt i dokumenter i henhold til Freedom of Information Act. I andre tilfælde, specielt hvor anmodningerne vedrører foreneligheden af overvågningen med amerikansk lovgivning, vil et sådant samarbejde involvere uafhængige tilsynsorganer (f.eks. generalinspektører) med ansvar for og bemyndigelse til at foretage en grundig undersøgelse (navnlig via adgang til alle relevante dokumenter og bemyndigelse til at anmode om oplysninger og udtalelser) og gribe ind over for manglende overholdelse ⁽¹⁷⁴⁾. Ombudsmanden i værnet om privatlivets fred kan ligeledes henvise sager til PCLOB ⁽¹⁷⁵⁾. Hvis en af disse tilsynsorganer konstaterer manglende overholdelse, skal den pågældende efterretningsenhed (f.eks. en efterretningstjeneste) afhjælpe den manglende overholdelse, eftersom ombudsmanden kun derved vil kunne give den enkelte person et »positivt« svar (dvs. at den manglende overholdelse er afhjulpnet), hvilket den amerikanske

⁽¹⁷²⁾ Hvis klageren søger indsigt i de amerikanske offentlige myndigheders dokumenter, finder reglerne og procedurerne i Freedom of Information Act anvendelse. Det omfatter muligheden for at søge retlig prøvelse (fremfor uafhængigt tilsyn) i tilfælde af, at sagen afvises, på de betingelser, der er fastsat i FOIA.

⁽¹⁷³⁾ I medfør af ombudsmandsmekanismen (bilag III), punkt 4, f), skal ombudsmanden i værnet om privatlivets fred kommunikere direkte med EU-klageinstansen for individuelle klager, som herefter skal varetage kommunikationen med den person, der indgiver anmodningen. Hvis direkte henvendelser er et led i de »underliggende processer«, der kan give den ønskede afhjælpning (f.eks. en anmodning om indsigt i henhold til FOIA, se punkt 5), vil disse henvendelser ske i overensstemmelse med gældende procedurer.

⁽¹⁷⁴⁾ Se ombudsmandsmekanismen (bilag III), punkt 2, a). Se også betragtning 0-0.

⁽¹⁷⁵⁾ Se ombudsmandsmekanismen (bilag III), punkt 2, c). Det anføres i den amerikanske regerings udredninger, at PCLOB løbende skal gennemgå de amerikanske terrorbekæmpelsesmyndigheders politikker og procedurer og gennemførelsen heraf med det formål at vurdere, om deres foranstaltninger »beskytter privatlivets fred og borgerlige rettigheder behørigt, og om de er i overensstemmelse med gældende love, bestemmelser og politikker til beskyttelse af privatlivets fred og borgerlige rettigheder«. PCLOB skal ligeledes »modtage og gennemgå rapporter og andre oplysninger fra de databeskyttelsesansvarlige og i påkommende tilfælde udstede anbefalinger til dem om deres aktiviteter«.

regering har forpligtet sig til. Som en del af samarbejdet vil ombudsmanden i værnet om privatlivets fred blive orienteret om undersøgelsens udfald, og ombudsmanden vil have midlerne til at sikre, at den modtager alle de oplysninger, der er nødvendige for at forberede sit svar.

- (121) Endelig er ombudsmanden i værnet om privatlivets fred uafhængig og modtager således ikke instrukser fra de amerikanske efterretningstjenester ⁽¹⁷⁶⁾. Dette er af væsentlig betydning, da ombudsmanden skal »bekræfte«, at i) klagen er blevet behørigt undersøgt, og at ii) den relevante amerikanske lovgivning — herunder navnlig de begrænsninger og garantier, der er anført i bilag VI — er blevet overholdt, eller at den manglende overholdelse er blevet afhjulpet i tilfælde af en overtrædelse. For at kunne give denne uafhængige bekræftelse skal ombudsmanden i værnet om privatlivets fred modtage de nødvendige oplysninger vedrørende undersøgelsen for at kunne vurdere nøjagtigheden af svaret til klageren. Derudover har den amerikanske udenrigsminister forpligtet sig til at sikre, at viceministeren vil udføre hvervet som ombudsmand i værnet om privatlivets fred på objektiv vis og fri for uhensigtsmæssig indflydelse, der vil kunne påvirke det svar, der skal gives.
- (122) Samlet set sikrer denne mekanisme, at individuelle klager bliver grundigt undersøgt og behandlet, og det i det mindste på tilsynsområdet vil involvere tilsynsorganer med den nødvendige ekspertise og undersøgelsesbeføjelser og en ombudsmand, som er i stand til at varetage sine opgaver fri for uretmæssig, navnlig politisk, indflydelse. Derudover vil de registrerede kunne indgive klager uden at skulle bevise eller blot forelægge tegn på, at de er blevet overvåget ⁽¹⁷⁷⁾. Kommissionen finder det på baggrund af disse elementer godtgjort, at der er tale om tilstrækkeligt og effektive garantier mod misbrug.
- (123) Kommissionen konkluderer på baggrund af ovenstående, at USA sikrer en effektiv retsbeskyttelse mod de amerikanske efterretningsmyndigheders indgreb i de grundlæggende rettigheder for de personer, hvis oplysninger overføres fra EU til USA under EU's og USA's værn om privatlivets fred.
- (124) Kommissionen noterer sig i den forbindelse Domstolens dom i Schrems-sagen, ifølge hvilken »lovgivning, der ikke fastsætter nogen mulighed for retssubjektet til at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet, [opfylder] ikke det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som denne er sikret ved chartrets artikel 47« ⁽¹⁷⁸⁾. Kommissionens vurdering har bekræftet, at der findes sådanne afhjælpende foranstaltninger i USA, herunder via indførelsen af ombudsmandsmekanismen. Ombudsmandsmekanismen omfatter uafhængigt tilsyn og undersøgelsesbeføjelser. Mekanismens effektivitet vil blive revurderet inden for rammerne af Kommissionens fortsatte overvågning af værnet om privatlivets fred, herunder gennem den årlige fælles evaluering, som også vil involvere ombudsmanden.

3.2. De amerikanske offentlige myndigheders adgang til og brug af personoplysninger med henblik på retshåndhævelse og andre offentlige interesser

- (125) Med hensyn til indgreb i personoplysninger overført under EU's og USA's værn om privatlivets fred med henblik på retshåndhævelse har den amerikanske regering (gennem det amerikanske justitsministerium) givet sikkerhed for de gældende begrænsninger og garantier, som efter Kommissionens opfattelse dokumenterer, at beskyttelsesniveauet er tilstrækkeligt.

⁽¹⁷⁶⁾ Se *Roman Zakharov v. Russia*, dom af 4.12.2015 (Store Afdeling), begæring nr. 47143/06, præmis 275 (»selv om det i princippet er ønskeligt at betro en dommer den tilsynsmæssige kontrol, kan ikke-retslige organers tilsyn betragtes som forenelig med konventionen under forudsætning af, at tilsynsorganet er uafhængig af de myndigheder, der foretager kontrollen, og at det har de fornødne, effektive tilsynsbeføjelser«).

⁽¹⁷⁷⁾ Se *Kennedy v. the United Kingdom*, dom af 18.5.2010, begæring nr. 26839/05, præmis 167.

⁽¹⁷⁸⁾ *Schrems*, præmis 95. Som det klart fremgår af dommens præmis 91 og 96 vedrører præmis 95 det beskyttelsesniveau, der er sikret i Unionens retsorden, og som tredjelandets beskyttelsesniveau »i det væsentlige« skal svare til. Ifølge dommens præmis 73 og 74 indebærer dette ikke, at det kan kræves, at et tredjeland sikrer et beskyttelsesniveau, som er identisk med EU's niveau, om end de midler, der anvendes, i praksis skal vise sig at være effektive.

- (126) Ifølge disse oplysninger skal de retshåndhævende myndigheder i henhold til fjerde amendment i den amerikanske forfatning ⁽¹⁷⁹⁾ først og fremmest have en dommerkendelse ⁽¹⁸⁰⁾, der afgives på grundlag af dokumentation for begrundet mistanke (»probable cause«), inden ransagning og beslaglæggelse. I de få specifikke særlige tilfælde, hvor der ikke skal foreligge en kendelse ⁽¹⁸¹⁾, er retshåndhævelsen betinget af en »rimelighedstest« ⁽¹⁸²⁾. Rimeligheden af en ransagning eller beslaglæggelse »vurderes ved på den ene side at vurdere, i hvilken grad den griber ind i en persons privatliv, og på den anden side vurdere, i hvilket omfang der er behov herfor for at fremme legitime regeringsinteresser« ⁽¹⁸³⁾. Fjerde amendment garanterer mere generelt privatlivets fred og den enkeltes værdighed og beskytter mod myndighedernes vilkårlige og invasive foranstaltninger ⁽¹⁸⁴⁾. Disse begreber afspejler principperne om nødvendighed og proportionalitet i EU-retten. Når de retshåndhævende myndigheder ikke længere har brug for de beslaglagte genstande som bevis, skal disse tilbagegives ⁽¹⁸⁵⁾.
- (127) Om end det fjerde amendment ikke omfatter ikke-amerikanske personer bosiddende uden for USA, er disse ikke desto mindre indirekte beskyttet heraf, under forudsætning af at det er amerikanske foretagender, der ligger inde med personoplysningerne, hvilket betyder, at de retshåndhævende myndigheder under alle omstændigheder skal anmode om en retskendelse (eller i det mindste opfylde kravet om rimelighed) ⁽¹⁸⁶⁾. Der ydes yderligere beskyttelse i særlige lovbestemmelser og i det amerikanske justitsministeriums retningslinjer, som begrænser de retshåndhævende myndigheders adgang til data, der opfylder princippet om nødvendighed og proportionalitet (f. eks. ved at kræve, at FBI anvender de mindst indgribende efterforskningsmetoder under hensyntagen til indvirkningen på privatlivets fred og borgerlige rettigheder) ⁽¹⁸⁷⁾. Ifølge den amerikanske regerings udredninger er der det samme eller et højere beskyttelsesniveau i forbindelse med retshåndhævende efterforskninger på delstatsniveau (efterforskninger omfattet af delstatslove) ⁽¹⁸⁸⁾.
- (128) Selv om en forudgående retskendelse afsagt af en domstol eller en grand jury (domstolens efterforskningsgren udpeget af en dommer) ikke er påkrævet i alle tilfælde ⁽¹⁸⁹⁾, er administrative pålæg (administrative subpoenas) begrænset til særlige sager, og de vil blive underlagt uafhængig domstolsprøvelse, i hvert fald når regeringen anmoder om at få håndhævet pålægget ved domstolene ⁽¹⁹⁰⁾.

⁽¹⁷⁹⁾ Fjerde amendment fastslår at, »folkets ret til sikkerhed for deres personer, boliger, papirer og ejendele imod urimelige ransagninger og anholdelser må ikke krænkes, og ingen kendelse herom må afsiges uden en sandsynlig årsag, der støtter sig til ed eller højtidelig erklæring og nøje beskriver det sted, der skal ransages, de personer, der skal arresteres, eller de ting, der skal beslaglægges«. Kun dommere kan udstede sådanne kendelser. Forbundskenndelser vedrørende kopiering af elektronisk lagrede oplysninger er reguleret af regel nr. 41 i Federal Rules of Criminal Procedure.

⁽¹⁸⁰⁾ Den amerikanske højesteret har gentagne gange henvist til ransagninger uden kendelse som »undtagelser«. Se f.eks. *Johnson v. United States*, 333 U.S. 10, 14 (1948), *McDonald v. United States*, 335 U.S. 451, 453 (1948), *Camara v. Municipal Court*, 387 U.S. 523, 528-29 (1967), *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352-53, 355 (1977). Den amerikanske højesteret har ligeledes jævnligt understreget, at »den mest grundlæggende forfatningsregel på området er, at ransagninger foretaget uden retslig proces og uden en dommers forudgående godkendelse, i sig selv er urimelige i henhold til fjerde amendment, med undtagelse af ganske få specifikke og velafgrænsede tilfælde«. Se f.eks. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971), *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352-53, 358 (1977).

⁽¹⁸¹⁾ *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

⁽¹⁸²⁾ PCLOB, Sec. 215 Report, s. 107, hvor der henvises til *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).

⁽¹⁸³⁾ PCLOB, Sec. 215 Report, s. 107, hvor der henvises til *Samson v. California*, 547 U.S. 843, 848 (2006).

⁽¹⁸⁴⁾ *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

⁽¹⁸⁵⁾ Se f.eks. *United States v. Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).

⁽¹⁸⁶⁾ Jf. *Roman Zakharov v. Russia*, dom af 4.12.2015 (Store Afdeling), begæring nr. 47143/06, præmis 269, ifølge hvilket »kravet om, at der for udbyderen af den elektroniske kommunikationstjeneste skal forevises en opfangningstilladelse, før der kan opnås adgang til en persons kommunikation, er en af de vigtigste beskyttelsesforanstaltninger mod retshåndhævende myndigheders misbrug, og sikrer, at der skaffes de rigtige tilladelser i alle sager om opfangning.«

⁽¹⁸⁷⁾ Det amerikanske justitsministeriums udredninger (bilag VII), s. 4, med yderligere henvisninger.

⁽¹⁸⁸⁾ Det amerikanske justitsministeriums udredninger (bilag VII), s. 2.

⁽¹⁸⁹⁾ Ifølge de oplysninger, som Kommissionen har modtaget — hvis der ses bort fra specifikke områder, der sandsynligvis ikke vil være relevante for dataoverførsler under EU's og USA's værn om privatlivets fred (f.eks. undersøgelser af sager om misbrug af sundhedsydelser, børnemishandling eller kontrollerede stoffer) — vedrører dette primært visse myndigheder omfattet af Electronic Communications Privacy Act (ECPA), nemlig anmodninger om abonnentoplysninger (United States Code, afsnit 18, paragraf 2703(c) (1)) og om indholdet af e-mail, der er ældre end 180 dage (United States Code, afsnit 18, paragraf 2703(b)). I sidstnævnte tilfælde skal den pågældende person imidlertid underrettes og har således mulighed for at anfægte anmodningen ved domstolene. Se ligeledes det amerikanske justitsministerium, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, kapitel 3: The Stored Communications Act, s. 115-138.

⁽¹⁹⁰⁾ Ifølge den amerikanske regerings udredninger kan modtagere af administrative pålæg anfægte dem ved domstolene med den begrundelse, at de er urimelige, dvs. overdrevne, undertrykkende eller byrdefulde. Se det amerikanske justitsministeriums udredninger (bilag VII), s. 2.

- (129) Det samme gælder for anvendelsen af administrative pålæg med henblik på beskyttelse af offentlige interesser. Ifølge den amerikanske regerings udredninger finder tilsvarende materielle begrænsninger anvendelse, da organer kun kan søge indsigt i oplysninger, der er relevante for anliggender omfattet af deres kompetence, og de skal respektere kravet om rimelighed.
- (130) 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. Disse muligheder, der navnlig er fastsat i Administrative Procedure Act (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.
- (131) I bestemmelserne om adgang til retlig prøvelse i Administrative Procedure Act ⁽¹⁹¹⁾ slås det fast, at »enhver person, mod hvem der er begået juridisk uret på grund af et agenturs foranstaltninger, eller som er blevet krænkede eller forurettet herved« kan begære retlig prøvelse ⁽¹⁹²⁾. Det omfatter muligheden for at anmode domstolen om at »erklære agenturets foranstaltninger, konstateringer og konklusioner for ulovlige og annullere dem, hvis de er vilkårlige, ustadige eller udtryk for magtmisbrug eller på anden vis ikke i overensstemmelse med loven« ⁽¹⁹³⁾.
- (132) Mere specifikt fastsættes der i afsnit II i Electronic Communications Privacy Act ⁽¹⁹⁴⁾ en række lovbestemte rettigheder, der regulerer retshåndhævende myndigheders adgang til indholdet af trådbåren, mundtlig eller elektronisk kommunikation, der lagres af tredjepartsudbydere ⁽¹⁹⁵⁾. Herved kriminaliseres den ulovlige adgang (dvs. den adgang, der ikke er godkendt af en domstol eller i øvrigt er tilladt) til sådan kommunikation, og den pågældende person får mulighed for at anlægge et civilt 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.
- (133) Ifølge Freedom of Information Act (FOIA, U.S.C., afsnit 5, paragraf 552) har enhver person desuden ret til indsigt i de amerikanske forbundsorganers optegnelser og, når de administrative klagemuligheder er udtømt, til at håndhæve denne ret ved domstolene, medmindre sådanne optegnelser pga. en fritagelse eller en særlig retshåndhævelsesundtagelse er beskyttet mod offentliggørelse ⁽¹⁹⁶⁾.

⁽¹⁹¹⁾ United States Code, afsnit 5, paragraf 702.

⁽¹⁹²⁾ Generelt er det kun agenturets »endelige« — og ikke »foreløbige, proceduremæssige eller mellemliggende« — foranstaltninger, der er genstand for retslig prøvelse. Jf. United States Code, afsnit 5, paragraf 704.

⁽¹⁹³⁾ United States Code, afsnit 5, paragraf 706 (2)(A).

⁽¹⁹⁴⁾ United States Code, afsnit 18, paragraf 2701-2712.

⁽¹⁹⁵⁾ ECPA beskytter kommunikationer, 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.

⁽¹⁹⁶⁾ Disse undtagelser er dog begrænsede. F.eks. er rettigheder i henhold til FOIA i følge United States Code, afsnit 5, paragraf 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 i forbindelse med en strafferetlig efterforskning eller 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.« (United States Code, afsnit 5, paragraf 552 (c)(1)).

- (134) Derudover giver adskillige andre bestemmelser den registrerede ret til at anlægge sag mod en amerikansk offentlig myndighed eller offentligt ansat for behandling af deres personoplysninger, herunder Wiretap Act ⁽¹⁹⁷⁾, Computer Fraud and Abuse Act ⁽¹⁹⁸⁾, Federal Torts Claim Act ⁽¹⁹⁹⁾, Right to Financial Privacy Act ⁽²⁰⁰⁾ og Fair Credit Reporting Act ⁽²⁰¹⁾.
- (135) Kommissionen konkluderer derfor, at USA har indført regler, hvorved det tilsigtes at begrænse de eventuelle indgreb med henblik på retshåndhævelse ⁽²⁰²⁾ og andre offentlige interesser i de grundlæggende rettigheder for de personer, hvis oplysninger overføres fra EU til USA under EU's og USA's værn om privatlivets fred, til det strengt nødvendige med henblik på at nå det tilsigtede mål, og at dette sikrer en effektiv retsbeskyttelse mod sådanne indgreb.

4. TILSTRÆKKELIGT BESKYTTELSESNIVEAU I EU'S OG USA'S VÆRN OM PRIVATLIVETS FRED

- (136) Kommissionen mener på baggrund af disse konklusioner, at USA sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til foretagender i USA under EU's og USA's værn om privatlivets fred.
- (137) Kommissionen finder navnlig, at de principper, som det amerikanske handelsministerium har opstillet, i deres helhed sikrer et niveau af beskyttelse af personoplysninger, der i det væsentlige svarer til det niveau, der er garanteret ved de grundlæggende principper i direktiv 95/46/EF.
- (138) Den effektive anvendelse af principperne er desuden garanteret ved gennemsigtighedskrav og handelsministeriets forvaltning af værnet om privatlivets fred.
- (139) Kommissionen mener desuden, at mekanismerne for tilsyn og klageadgang i værnet om privatlivets fred gør det muligt at identificere overtrædelser af principperne begået af foretagender i værnet om privatlivets fred og straffe disse i praksis og sikre registrerede retsmidler med henblik på at få adgang til personoplysninger, som vedrører de pågældende, eller til at få sådanne oplysninger berigtiget eller slettet.
- (140) På baggrund af de tilgængelige oplysninger om den amerikanske retsorden, herunder udredningerne og tilsagnene fra den amerikanske regering og begrænsningerne pålagt selvcertificerede foretagender i forbindelse med deres tilslutning til principperne, mener Kommissionen endelig, at eventuelle indgreb fra de amerikanske offentlige myndigheders side i de grundlæggende rettigheder for de personer, hvis oplysninger overføres fra EU til USA under EU's og USA's værn om privatlivets fred med henblik på beskyttelse af den nationale sikkerhed, retshåndhævelse og andre offentlige interesser, vil blive begrænset til det strengt nødvendige med henblik på at nå det tilsigtede legitime mål, og at der er en effektiv retsbeskyttelse mod sådanne indgreb.

⁽¹⁹⁷⁾ United States Code, afsnit 18, paragraf 2510 ff. Ifølge Wiretap Act (United States Code, afsnit 18, paragraf 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 adresseringsoplysninger og andre ikke-indholdsmæssige oplysninger (f.eks. IP-adresse, afsender- og modtager e-mailadresse) se også kapitler om Pen Registers og Trap and Trace Devices i afsnit 18 (United States Code, afsnit 18, paragraf 3121-3127 og vedrørende private søgsmål paragraf 2707).

⁽¹⁹⁸⁾ United States Code, afsnit 18, paragraf 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 finansiel institution, den amerikanske regerings computersystemer eller en anden specificeret computer, herunder, under visse omstændigheder, mod en individuel embedsmand.

⁽¹⁹⁹⁾ United States Code, afsnit 28, paragraf 2671 ff. 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.«

⁽²⁰⁰⁾ United States Code, afsnit 12, paragraf 3401 ff. 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 lovovertredelse. Statslig adgang til beskyttede finansielle oplysninger er generelt forbudt, mindre 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 søges, underrettes om.

⁽²⁰¹⁾ United States Code, afsnit 15, paragraf 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 forbruger-kreditrapporter eller, under visse omstændigheder, mod en offentlig myndighed.

⁽²⁰²⁾ Domstolen har slået fast, at retshåndhævelse udgør et legitimt politisk mål. Se de forenede sager C-293/12 og C-594/12, Digital Rights Ireland m.fl., EU:C:2014:238, præmis 42. Se ligeledes artikel 8, stk. 2, i den europæiske menneskerettighedskonvention og Menneskerettighedsdomstolens dom i *Weber and Saravia v. Germany*, begæring nr. 54934/00, præmis 104.

- (141) Kommissionen konkluderer, at dette opfylder kravene i artikel 25 i direktiv 95/46/EF sammenholdt med EU's Charter om grundlæggende rettigheder som anført af Domstolen, navnlig i Schrems-dommen.

5. DATABESKYTTELSESMYNDIGHEDERNES FORANSTALTNINGER OG OPLYSNINGER TIL KOMMISSIONEN

- (142) I Schrems-dommen præciserede Domstolen, at Kommissionen ikke har kompetence til at begrænse databeskyttelsesmyndighedernes beføjelser i medfør af artikel 28 i direktiv 95/46/EF (herunder beføjelsen til at suspendere dataoverførsler) i det tilfælde, hvor en person i forbindelse med en anmodning i henhold til denne bestemmelse rejser tvivl om, hvorvidt en afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet er forenelig med beskyttelsen af den grundlæggende ret til privatliv og databeskyttelse ⁽²⁰³⁾.
- (143) For at sikre en effektiv overvågning af, hvordan alle dele af værnet om privatlivets fred fungerer, skal medlemsstaterne informere Kommissionen om relevante foranstaltningerne truffet af databeskyttelsesmyndighederne.
- (144) Domstolen fastslog endvidere, at medlemsstaterne og deres organer i medfør af artikel 25, stk. 6, andet afsnit, i direktiv 95/46/EF skal træffe de nødvendige foranstaltninger for at overholde EU-institutionernes retsakter, da der i princippet gælder en formodning om, at disse retsakter er lovlige, og de afføder derfor retsvirkninger, så længe de ikke er blevet trukket tilbage, annulleret under et annullationssøgsmål eller erklæret ugyldige som følge af en præjudiciel forelæggelse eller en ulovlighedsindsigelse. En afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet i medfør af artikel 25, stk. 6, i direktiv 95/46/EF er således bindende for alle de organer i medlemsstaterne, som den er rettet til, herunder deres uafhængige tilsynsmyndigheder ⁽²⁰⁴⁾. Hvis en sådan myndighed har modtaget en klage, der rejser tvivl om, hvorvidt en afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet er forenelig med beskyttelsen af den grundlæggende ret til privatliv og databeskyttelse, og myndigheden finder, at klagepunkterne er velbegrundede, skal der i national ret indføres retsmidler, der gør det muligt for myndigheden at gøre klagepunkterne gældende for en national domstol, der er forpligtet til at udsætte sagen og forelægge Domstolen et præjudicielt spørgsmål ⁽²⁰⁵⁾.

6. REGELMÆSSIG EVALUERING AF KONSTATERINGEN AF ET TILSTRÆKKELIGT BESKYTTELSESLEVELAU

- (145) Henset til den omstændighed, at det beskyttelsesniveau, som den amerikanske retsorden sikrer, kan ændre sig, vil Kommissionen efter vedtagelse af denne afgørelse med regelmæssige mellemrum undersøge, om konstateringen af et tilstrækkeligt beskyttelsesniveau, som er sikret af USA under EU's og USA's værn om privatlivets fred, stadig er faktisk og retligt begrundet. En sådan undersøgelse skal under alle omstændigheder foretages, når Kommissionen modtager oplysninger, der rejser begrundet tvivl i denne henseende ⁽²⁰⁶⁾.
- (146) Kommissionen vil derfor løbende overvåge den overordnede ramme for overførsel af personoplysninger under EU's og USA's værn om privatlivets fred samt de amerikanske myndigheders overholdelse af de udredninger og tilsagn, der er anført i dokumenterne knyttet til denne afgørelse. For at fremme denne proces har USA forpligtet sig til at underrette Kommissionen om væsentlige ændringer af amerikansk ret, der er relevante for værnet om privatlivets fred, og som vedrører databeskyttelse og begrænsninger og garantier gældende for offentlige myndigheds adgang til personoplysninger. Denne afgørelse vil desuden blive underlagt en årlig fælles evaluering af alle aspekter af EU's og USA's værn om privatlivets fred, herunder af foreneligheden af de nationale sikkerheds- og retshåndhævelsesundtagelser med principperne. Eftersom konstateringen af et tilstrækkeligt beskyttelsesniveau kan påvirkes af udviklingen af EU-retten, vil Kommissionen desuden vurdere det beskyttelsesniveau, som værnet om privatlivets fred giver, når den generelle forordning om databeskyttelse begynder at finde anvendelse.
- (147) Med henblik på den årlige fælles evaluering, der henvises til i bilag I, II og VI, vil Kommissionen mødes med det amerikanske handelsministerium og FTC, i påkommende tilfælde ledsaget af repræsentanter fra andre ministerier og agenturer involveret i gennemførelsen af ordningen for værnet om privatlivets fred, og i forbindelse med nationale sikkerhedsanliggender med repræsentanter fra ODNI, andre efterretningsenheder og ombudsmanden. Repræsentanter fra EU's databeskyttelsesmyndigheder og fra Artikel 29-Gruppen har mulighed for at deltage i dette møde.

⁽²⁰³⁾ Schrems, præmis 40 ff., s. 101-103.

⁽²⁰⁴⁾ Schrems, præmis 51, 52 og 62.

⁽²⁰⁵⁾ Schrems, præmis 65.

⁽²⁰⁶⁾ Schrems, præmis 76.

- (148) I forbindelse med den årlige fælles evaluering vil Kommissionen anmode det amerikanske handelsministerium om at tilvejebringe omfattende oplysninger om alle aspekter af EU's og USA's værn om privatlivets fred, herunder om sager modtaget af handelsministeriet fra databeskyttelsesmyndighederne og resultaterne af ex officio-kontrol af overholdelsen. Kommissionen vil ligeledes søge at få afklaret eventuelle spørgsmål vedrørende EU's og USA's værn om privatlivets fred og dets funktion foranlediget af tilgængelige oplysninger, herunder gennemsigtighedsrapporter under USA FREEDOM Act, offentliggjorte rapporter fra de amerikanske nationale efterretningsmyndigheder, databeskyttelsesmyndighederne, grupper involveret i beskyttelsen af privatlivets fred, medierapporter eller enhver anden mulig kilde. For at lette Kommissionens opgave i denne forbindelse skal medlemsstaterne desuden underrette Kommissionen om tilfælde, hvor de foranstaltninger, der træffes af de organer, som er ansvarlige for at sikre overholdelsen af principperne i USA, ikke sikrer overholdelsen, og om eventuelle tegn på, at de foranstaltninger, der træffes af de amerikanske offentlige myndigheder med ansvar for den nationale sikkerhed eller forebyggelse, efterforskning, afsløring og retsforfølgelse i straffesager, ikke sikrer det nødvendige beskyttelsesniveau.
- (149) Kommissionen vil udarbejde en offentlig rapport til Europa-Parlamentet og Rådet på grundlag af den årlige fælles evaluering.

7. SUSPENSION AF AFGØRELSEN OM TILSTRÆKKELIGHEDEN AF BESKYTTELSESNIVEAUET

- (150) Hvis Kommissionen på grundlag af kontrollerne eller andre tilgængelige oplysninger konkluderer, at det beskyttelsesniveau, som værnet om privatlivets fred giver, ikke længere i det væsentlige svarer til beskyttelsesniveauet i Unionen, eller at der er klare tegn på, at det ikke længere kan sikres, at principperne om beskyttelse af privatlivets fred overholdes effektivt i USA, eller at de foranstaltninger, der træffes af de amerikanske offentlige myndigheder med ansvar for den nationale sikkerhed eller forebyggelse, efterforskning, afsløring og retsforfølgelse i straffesager, ikke sikrer det nødvendige beskyttelsesniveau, vil Kommissionen underrette det amerikanske handelsministerium herom og anmode om, at der træffes passende foranstaltninger med henblik på en hurtig reaktion på en potentiel manglende overholdelse af principperne om beskyttelse af privatlivets fred inden for en angivet rimelig tidsramme. Hvis de amerikanske myndigheder efter udløbet af den angivne tidsramme ikke på tilfredsstillende vis dokumenterer, at EU's og USA's værn om privatlivets fred fortsat sikrer en effektiv overholdelse og et tilstrækkeligt beskyttelsesniveau, vil Kommissionen indlede proceduren med henblik på en delvis eller fuldstændig suspension eller ophævelse af denne afgørelse ⁽²⁰⁷⁾. Kommissionen kan alternativt foreslå at ændre afgørelsen, f.eks. ved at begrænse konstateringen af et tilstrækkeligt beskyttelsesniveau til dataoverførsler underlagt yderligere betingelser.
- (151) Kommissionen vil navnlig indlede proceduren for suspension eller ophævelse:
- a) når der tegn på, at de amerikanske myndigheder ikke overholder de udredninger og tilsagn, der er anført i dokumenterne knyttet til nærværende afgørelse, herunder betingelserne og begrænsningerne for de amerikanske offentlige myndigheders adgang til personoplysninger overført under værnet om privatlivets fred med henblik på beskyttelsen af den nationale sikkerhed, retshåndhævelse og andre offentlige interesser
 - b) når klager fra registrerede i EU systematisk ikke behandles effektivt. I denne forbindelse vil Kommissionen tage højde for alle de forhold, der indvirker på muligheden for, at registrerede i EU kan gøre deres rettigheder gældende, herunder navnlig selvcertificerede amerikanske foretagenders frivillige tilsagn om at samarbejde med og rette sig efter databeskyttelsesmyndighedernes anbefalinger eller
 - c) når ombudsmanden i værnet om privatlivets fred systematisk ikke reagerer rettidigt og behørigt på anmodninger fra registrerede i EU.
- (152) I forbindelse med den årlige fælles evaluering af, hvordan EU's og USA's værn om privatlivets fred fungerer, vil Kommissionen ligeledes overveje at indlede proceduren med henblik på ændring, suspension eller ophævelse af denne afgørelse, hvis det amerikanske handelsministerium eller andre ministerier eller agenturer involveret i gennemførelsen af værnet om privatlivets fred — eller i forbindelse med nationale sikkerhedsanliggender — repræsentanter fra de amerikanske efterretningsenheder eller ombudsmanden ikke forelægger de oplysninger og præciseringer, der er nødvendige for at vurdere overholdelsen af principperne om beskyttelse af privatlivets fred, klagebehandlingsprocedurens effektivitet eller en eventuel sænkning af det nødvendige beskyttelsesniveau som

⁽²⁰⁷⁾ Fra datoen for anvendelse af den generelle forordning om databeskyttelse vil Kommissionen gøre brug af sine beføjelser til i behørigt begrundede særligt hastende tilfælde at vedtage en gennemførelsesretsakt, der suspenderer nærværende afgørelse og finder anvendelse straks uden forudgående forelæggelse for det relevante komitologiudvalg, og som er gældende i højst seks måneder.

følge af de amerikanske efterretningsenheders foranstaltninger, herunder navnlig som følge af indsamling og/eller adgang til personoplysninger, som ikke er begrænset til, hvad der er strengt nødvendigt og proportionalt. Kommissionen tager i denne forbindelse hensyn til, i hvilket omfang de relevante oplysninger kan opnås fra andre kilder, herunder rapporter fra selvcertificerede amerikanske foretagender, i overensstemmelse med USA FREEDOM Act.

- (153) Denne afgørelse tager højde for de udtalelser, som den ved direktiv 95/46/EF, artikel 29, nedsatte gruppe om beskyttelse af personoplysninger i forbindelse med behandling af personoplysninger har afgivet om det beskyttelsesniveau, der gives med EU's og USA's værn om privatlivets fred ⁽²⁰⁸⁾.
- (154) Europa-Parlamentet vedtog en beslutning om transatlantiske datastrømme ⁽²⁰⁹⁾.
- (155) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 31, stk. 1, i direktiv 95/46/EF —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

1. Med henblik på artikel 25, stk. 2, i direktiv 95/46/EF sikrer USA et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til foretagender i USA under EU's og USA's værn om privatlivets fred.
2. EU's og USA's værn om privatlivets fred består af de principper, som er opstillet af det amerikanske handelsministerium den 7. juli 2016 som fastsat i bilag II og de officielle udredninger og tilsagn indeholdt i de dokumenter, der er opført i bilag I, III og VII.
3. Med henblik på stk. 1 overføres personoplysninger under EU's og USA's værn om privatlivets fred, hvis de overføres fra EU til foretagender i USA, der er opført på »listen over deltagere i værnet om privatlivets fred«, som føres og offentliggøres af det amerikanske handelsministerium i overensstemmelse med afsnit I og III i principperne i bilag II.

Artikel 2

Denne afgørelse har ingen indvirkning på anvendelsen af de bestemmelser i direktiv 95/46/EF, som vedrører behandling af personoplysninger i medlemsstaterne, især artikel 4, ud over artikel 25, stk. 1.

Artikel 3

Når de kompetente myndigheder i medlemsstaterne udøver deres beføjelser i medfør af artikel 28, stk. 3, i direktiv 95/46/EF, og dette fører til suspension eller definitivt forbud mod dataoverførsel til et foretagende i USA, der er opført på listen over deltagere i værnet om privatlivets fred i overensstemmelse med afsnit I og III i principperne i bilag II, med det formål at beskytte personer i forbindelse med behandlingen af deres personoplysninger, underretter den pågældende medlemsstat straks Kommissionen herom.

Artikel 4

1. Kommissionen vil løbende overvåge, hvordan EU's og USA's værn om privatlivets fred fungerer, for at vurdere, om USA fortsat sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres under værnet fra EU til foretagender i USA.

⁽²⁰⁸⁾ Se udtalelse 01/2016 om afgørelsen om tilstrækkeligheden af EU's og USA's værn om privatlivets fred, som blev vedtaget den 13. april 2016.

⁽²⁰⁹⁾ Europa-Parlamentets beslutning af 26. maj 2016 om transatlantiske datastrømme (2016/2727(RSP)).

2. Medlemsstaterne og Kommissionen underretter hinanden om tilfælde, hvor regeringsorganer i USA med lovbestemte beføjelser til at håndhæve overholdelsen af principperne i bilag II tilsyneladende ikke har indført effektive afslørings- og tilsynsmekanismer, der gør det muligt i praksis at identificere og sanktionere tilsidesættelser af principperne.

3. Medlemsstaterne og Kommissionen underretter gensidigt 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 ud over, hvad der er strengt nødvendigt, og/eller hvor der tilsyneladende ikke er en effektiv retsbeskyttelse mod sådanne indgreb.

4. Kommissionen skal senest et år fra datoen for meddelelse af denne afgørelse til medlemsstaterne og herefter hvert år evaluere konklusionen i artikel 1, stk. 1, på grundlag af alle tilgængelige oplysninger, herunder oplysningerne modtaget som led i den årlige fælles evaluering, der henvises til i bilag I, II og VI.

5. Kommissionen aflægger rapport om relevante resultater til det udvalg, der er nedsat ved artikel 31 i direktiv 95/46/EF.

6. Kommissionen forelægger et udkast til foranstaltninger i overensstemmelse med den i artikel 31, stk. 2, i direktiv 95/46/EF fastsatte procedure med henblik på at suspendere, ændre eller ophæve nærværende afgørelse eller begrænse dens anvendelsesområde, herunder når der er tegn på:

- at de amerikanske offentlige myndigheder ikke overholder de udredninger og tilsagn, der er anført i dokumenterne knyttet til denne afgørelse, herunder betingelserne og begrænsningerne for de amerikanske offentlige myndigheders adgang til personoplysninger overført under EU's og USA's værn om privatlivets fred med henblik på beskyttelsen af den nationale sikkerhed, retshåndhævelse og andre offentlige interesser
- at klager fra registrerede i EU systematisk ikke behandles effektivt, eller
- når ombudsmanden i værnet om privatlivets fred systematisk ikke reagerer rettidigt og behørigt på anmodninger fra registrerede i EU som påkrævet i bilag III, afsnit 4, litra e).

Kommissionen forelægger ligeledes et udkast til foranstaltninger, hvis de organer, der skal sikre, at EU's og USA's værn om privatlivets fred fungerer i USA, ikke samarbejder, og Kommissionen således ikke kan vurdere, om konklusionen i artikel 1, stk. 1, er berørt.

Artikel 5

Medlemsstaterne træffer de nødvendige foranstaltninger for at efterkomme denne afgørelse.

Artikel 6

Denne afgørelse er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 12. juli 2016.

På Kommissionens vegne
Věra JOUROVÁ
Medlem af Kommissionen

BILAG I

Brev fra den amerikanske handelsminister Penny Pritzker

Den 7. juli 2016

Věra Jourová
Kommissær for retlige anliggender, forbrugere og ligestilling mellem mænd og kvinder
Europa-Kommissionen
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
Belgien

Kære kommissær Věra Jourová,

Det glæder mig at fremsende en pakke med dokumenter på vegne af USA vedrørende EU's og USA's værn om privatlivets fred, som er resultatet af to års udbytterige drøftelser mellem vores team. Denne pakke udgør sammen med andre materialer, som Kommissionen har adgang til via offentlige kilder, et meget solidt grundlag for Europa-Kommissionens vedtagelse af en ny afgørelse om et tilstrækkeligt beskyttelsesniveau ⁽¹⁾.

Vi bør begge være stolte over forbedringerne af ordningen. Værnet om privatlivets fred er baseret på principper, der er stærk enighed om på begge sider af Atlanten, og vi har styrket samarbejdet. Gennem vores samarbejde har vi reel mulighed for at forbedre beskyttelsen af privatlivets fred i hele verden.

Pakken vedrørende værnet om privatlivets fred indeholder principperne til værn om privatlivets fred samt et brev vedføjet som bilag 1 fra det amerikanske handelsministeriums International Trade Administration, som forvalter programmet, hvor der redegøres for de tilsagn, som ministeriet har afgivet for at sikre, at værnet om privatlivets fred fungerer effektivt. Pakken indeholder ligeledes bilag 2, der omfatter handelsministeriets andre tilsagn vedrørende den nye voldgiftsmodel under værnet om privatlivets fred.

Jeg har anmodet mit personale om at afsætte alle nødvendige ressourcer til at sikre en hurtig og fuldstændig gennemførelse af ordningen for værnet om privatlivets fred og sikre, at tilsagnene i bilag 1 og 2 efterleves rettidigt.

Pakken vedrørende værnet om privatlivets fred indeholder ligeledes andre dokumenter fra andre amerikanske instanser:

- Et brev fra Federal Trade Commission (FTC), hvor der redegøres for FTC's håndhævelse af værnet om privatlivets fred
- Et brev fra det amerikanske transportministerium, hvor der redegøres for FTC's håndhævelse af værnet om privatlivets fred
- To breve fra Office of the Director of National Intelligence (ODNI) vedrørende de garantier og begrænsninger, der finder anvendelse på de amerikanske nationale sikkerhedsmyndigheder
- Et brev fra det amerikanske udenrigsministerium og et ledsagende memorandum, hvor der redegøres for udenrigsministeriets tilsagn om at oprette en ny ombudsmand i værnet om privatlivets fred, til hvem der kan indgives forespørgsler om den amerikanske signalefterretningspraksis 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.

USA tager disse tilsagn meget alvorligt.

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

Senest 30 dage efter den endelige godkendelse af afgørelsen om et tilstrækkeligt beskyttelsesniveau vil hele pakken vedrørende værnet om privatlivets fred blive indleveret til Federal Register med henblik på offentliggørelse.

Vi glæder os til vores samarbejde om gennemførelsen af værnet om privatlivets fred og i den kommende fase i denne proces.

Med venlig hilsen

Penny Pritzker



Bilag 1

Brev fra fungerende viceminister for international handel Ken Hyatt

Věra Jourová
Kommissær for retlige anliggender, forbrugere og ligestilling mellem mænd og kvinder
Europa-Kommissionen
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
Belgien

Kære kommissær Věra Jourová,

Det glæder mig på vegne af International Trade Administration at redegøre for den forbedrede beskyttelse af personoplysninger under ordningen for EU's og USA's værn om privatlivets fred (»været om privatlivets fred« eller »ordningen«) og de tilsagn, som det amerikanske handelsministerium (»ministeriet«) har afgivet for at sikre, at været om privatlivets fred fungerer effektivt. Færdiggørelsen af denne historiske ordning er et vigtigt resultat for privatlivets fred og for virksomheder på begge sider af Atlanten. Den giver privatpersoner i EU en tro på, at deres oplysninger vil blive beskyttet, og at de vil have adgang til retsmidler til afhjælpning af problemer. Den giver en sikkerhed, der vil medvirke til at fremme den transatlantiske økonomi ved at sikre, at tusindvis af europæiske og amerikanske virksomheder fortsat kan investere og gøre forretninger på tværs af grænserne. Været om privatlivets fred er resultatet af to års hårdt arbejde og samarbejde med vores kolleger i Europa-Kommissionen (»Kommissionen«). Vi glæder os til vores fortsatte samarbejde med Kommissionen om at sikre, at været om privatlivets fred fungerer efter hensigten.

Vi har samarbejdet med Kommissionen om at udvikle været om privatlivets fred, således at foretagender i USA får mulighed for at opfylde kravene om tilstrækkelig beskyttelse af personoplysninger i EU-retten. Den nye ordning indebærer en række væsentlige fordele for både personer og virksomheder. For det første er der en række vigtige bestemmelser om beskyttelse af privatpersoners personoplysninger i EU. De deltagende amerikanske foretagender skal udvikle en overensstemmende politik til beskyttelse af privatlivets fred, offentligt forpligte sig til at overholde principperne til værn om privatlivets fred, således at forpligtelsen kan kræves opfyldt i henhold til amerikansk ret, årligt recertificere deres overholdelse over for ministeriet, give privatpersoner i EU gratis adgang til en uafhængig tvistbilæggelsestjeneste og være underlagt den amerikanske Federal Trade Commission (»FTC«), transportministeriet eller et andet håndhævelsesorgans kompetence. Været om privatlivets fred vil for det andet give tusindvis af 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. Det transatlantiske økonomiske forhold er allerede verdens største og tegner sig for halvdelen af det globale økonomiske output og for næsten 1 bio. USD i varer og tjenester og understøtter millioner af arbejdspladser på begge sider af Atlanten. Virksomheder, der er afhængige af transatlantiske datastrømme, kommer fra alle industrisektorer og omfatter store Fortune 500-selskaber samt mange små og mellemstore virksomheder (SMV'er). Transatlantiske datastrømme giver amerikanske foretagender mulighed for at behandle oplysninger, der er nødvendige for at tilbyde europæiske borgere varer, tjenester og beskæftigelsesmuligheder. Været om privatlivets fred er baseret på fælles principper om privatlivets fred, bygger bro mellem vores forskellige retlige procedurer og fremmer opfyldelsen af handelsmæssige og økonomiske mål i både Europa og USA.

Selv om et foretagende selv afgør, om det vil selvcertificere sin tilslutning til denne nye ordning, kan Federal Trade Commission eller transportministeriet, afhængigt af hvilken myndighed der har kompetence over foretagendet i været om privatlivets fred, når først foretagendet offentligt har forpligtet sig til at overholde principperne til værn om privatlivets fred, kræve, at foretagendets tilsagn opfyldes i henhold til amerikansk ret.

Forbedringer i medfør af principperne til værn om privatlivets fred

Det nye værn om privatlivets fred styrker beskyttelsen af privatlivets fred ved at:

- kræve, at registrerede får flere oplysninger i overensstemmelse med princippet om oplysningspligt, herunder en erklæring om foretagendets deltagelse i været om privatlivets fred, en erklæring om den enkeltes ret til indsigt i personoplysninger, og at den relevante uafhængige tvistbilæggesinstans identificeres
- styrke beskyttelsen af personoplysninger, der overføres fra et foretagende i været om privatlivets fred til en dataansvarlig tredjemand, ved at kræve, at parterne indgår en aftale, 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

- styrke beskyttelsen af personoplysninger, der overføres fra et foretagende i værnet om privatlivets fred til en tredjemand, der fungerer som mellemmand, ved at kræve, at et foretagende i værnet om privatlivets fred træffer rimelige og passende foranstaltninger for at sikre, at mellemmanden rent faktisk behandler de overførte personoplysninger i overensstemmelse med foretagendets forpligtelser i henhold til principperne, efter varsel tager rimelige og passende skridt til at stoppe og afhjælpe uautoriseret behandling og forelægger et sammendrag eller en repræsentativ kopi af de relevante bestemmelser om beskyttelse af privatlivets fred i aftalen med den pågældende mellemmand for ministeriet på anmodning
- sikre, at et foretagende i værnet om privatlivets fred har ansvaret for behandlingen af de personoplysninger, det modtager under værnet om privatlivets fred, og for efterfølgende overførsler til en tredjemand, der fungerer som mellemmand på dets vegne, og at foretagendet i værnet om privatlivets fred fortsat har ansvaret i medfør af principperne, hvis dets mellemmand behandler disse personoplysninger i strid med principperne, medmindre foretagendet beviser, at det ikke er skyld i den begivenhed, der medførte skade
- præcisere, at foretagender i værnet om privatlivets fred skal begrænse personoplysninger til de oplysninger, der er relevante for formålene med behandlingen
- kræve, at et foretagende hvert år bekræfter over for ministeriet, at det fortsat vil anvende principperne på de oplysninger, som det modtog, mens det deltog i værnet om privatlivets fred, hvis det forlader værnet om privatlivets fred og vælger at beholde disse oplysninger
- kræve, at registrerede får gratis adgang til uafhængige klageinstanser
- kræve, at foretagenderne og deres udpegede uafhængige klageinstanser straks besvarer forespørgsler og anmodninger fra handelsministeriet om oplysninger om værnet om privatlivets fred
- kræve, at foretagender straks besvarer klager over manglende overholdelse af principperne, som EU-medlemsstaternes myndigheder henviser via ministeriet og
- kræve, at et foretagende i værnet om privatlivets fred offentliggør alle relevante afsnit relateret til værnet om privatlivets fred i alle overholdelses- eller vurderingsrapporter forelagt FTC, hvis det bliver genstand for en FTC- eller domstolsafgørelse om manglende overholdelse.

Det amerikanske handelsministeriums forvaltning af og tilsyn med programmet for værnet om privatlivets fred

Ministeriet gentager sit tilsagn om at oprette og offentliggøre en officiel liste over amerikanske foretagender, der har foretaget selvcertificering over for ministeriet og offentligt erklæret, at de har tilsluttet sig principperne (»listen over deltagere i værnet om privatlivets fred«). Ministeriet vil ajourføre listen over deltagere i værnet om privatlivets fred ved at fjerne foretagender, 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 foretagender, der tidligere har foretaget selvcertificering over for ministeriet, men som er blevet fjernet fra listen over deltagere i værnet om privatlivets fred, herunder foretagender, der er blevet fjernet på grund af vedvarende overtrædelse af principperne. Ministeriet vil angive årsagen til, at det enkelte foretagende blev fjernet fra listen.

Ministeriet forpligter sig ligeledes til at styrke forvaltningen af og tilsynet med værnet om privatlivets fred. Ministeriet vil navnlig:

Flere oplysninger på webstedet for værnet om privatlivets fred

- oprette listen over deltagere i værnet om privatlivets fred og en fortegnelse over de foretagender, der tidligere har foretaget selvcertificering og tilsluttet sig principperne, men som ikke længere er dækket af værnet om privatlivets fred
- tydeligt præcisere, at alle foretagender, der er fjernet fra listen over deltagere i værnet om privatlivets fred, ikke længere er dækket af værnet om privatlivets fred, men at de ikke desto mindre stadig skal anvende principperne på de personoplysninger, som de modtog, mens de deltog i værnet om privatlivets fred, så længe de er i besiddelse af disse oplysninger og
- angive et link til listen over FTC-sager relateret til værnet om privatlivets fred på FTC's websted

Kontrol af selvcertificeringskrav

- inden afslutningen af behandlingen af et foretagendes selvcertificering (eller årlige recertificering) og opførelsen af et foretagende på listen over deltagere i værnet om privatlivets fred, kontrollere, at foretagendet har:
 - anført de krævede kontaktoplysninger for foretagendet
 - beskrevet foretagendets aktiviteter i relation til personoplysninger modtaget fra EU
 - angivet, hvilke personoplysninger der er omfattet af selvcertificeringen
- angivet webadressen på det sted, hvor programmet til beskyttelse af privatlivets fred er tilgængeligt, hvis foretagendet har et offentligt websted, eller hvis foretagendet ikke har et offentligt websted, angivet adressen på det sted, hvor offentligheden kan få adgang til programmet til beskyttelse af privatlivets fred
- angivet i sit relevante program til beskyttelse af privatlivets fred, at det tilslutter sig principperne, og hvis programmet er tilgængeligt online, et hyperlink til ministeriets websted for værnet om privatlivets fred
- angivet det specifikke lovbestemte organ, der har kompetence til at behandle klager over foretagender 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)
- angivet, at det vil samarbejde med databeskyttelsesmyndighederne med henblik på at undersøge og afgøre eventuelle klager, der modtages under værnet om privatlivets fred, herunder navnlig besvare deres forespørgsler, når registrerede i EU har indbragt deres klager direkte til deres nationale databeskyttelsesmyndigheder, hvis foretagendet vælger at opfylde kravene i punkt a), nr. i) og iii), i princippet om klageadgang, håndhævelse og ansvar ved at forpligte sig til at samarbejde med de relevante databeskyttelsesmyndigheder i EU
- angivet ethvert program til beskyttelse af privatlivets fred, som foretagendet deltager i
- angivet metoden til kontrol af overholdelsen af principperne (f.eks. intern kontrol, tredjemandskontrol)
- angivet den uafhængige klageinstans, der kan behandle uløste sager, i sin selvcertificeringsanmeldelse og i sit program til beskyttelse af privatlivets fred
- angivet i sit relevante program til beskyttelse af privatlivets fred, hvis programmet er tilgængeligt online, et hyperlink til webstedet og klageformular for den uafhængige klageinstans, der kan behandle uløste sager og
- angivet, hvis foretagendet har anført, at det agter at modtage oplysninger om menneskelige ressourcer, der overføres fra EU til brug inden for rammerne af et ansættelsesforhold, at det vil samarbejde med og rette sig efter databeskyttelsesmyndighedernes anbefalinger om afgørelsen af klager over foretagendets aktiviteter i relation til disse oplysninger, fremsendt en kopi af sit program til beskyttelse af oplysninger om menneskelige ressourcer til ministeriet og angivet, hvor de berørte medarbejdere kan få adgang til programmet til beskyttelse af privatlivets fred.
- samarbejde med uafhængige klageinstanser for at kontrollere, at foretagenderne rent faktisk har ladet sig registrere ved den relevante instans angivet i deres selvcertificeringsanmeldelser, hvis denne registrering er nødvendig

Større opfølgningsindsats over for foretagender, der er blevet fjernet fra listen over deltagere i værnet om privatlivets fred

- meddele foretagender, der er blevet fjernet fra listen over deltagere i værnet om privatlivets fred på grund af »vedvarende overtrædelse«, at de ikke må beholde oplysninger indsamlet under værnet om privatlivets fred og
- fremsende spørgeskemaer til foretagender, hvis selvcertificeringer er udløbet, eller som frivilligt har trukket sig ud af værnet om privatlivets fred, for at kontrollere, om foretagendet agter at tilbagesende eller slette personoplysningerne eller fortsat vil anvende principperne på de personoplysninger, som de modtog, mens de deltog i værnet om privatlivets fred, og hvis de beholder personoplysningerne, finde ud af, hvem der fremover fungerer som kontaktpunkt for spørgsmål relateret til værnet om privatlivets fred

Søgning efter og håndtering af falske påstande om deltagelse i værnet

- gennemgå programmerne til beskyttelse af privatlivets fred for foretagender, der tidligere har deltaget i programmet for værnet om privatlivets fred, men som er blevet fjernet fra listen over deltagere i værnet om privatlivets fred, for at finde eventuelle falske påstande om deltagelse i værnet om privatlivets fred
- løbende, når et foretagende: a) trækker sig ud af værnet om privatlivets fred, b) ikke recertificerer sin tilslutning til principperne eller c) fjernes som deltager i værnet om privatlivets fred, navnlig på grund af »vedvarende overtrædelse«, forpligte sig til ex officio at kontrollere, at foretagendet har fjernet alle henvisninger til værnet om privatlivets fred i relevante offentliggjorte programmer til beskyttelse af privatlivets fred, der lader formode, at foretagendet fortsat deltager aktivt i værnet om privatlivets fred og er berettiget til at drage fordel heraf. Hvis ministeriet konstaterer, at disse henvisninger ikke er blevet fjernet, vil ministeriet advare foretagendet om, at ministeriet i påkommende tilfælde vil henvise sagen til det relevante organ med henblik på eventuel håndhævelse, hvis foretagendet fastholder påstande om certificering under værnet om privatlivets fred. Hvis foretagendet hverken fjerner henvisningerne eller selvcertificerer sin tilslutning til principperne til værn om privatlivets fred, vil ministeriet ex officio henvise sagen til FTC, transportministeriet eller et andet relevant håndhævelsesorgan eller, hvis det er relevant, træffe foranstaltninger for at sikre, at certificeringsmærket for værnet om privatlivets fred fjernes
- træffe andre foranstaltninger for at identificere falske påstande om deltagelse i værnet om privatlivets fred og uretmæssig brug af certificeringsmærket for værnet om privatlivets fred, herunder ved hjælp af internetsøgninger for at identificere websteder med billeder af certificeringsmærket for værnet om privatlivets fred og henvisninger til værnet om privatlivets fred i foretagendernes programmer til beskyttelse af privatlivets fred
- straks tage fat på alle problemer, der identificeres under ex officio-overvågningen af falske påstande om deltagelse og misbrug af certificeringsmærket, herunder advare foretagender, der afgiver urigtige oplysninger om deres deltagelse i programmet for værnet om privatlivets fred, som beskrevet ovenfor
- træffe andre relevante korrigerende foranstaltninger, herunder ved brug af de retsmidler, som ministeriet har adgang til, og henvise sager til FTC, transportministeriet eller et andet relevant håndhævelsesorgan og
- straks gennemgå og behandle klager over falske påstande om deltagelse til ministeriet.

Ministeriet vil gennemgå foretagenders programmer til beskyttelse af privatlivets fred med henblik på en mere effektiv identifikation og imødegåelse af falske påstande om deltagelse i værnet om privatlivets fred. Ministeriet vil navnlig gennemgå programmerne til beskyttelse af privatlivets fred for foretagender, hvis selvcertificering er udløbet, fordi de ikke har recertificeret deres tilslutning til principperne. Ministeriet vil foretage denne type gennemgang for at kontrollere, at disse foretagender har fjernet alle henvisninger til værnet om privatlivets fred i relevante offentliggjorte programmer til beskyttelse af privatlivets fred, der lader formode, at foretagenderne fortsat deltager aktivt i værnet om privatlivets fred. I forbindelse med disse gennemgange vil ministeriet identificere foretagender, som ikke har fjernet disse henvisninger, og sende disse foretagender et brev fra ministeriets Office of General Counsel med en advarsel om, at der kan blive iværksat håndhævelsesforanstaltninger, hvis henvisningerne ikke fjernes. Ministeriet vil træffe opfølgende tiltag for at sikre, at foretagenderne enten fjerner de ukorrekte henvisninger eller recertificerer deres tilslutning til principperne. Ministeriet vil desuden gøre en indsats for at identificere falske påstande om deltagelse i værnet om privatlivets fred fremsat af foretagender, der aldrig har deltaget i programmet for værnet om privatlivets fred, og vil træffe tilsvarende korrigerende foranstaltninger over for disse foretagender.

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

- løbende overvåge den effektive overholdelse, herunder ved fremsendelse af detaljerede spørgeskemaer til deltagende foretagender, for at identificere problemer, som kan berettiggere yderligere opfølgning. Denne kontrol af overholdelsen foretages navnlig: a) når ministeriet har modtaget specifikke klager, der ikke er chikanerende, om et foretagendes manglende overholdelse af principperne, b) når et foretagende ikke besvarer forespørgsler fra ministeriet om oplysninger om værnet om privatlivets fred på tilfredsstillende vis, eller c) når der er troværdig dokumentation for, at et foretagende ikke opfylder sine forpligtelser under værnet om privatlivets fred. Ministeriet vil, når det er relevant, drøfte denne kontrol af overholdelsen med de kompetente databeskyttelsesmyndigheder og
- regelmæssigt vurdere forvaltningen af og tilsynet med programmet for værnet om privatlivets fred for at sikre, at overvågningen er tilstrækkelig til at takle nye problemer, efterhånden som de opstår.

Ministeriet har øget tildelingen af ressourcer til forvaltningen af og tilsynet med programmet for værnet om privatlivets fred, herunder fordoblet antallet af medarbejdere med ansvar for forvaltningen af og tilsynet med programmet. Ministeriet vil også fremover afsætte tilstrækkelige ressourcer til denne indsats for at sikre en effektiv overvågning og forvaltning af programmet.

Skræddersyet websted for værnet om privatlivets fred til bestemte målgrupper

Ministeriet vil skræddersy webstedet for værnet om privatlivets fred til tre bestemte målgrupper: privatpersoner og virksomheder i EU samt amerikanske virksomheder. Angivelsen 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) privatpersoners rettigheder i EU under værnet om privatlivets fred, 2) de klageinstanser, som privatpersoner i EU har adgang til, når de mener, at et foretagende ikke har opfyldt sin forpligtelse til at overholde principperne, og 3) hvor man kan finde oplysninger om et foretagendes selvcertificering under værnet om privatlivets fred. Med hensyn til EU-virksomheder vil det blive lettere at kontrollere: 1) om et foretagende er berettiget til at drage fordel af værnet om privatlivets fred, 2) den type oplysninger, der er dækket af et foretagendes selvcertificering under værnet om privatlivets fred, 3) det program til beskyttelse af privatlivets fred, som de dækkede oplysninger er omfattet af, og 4) den metode, som foretagendet anvender til at verificere sin tilslutning til principperne.

Øget samarbejde 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 et foretagende 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 foretagendet. Kontaktpunktet vil ligeledes få henvist sager om foretagender, der fremsætter falske påstande om deltagelse i værnet om privatlivets fred, selv om de aldrig har selvcertificeret deres tilslutning til principperne. Kontaktpunktet vil bistå databeskyttelsesmyndigheder, der søger oplysninger om et specifikt foretagendes selvcertificering eller tidligere deltagelse i programmet, og kontaktpunktet vil besvare databeskyttelsesmyndighedernes forespørgsler om gennemførelsen af specifikke krav under værnet om privatlivets fred. Ministeriet vil ligeledes give databeskyttelsesmyndighederne materiale om værnet om privatlivets fred, som de kan offentliggøre på deres egne websteder for at øge gennemsigtigheden for privatpersoner og virksomheder i EU. Øget kendskab til værnet om privatlivets fred og rettigheder og forpligtelser under værnet bør gøre det lettere at identificere problemer, efterhånden som de opstår, således at de kan takles på passende vis.

Fremme af afgørelser af klager om manglende overholdelse

Ministeriet vil gennem det særlige kontaktpunkt modtage klager over foretagender, der ikke overholder principperne, henvist til ministeriet fra databeskyttelsesmyndighederne. Ministeriet vil gøre sit yderste for at fremme afgørelsen af klager i samarbejde med foretagendet i værnet om privatlivets fred. Ministeriet vil informere databeskyttelsesmyndigheden om status senest 90 dage efter modtagelsen af klager. For at lette indgivelsen af sådanne klager vil ministeriet udarbejde en standardformular, som databeskyttelsesmyndighederne kan fremsende til ministeriets særlige kontaktpunkt. Det særlige kontaktpunkt vil identificere alle henvisningerne fra databeskyttelsesmyndighederne, som ministeriet har modtaget, og i forbindelse med den nedenfor beskrevne årlige evaluering vil ministeriet udarbejde en rapport, hvor de klager, ministeriet modtager hvert år, analyseres i aggregeret form.

Indførelse af voldgiftsprocedurer og valg af voldgiftsmænd i samarbejde med Kommissionen

Ministeriet vil opfylde sine tilsagn i bilag I og offentliggøre procedurerne, når parterne er nået til enighed.

Fælles mekanisme til evaluering af, hvordan værnet om privatlivets fred fungerer

Handelsministeriet, FTC og andre relevante organer vil afholde årlige møder med Kommissionen, interesserede databeskyttelsesmyndigheder og relevante repræsentanter fra Artikel 29-Gruppen, hvor ministeriet vil gøre status over programmet for værnet om privatlivets fred. De årlige møder vil omfatte drøftelser af aktuelle spørgsmål om funktionen og gennemførelsen af, tilsynet med og håndhævelsen af værnet om privatlivets fred, herunder af henvisninger modtaget af ministeriet fra databeskyttelsesmyndighederne og resultaterne af ex officio-kontrollen af overholdelsen, og møderne kan ligeledes omfatte drøftelser af relevante lovændringer. Den første årlige evaluering og de efterfølgende evalueringer, hvor det er relevant, vil omfatte en dialog om andre spørgsmål, såsom på området for automatiske afgørelser, herunder aspekter vedrørende ligheder og forskelle for så vidt angår fremgangsmåderne i EU og USA.

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 værnet om privatlivets fred for så vidt angår databeskyttelsen og de begrænsninger og beskyttelsesgarantier, der gælder for amerikanske myndigheders adgang til og efterfølgende anvendelse af personoplysninger.

Den nationale sikkerhedsundtagelse

Med hensyn til de begrænsninger, der gælder for tilslutningen til principperne til værn om privatlivets fred af hensyn til den nationale sikkerhed, har General Counsel of the Office of the Director of National Intelligence, Robert Litt, ligeledes sendt to breve til Justin Antonipillai og Ted Dean i handelsministeriet, og disse er blevet fremsendt til Dem. I brevene redegøres bl.a. indgående for de politikker, garantier og begrænsninger, der finder anvendelse på signalefterretningsaktiviteter i USA. I brevene redegøres ligeledes for de amerikanske efterretningstjenesters åbenhed omkring disse spørgsmål. Da Kommissionen er i gang med at vurdere ordningen for værnet om privatlivets fred, giver oplysningerne i disse breve den nødvendige sikkerhed til at konkludere, at værnet om privatlivets fred vil fungere efter hensigten i overensstemmelse med værnets principper. Vi forstår, at Kommissionen fremover muligvis vil anvende oplysninger, der allerede er blevet offentliggjort af de amerikanske efterretningstjenester, og andre oplysninger i den årlige evaluering af ordningen for værnet om privatlivets fred.

På grundlag af principperne til værn om privatlivets fred og de ledsagende breve og materialer, herunder ministeriets tilsagn vedrørende forvaltningen af og tilsynet med ordningen for værnet om privatlivets fred, forventer vi, at Kommissionen vil vurdere, at ordningen for EU's og USA's værn om privatlivets fred giver en tilstrækkelig beskyttelse i henhold til EU-retten, og at der fortsat vil blive overført oplysninger fra EU til foretagender, der deltager i værnet om privatlivets fred.

Med venlig hilsen

Ken Hyatt

*Bilag 2***Voldgiftsmodel***BILAG I*

I dette bilag I angives de betingelser, på hvilke foretagender i værnet om privatlivets fred 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's og USA's værn om privatlivets fred. 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 mekanismer i værnet om privatlivets fred.

A. Anvendelsesområde

Den registrerede har adgang til voldgift i forbindelse med øvrige krav for at få afgjort, om et foretagende i værnet om privatlivets fred 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 værnet om privatlivets fred.

B. Tilgængelige retsmidler

Denne mulighed for voldgift giver udelukkende panelet i værnet om privatlivets fred (der består af en eller tre voldgiftsmænd som aftalt af 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 afhjælpe overtrædelser af principperne i forhold til de registrerede. Dette er voldgiftspanelets eneste beføjelser, for så vidt angår retsmidler. Panelet skal tage højde for andre retsmidler, der allerede er blevet pålagt gennem andre mekanismer i værnet om privatlivets fred, 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 at kræve voldgift, skal træffe følgende foranstaltninger inden indgivelse af en begæring om voldgift: 1) rette direkte henvendelse til foretagendet og fremføre den påståede overtrædelse og give foretagendet mulighed for at løse problemet inden for den tidsramme, der er anført i afsnit III.11, d), nr. i), i principperne, 2) gøre brug af den uafhængige klageinstans i henhold til principperne, og 3) rejse sagen gennem den pågældendes databeskyttelsesmyndighed over for handelsministeriet og give handelsministeriet 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 gentagende 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 EU-databeskyttelsesmyndighed 1) er bemyndiget i henhold til afsnit III.5 eller III.9 i principperne, eller 2) er bemyndiget til at rette direkte henvendelse til foretagendet 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. Voldgiftsavgørelser 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⁾ Afsnit I.5 i principperne.

E. Domstolsprøvelse og håndhævelse

Registrerede og foretagender i værnet om privatlivets fred har adgang til domstolsprøvelse og håndhævelse af voldgiftsafgørelser i henhold til amerikansk ret under Federal Arbitration Act (⁽¹⁾). Disse sager skal indbringes for den forbundsdomstol (federal district court), inden for hvis jurisdiktion hovedforretningsstedet for foretagendet i værnet om privatlivets fred 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 fra den nedenstående liste over voldgiftsmænd.

I overensstemmelse med gældende ret vil det amerikanske handelsministerium og Europa-Kommissionen udarbejde en liste med mindst 20 voldgiftsmænd valgt på baggrund af deres uafhængighed, integritet og ekspertise. Processen er som følger:

Voldgiftsmænd:

- 1) er opført på listen i en periode på tre år, der ekstraordinært kan forlænges i yderligere tre år
- 2) må ikke modtage instrukser fra eller være tilknyttet nogen part eller noget foretagende i værnet om privatlivets fred, 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.

G. Voldgiftsprocedurer

I henhold til gældende ret skal det amerikanske handelsministerium og Europa-Kommissionen senest seks måneder efter vedtagelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet nå til enighed om en række eksisterende veletablerede amerikanske voldgiftsprocedurer (f.eks. AAA eller JAMS), som skal finde anvendelse på sager, der indbringes for panelet i værnet om privatlivets fred, 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 foretagendet. 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.

(¹) 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. juni 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, forholdet 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 opstået 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.

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 beslutter, at dette i den specifikke voldgiftssag ville føre til uberettigede eller uforholdsmæssige omkostninger.
7. Materiale forelagt voldgiftsmænd vil blive fortroligt behandlet 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 leveringen af meddelelsen til det pågældende foretagende, medmindre parter aftaler andet.

H. Omkostninger

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

Under iagttagelse af gældende ret vil handelsministeriet etablere en fond, der skal finansieres via årlige bidrag fra foretagenderne i værnet om privatlivets fred, som til dels er baseret på foretagendets størrelse, og fonden vil dække voldgiftsomkostningerne, herunder voldgiftsmændenes honorarer, op til maksimumsbeløb i samråd med Europa-Kommissionen. Fonden vil blive forvaltet af en tredjemand, der regelmæssigt vil rapportere om fondens drift. I forbindelse med den årlige evaluering vil handelsministeriet og Europa-Kommissionen evaluere fondens drift, herunder behovet for at justere bidragene eller maksimumsbeløbene, og vil bl.a. se på antallet af voldgiftssager, voldgiftsomkostningerne og behandlingstiden ud fra en fælles forståelse af, at foretagenderne i værnet om privatlivets fred ikke må pålægges en urimelig stor økonomisk byrde. Advokatsalærer er ikke omfattet af denne bestemmelse eller nogen fond under denne bestemmelse.

BILAG II

PRINCIPPERNE I ORDNINGEN FOR EU'S OG USA'S VÆRN OM PRIVATLIVETS FRED FRA DET AMERIKANSKE HANDELSMINISTERIUM

I. OVERSIGT

1. Selv om USA og EU begge har som målsætning at fremme beskyttelsen af privatlivets fred, har de ikke valgt samme fremgangsmåde. I USA anvendes således en fremgangsmåde på sektorplan med en kombination af lovgivning, administrative bestemmelser og selvregulering. På grund af disse forskelle og for at sikre foretagender i USA en pålidelig mekanisme til overførsler af personoplysninger fra EU til USA og samtidig sikre, at registrerede i EU fortsat nyder godt af effektive garantier og beskyttelse, hvilket er et krav i EU-lovgivningen for behandling af personoplysninger, der overføres til tredjelande, har det amerikanske handelsministerium i medfør af sine lovbestemte beføjelser opstillet disse principper til værn om privatlivets fred, herunder de supplerende principper (samlet benævnt »principperne«) med henblik på at fremme og udvikle den internationale handel (15 U.S.C. § 1512). Principperne er udviklet i samarbejde med Europa-Kommissionen og industrien og andre interessenter for at fremme handlen mellem USA og EU. De er udelukkende beregnet på at blive anvendt af amerikanske foretagender, der modtager personoplysninger fra EU, og som ønsker at leve op til kravene vedrørende værnet om privatlivets fred og således drage fordel af Europa-Kommissionens afgørelse om et tilstrækkeligt beskyttelsesniveau ⁽¹⁾. Principperne har ingen indvirkning på anvendelsen af nationale bestemmelser til gennemførelse af direktiv 95/46/EF (»direktivet«), som vedrører behandling af personoplysninger i medlemsstaterne. Principperne begrænser heller ikke andre forpligtelser til at sikre privatlivets fred i amerikansk ret.
2. For at kunne overføre personoplysninger fra EU under værnet om privatlivets fred skal et foretagende foretage selvcertificering om tilslutning til principperne over for det amerikanske handelsministerium (eller dets repræsentant) (»ministeriet«). Et foretagende kan frit vælge, om det vil tilslutte sig principperne til værn om privatlivets fred, men det skal overholde principperne fuldt ud. Et foretagende, der foretager selvcertificering over for ministeriet og offentligt erklærer, at det har tilsluttet sig principperne, skal således overholde principperne fuldt ud. Inden et foretagende kan tilslutte sig værnet om privatlivets fred, skal det: a) omfattes af de undersøgelses- og håndhævelsesbeføjelser, der er tillagt Federal Trade Commission (»FTC«), transportministeriet 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 det forpligter sig til at overholde principperne, c) offentliggøre sine programmer til beskyttelse af privatlivets fred i overensstemmelse med disse principper og d) gennemføre dem fuldt ud. Såfremt et foretagende ikke overholder principperne, kan det drages til ansvar i henhold til Section 5 i Federal Trade Commission Act (15 U.S.C. § 45(a)), der forbyder illoyal eller vildledende praksis i forbindelse med handel, eller andre love eller bestemmelser, der forbyder denne praksis.
3. Handelsministeriet vil oprette og offentliggøre en officiel liste over amerikanske foretagender, der har foretaget selvcertificering over for ministeriet og offentligt erklæret, at de har tilsluttet sig principperne (»listen over deltagere i værnet om privatlivets fred«). Foretagendet drager fordel af værnet om privatlivets fred fra den dato, hvor ministeriet opfører foretagendet på listen over deltagere i værnet om privatlivets fred. Ministeriet vil fjerne et foretagende fra listen over deltagere i værnet om privatlivets fred, hvis foretagendet frivilligt trækker sig ud af værnet om privatlivets fred eller ikke indsender sin årlige anmeldelse om recertificering til ministeriet. Når et foretagende fjernes fra listen over deltagere i værnet om privatlivets fred, kan det ikke længere drage fordel af Europa-Kommissionens afgørelse om et tilstrækkeligt beskyttelsesniveau til at modtage personoplysninger fra EU. Foretagendet skal fortsat anvende principperne på de personoplysninger, som det modtog, mens det deltog i værnet om privatlivets fred, og hvert år bekræfte over for ministeriet, at det fortsat vil anvende principperne, så længe det er i besiddelse af disse oplysninger. I modsat fald skal foretagendet tilbagesende eller slette oplysningerne eller sikre en tilstrækkelig beskyttelse af personoplysningerne på en anden godkendt måde. Ministeriet vil ligeledes fjerne de foretagender fra listen over deltagere i værnet om privatlivets fred, der vedvarende overtræder principperne om beskyttelse af privatlivets fred. Disse foretagender kan ikke drage fordel af værnet om privatlivets fred og skal tilbagesende eller slette personoplysninger modtaget under værnet om privatlivets fred.
4. Ministeriet vil ligeledes oprette og offentliggøre en officiel fortegnelse over amerikanske foretagender, der tidligere har foretaget selvcertificering over for ministeriet, men som er blevet fjernet fra listen over deltagere i værnet om privatlivets fred. Ministeriet vil klart advare om, at disse foretagender ikke deltager i værnet om privatlivets fred, at fjernelse fra listen over deltagere i værnet om privatlivets fred betyder, at disse foretagender ikke kan hævde, at de overholder principperne i værnet om privatlivets fred og skal undgå erklæringer eller vildledende praksis, der lader formode, at de deltager i værnet om privatlivets fred, og at disse foretagender ikke længere kan drage fordel af

⁽¹⁾ 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 opstået 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.

Europa-Kommissionens afgørelse om et tilstrækkeligt beskyttelsesniveau, der giver disse foretagender mulighed for at modtage personoplysninger fra EU. FTC, transportministeriet eller andre håndhævelsesmyndigheder kan træffe håndhævelsesforanstaltninger over for et foretagende, der fortsat hævder, at det deltager i værnet om privatlivets fred eller afgiver andre urigtige oplysninger om værnet om privatlivets fred, efter at det er blevet fjernet fra listen over deltagere i værnet om privatlivets fred.

5. Tilslutning til disse principper kan være begrænset a) til et niveau, der er tilstrækkeligt til at opfylde kravene med hensyn til den nationale sikkerhed, den offentlige interesse eller retshåndhævelsen, b) af love, administrative bestemmelser eller retspraksis, der medfører modstridende forpligtelser eller udtrykkelige tilladelser, såfremt foretagender 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, direktivet eller medlemsstaternes lovgivning tillader undtagelser eller dispensationer, såfremt sådanne undtagelser eller dispensationer også finder anvendelse i sammenlignelig kontekst. I overensstemmelse med det overordnede mål om at fremme beskyttelsen af privatlivets fred bør foretagenderne bestræbe sig på at gennemføre disse principper på fuldstændig og gennemskelig vis, hvilket omfatter, at de i deres program til beskyttelse af privatlivets fred angiver, på hvilke punkter eventuelle undtagelser fra principperne i henhold til ovenstående punkt b) finder generel anvendelse. Når principperne og/eller amerikansk ret giver mulighed derfor, forventes foretagenderne af samme årsag at vælge det højere beskyttelsesniveau, når det er muligt.
6. Foretagenderne er forpligtet til at anvende principperne på alle personoplysninger overført under værnet om privatlivets fred, efter at de har tilsluttet sig værnet om privatlivets fred. Et foretagende, der ønsker at udvide sin dækning under værnet om privatlivets fred 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 det foretager selvcertificering til handelsministeriet, og opfylde de krav, der er fastsat i det supplerende princip om selvcertificering.
7. Amerikansk ret finder anvendelse på fortolkningen og overholdelsen af principperne og relevante programmer til beskyttelse af privatlivets fred iværksat af foretagender i værnet om privatlivets fred, undtagen når disse foretagender 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 direktivet, som modtages fra EU af et foretagende 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 slettelse eller tilintetgørelse
 - c. »dataansvarlig«: en person eller et foretagende, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.
9. Principperne finder anvendelse fra datoen for den endelige godkendelse af Europa-Kommissionens afgørelse om et tilstrækkeligt beskyttelsesniveau.

II. PRINCIPPER

1. Oplysningspligt

- a. Et foretagende skal oplyse registrerede om:
 - i. sin deltagelse i værnet om privatlivets fred og angive et link til eller webadressen for listen over deltagere i værnet om privatlivets fred
 - ii. typer indsamlede personoplysninger og i påkommende tilfælde foretagendets enheder eller datterselskaber, der ligeledes har tilsluttet sig principperne

- iii. sit tilsagn om at anvende principperne på alle personoplysninger modtaget fra EU under værnet om privatlivets fred
 - iv. hvilke formål der ligger til grund for indsamlingen og anvendelsen af personoplysninger om de pågældende
 - v. hvorledes foretagendet 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 foretagendet tilbyder den enkelte med henblik på at begrænse anvendelsen eller videregivelsen af dennes personoplysninger
 - ix. den udpegede uafhængige tvistbilægelsesinstans, 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 tvistbilægelsesinstans i EU eller 3) en alternativ tvistbilægelsesinstans i USA
 - x. det forhold, at foretagendet 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 sagen afgøres ved bindende voldgift
 - xii. kravet om at videregive personoplysninger på grundlag af offentlige myndigheders lovlige anmodninger, herunder om at opfylde nationale sikkerheds- og retshåndhævelseskrav
 - xiii. sit ansvar for videreoverførsel til tredjemænd.
- b. Oplysningspligten skal formidles klart og tydeligt, når den enkelte første gang anmodes om at levere personoplysninger til foretagendet, eller så hurtigt som muligt derefter, dog under alle omstændigheder inden foretagendet anvender de pågældende personoplysninger til et andet formål end det, hvortil de oprindeligt blev indsamlet eller behandlet af det foretagende, der har overført oplysningerne eller videregiver dem for første gang til tredjemand.

2. Valgfrihed

- a. Et foretagende skal give den enkelte mulighed for at vælge (opt out), hvorvidt dennes personoplysninger skal 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 foretagendet og i henhold til dets instrukser. Foretagendet 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 foretagender indhente de pågældende personers udtrykkelige samtykke (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. Et foretagende skal under alle omstændigheder behandle enhver personoplysning, som det modtager fra tredjemand, som følsom, når oplysningen af den pågældende tredjemand betegnes og behandles som sådan.

3. Ansvar for videreoverførsel

- a. Et foretagende må udelukkende overføre personoplysninger til tredjemand, der handler som dataansvarlig, hvis det overholder principperne om oplysningspligt og valgfrihed. Foretagender 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 foretagendet, hvis denne fastslår ikke længere at kunne opfylde denne pligt. Det skal fremgå af aftalen, at når dette fastslås, skal den tredjemand, der handler som dataansvarlig, ophøre med behandlingen eller træffe andre rimelige og passende korrigerende foranstaltninger.
- b. Ved overførsel af personoplysninger til tredjemand, der fungerer som mellemmand, skal foretagendet: 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 foretagendets forpligtelser i henhold til principperne, iv) kræve, at mellemmanden underretter foretagendet, hvis vedkommende fastslår ikke længere at kunne opfylde sin pligt til at sikre samme beskyttelse af privatlivets fred som i principperne, v) efter varsel, inklusive under punkt iv), tage rimelige og passende skridt til at stoppe og afhjælpe uautoriseret behandling og vi) forelægge et sammendrag eller en repræsentativ kopi af de relevante bestemmelser om beskyttelse af privatlivets fred i aftalen med den pågældende mellemmand for ministeriet på anmodning.

4. Sikkerhed

- a. Foretagender, der opretter, vedligeholder, anvender eller spreder personoplysninger, skal træffe rimelige og passende foranstaltninger for at beskytte disse oplysninger mod tab, misbrug og uautoriseret adgang, videregivelse, ændring og ødelæggelse 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 ⁽¹⁾. Et foretagende 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. Et foretagende skal, i det omfang det er nødvendigt, træffe passende foranstaltninger for at sikre, at personoplysningerne er pålidelige, nøjagtige, fuldstændige og ajourførte. Et foretagende skal overholde principperne, så længe det er i besiddelse af disse oplysninger.
- b. Oplysninger kan opbevares på en måde, der gør det muligt at identificere den enkelte person eller gøre denne identificerbar ⁽²⁾, så længe de tjener et formål for behandling i den i punkt 5a anvendte betydning. Denne forpligtelse forhindrer ikke organisationer i at behandle personoplysninger i længere tid ad gangen og i det omfang, at en sådan behandling med rimelighed tjener 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 andre principper og bestemmelser i ordningen. Organisationer bør træffe rimelige og passende foranstaltninger for at overholde denne bestemmelse.

6. Indsigt

- a. Den registrerede skal have adgang til de personoplysninger, som et foretagende 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 de pågældendes privatliv, eller medmindre andre personers rettigheder herved krænkes.

⁽¹⁾ Forudsat at Kommissionens afgørelse om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred, finder anvendelse på Island, Liechtenstein og Norge, omfatter pakken vedrørende værnet om privatlivets fred både Den Europæiske Union og disse tre lande. Henvisninger til EU og EU's medlemsstater læses derfor som omfattende Island, Liechtenstein og Norge.

⁽²⁾ 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 på baggrund af konteksten for indsamlingen.

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 gøre indsigelse, hvis principperne ikke overholdes, og at det får konsekvenser for et foretagende, hvis det ikke overholder principperne. Disse mekanismer må som minimum omfatte:
 - i. let tilgængelige uafhængige indsigelsesprocedurer, 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 foretagender 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 et foretagende, der har erklæret at ville tilslutte principperne, ikke overholder disse, samt bestemmelser om sanktioner for disse foretagender. Disse sanktioner skal være af en sådan karakter, at foretagenderne tilskyndes til at overholde principperne.
- b. Foretagenderne og deres udpegede uafhængige klageinstanser skal straks besvare forespørgsler og anmodninger fra ministeriet om oplysninger vedrørende værnet om privatlivets fred. Alle foretagender skal straks besvare klager over manglende overholdelse af principperne, som EU-medlemsstaternes myndigheder henviser via ministeriet. Foretagender, der har valgt at samarbejde med databeskyttelsesmyndighederne, herunder foretagender, der behandler oplysninger om menneskelige ressourcer, skal underrette disse myndigheder direkte om undersøgelser og afgørelser af klager.
- c. Foretagender 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 det pågældende foretagende i overensstemmelse med procedurerne og på de betingelser, der er anført i bilag I.
- d. I forbindelse med videreoverførsel har et foretagende i værnet om privatlivets fred ansvaret for behandlingen af de personoplysninger, det modtager under værnet om privatlivets fred, og for efterfølgende overførsler til en tredjemand, der fungerer som mellemmand på dets vegne. Foretagendet i værnet om privatlivets fred har fortsat ansvaret i henhold til principperne, hvis dets mellemmand behandler disse personoplysninger i strid med principperne, medmindre foretagendet beviser, at det ikke er skyld i den begivenhed, der medførte skade.
- e. Når et foretagende bliver genstand for en FTC- eller domstolsafgørelse om manglende overholdelse, skal foretagendet offentliggøre alle relevante afsnit relateret til værnet om privatlivets fred i alle overholdelses- eller vurderingsrapporter forelagt FTC, i det omfang det er foreneligt med fortrolighedskrav. Ministeriet har udpeget et særligt kontaktpunkt, som databeskyttelsesmyndighederne kan rette henvendelse til, når foretagender i værnet om privatlivets fred ikke overholder principperne. FTC 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. Et foretagende skal ikke indhente udtrykkeligt samtykke (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 almennyttigt 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 et foretagendes 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 og direktivets undtagelser for journalistisk materiale 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 foretagenders 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 til værn om privatlivets fred.

3. Subsidiært ansvar

- a. Internetudbydere, teleselskaber eller andre foretagender er ikke ansvarlige i henhold til principperne til værn om privatlivets fred, når de på vegne af andre foretagender blot sender, dirigerer, omstiller eller lagrer oplysninger. Hverken direktivet eller værnet om privatlivets fred danner grundlag for subsidiært ansvar. Et foretagende kan ikke drages til ansvar, når det 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 foretagender i værnet om privatlivets fred, revideres jævnligt. Disse revisioner, navnlig revisioner, hvor der ses nærmere på eventuelle uregelmæssigheder, kan sættes på spil ved en for tidlig videregivelse. Et foretagende i værnet om privatlivets fred, 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 foretagendets legitime interesser. Disse legitime interesser omfatter overvågningen af foretagenders overholdelse af deres retlige forpligtelser og legitime regnskabsaktiviteter samt behovet for fortrolighed i forbindelse med eventuelle opkøb, fusioner, joint ventures eller lignende aktiviteter, der udføres af investeringsbanker eller revisorer.

5. Databeskyttelsesmyndighedernes rolle

- a. Foretagender skal opfylde deres forpligtelser til at samarbejde med EU's databeskyttelsesmyndigheder som beskrevet nedenfor. Amerikanske foretagender, der modtager personoplysninger fra EU, er i medfør af værnet om privatlivets fred forpligtet til at iværksætte effektive metoder, der gør dem i stand til at overholde principperne til værn om privatlivets fred. Mere specifikt skal de som fastsat i princippet om klageadgang, håndhævelse og ansvar: punkt a), nr. i), give de registrerede mulighed for at gøre indsigelse, punkt a), nr. ii), iværksætte kontrolprocedurer med henblik på at undersøge, om de lever op til deres erklæringer og løfter 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 bestemmelser om sanktioner for disse foretagender. Et foretagende kan opfylde punkt a), nr. i) og iii), i princippet om klageadgang, håndhævelse og ansvar, hvis det opfylder følgende krav med hensyn til samarbejde med databeskyttelsesmyndighederne.

- b. Et foretagende forpligter sig til at samarbejde med databeskyttelsesmyndighederne ved i sin selvcertificeringssangmældelse om tilslutning til værnet om privatlivets fred til handelsministeriet (se supplerende princip om selvcertificering) at erklære, at foretagendet agter:
- at overholde kravene i punkt a), nr. i) og iii), i princippet om klageadgang, håndhævelse og ansvar under værnet om privatlivets fred ved at forpligte sig til at samarbejde med databeskyttelsesmyndighederne
 - at samarbejde med databeskyttelsesmyndighederne med henblik på at undersøge og afgøre eventuelle klager, der modtages under værnet om privatlivets fred og
 - at rette sig efter enhver anbefaling fra databeskyttelsesmyndighederne, når de vurderer, at foretagendet skal træffe specifikke foranstaltninger for at overholde principperne til værn om privatlivets fred, herunder foretage udbedrende foranstaltninger eller betale skadeserstatning til de personer, der er berørt af den manglende overholdelse af disse principper, og at det vil give databeskyttelsesmyndigheden en skriftlig bekræftelse på, at disse foranstaltninger er truffet.
- c. Databeskyttelsesmyndighedernes paneler
- Samarbejdet med databeskyttelsesmyndighederne vil være baseret på formidling af information og anbefalinger:
 - 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.
 - Panelet vil give de berørte amerikanske foretagender anbefalinger om endnu ikke afgjorte klager fra registrerede over behandlingen af personoplysninger, der er blevet overført fra EU under værnet om privatlivets fred. Disse anbefalinger vil blive udformet med henblik på at sikre en korrekt anvendelse af principperne til værn om privatlivets fred og skal indeholde oplysninger om de retsmidler, som den eller de pågældende kan gøre brug af, og som databeskyttelsesmyndighederne finder passende.
 - Panelet vil fremsætte anbefalinger, når det får henvist en sag fra et foretagende, og/eller når det modtager en klage direkte fra registrerede over foretagender, der har forpligtet sig til at samarbejde med databeskyttelsesmyndighederne inden for rammerne af værnet om privatlivets fred, og panelet vil opfordre og om nødvendigt hjælpe de registrerede med i første omgang at anvende eventuelle interne klagemuligheder, som det pågældende foretagende tilbyder.
 - 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.
 - Panelet vil, såfremt det finder det formålstjenligt, offentliggøre resultaterne af sin behandling af klager.
 - Panelet eller de enkelte databeskyttelsesmyndigheder kan ikke drages til ansvar for panelets anbefalinger.
 - Som beskrevet ovenfor skal et foretagende, der vælger denne mulighed for bilæggelse af tvister, forpligte sig til at rette sig efter databeskyttelsesmyndighedernes anbefalinger. Hvis et foretagende ikke har rettet sig efter en anbefaling senest 25 dage efter anbefalingens afgivelse og ikke har givet nogen tilfredsstillende forklaring på denne forsikelse, vil panelet meddele, at det agter at indbringe sagen for Federal Trade Commission, 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 handelsministeriet med henblik på at få ændret listen over deltagere i værnet om privatlivets fred. Enhver misligholdelse af forpligtelsen til at samarbejde med databeskyttelsesmyndighederne og enhver overtrædelse af principperne til værn mod privatlivets fred vil kunne retsforfølges som vildledende praksis i henhold til Section 5 i Federal Trade Commission Act eller en anden tilsvarende lov.
- d. Et foretagende, der deltager i værnet om privatlivets fred og ønsker, at oplysninger om menneskelige ressourcer, der er overført fra EU inden for rammerne af et ansættelsesforhold, skal være omfattet af principperne til værn om privatlivets fred, skal forpligte sig til at samarbejde med databeskyttelsesmyndighederne om sådanne oplysninger (se det supplerende princip om oplysninger om menneskelige ressource).

- e. Foretagender, der vælger denne løsning, vil blive anmodet om at betale et årligt gebyr til dækning af panelets driftsomkostninger, og de kan derudover blive anmodet om at dække eventuelle udgifter til oversættelse, som opstår som følge af panelets behandling af henviste sager eller klager. Det årlige gebyr vil ikke overstige 500 USD og vil være mindre for små foretagender.

6. Selvcertificering

- a. Foretagendet drager fordel af værnet om privatlivets fred fra den dato, hvor ministeret har opført foretagendets anmeldelse om selvcertificering på listen over deltagere i værnet om privatlivets fred efter at have fastslået, at anmeldelsen er fuldstændig.
- b. Et foretagende skal foretage selvcertificering om tilslutning til værnet om privatlivets fred ved et fremsende en anmeldelse om selvcertificering til ministeriet underskrevet af en ledende medarbejder på vegne af det foretagende, der tilslutter sig værnet om privatlivets fred. Anmeldelsen skal som minimum indeholde følgende oplysninger:
 - i. foretagendets navn, postadresse, e-postadresse, telefon- og faxnumre
 - ii. en beskrivelse af foretagendets aktiviteter i relation til personoplysninger modtaget fra EU og
 - iii. en beskrivelse af foretagendets program til beskyttelse af privatlivets fred med hensyn til disse personoplysninger, herunder:
 - 1. Webadressen på det sted, hvor programmet til beskyttelse af privatlivets fred er tilgængeligt, hvis foretagendet har et offentligt websted, eller hvis foretagendet ikke har et offentligt websted, adressen på det sted, hvor offentligheden kan få adgang til programmet til beskyttelse af privatlivets fred
 - 2. Datoen for iværksættelse af dette program
 - 3. En kontaktadresse for behandlingen af eventuelle klager, anmodninger om indsigt og andre anliggender i forbindelse med værnet om privatlivets fred
 - 4. Det specifikke lovbestemte organ, der har kompetence til at behandle klager over foretagender 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)
 - 5. Betegnelsen på ethvert program til beskyttelse af privatlivets fred, som foretagendet deltager i
 - 6. Den pågældende kontrolmetode (f.eks. intern kontrol, tredjemandskontrol) (se supplerende princip om kontrol) og
 - 7. Den uafhængige klageinstans, der kan behandle uløste sager.
- c. Hvis et foretagende ønsker, at fordelene ved værnet om privatlivets fred også skal dække oplysninger om menneskelige ressourcer, der overføres fra EU til brug inden for rammerne af et ansættelsesforhold, kan det foretage sådanne overførsler, hvis der findes et lovbestemt organ, der har kompetence til at behandle klager over det pågældende foretagende vedrørende oplysninger om menneskelige ressourcer, og som er anført i principperne eller i et fremtidigt bilag til principperne. Desuden skal foretagendet anføre dette i sin anmeldelse om selvcertificering og angive, at det 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 det agter at følge disse myndigheders anbefalinger. Foretagendet skal også fremsende en kopi af sit program til beskyttelse af oplysninger om menneskelige ressourcer til ministeriet og oplyse, hvor de berørte medarbejdere kan få adgang til programmet til beskyttelse af privatlivets fred.
- d. Ministeriet vil oprette listen over de foretagender, der har fremsendt fuldstændige anmeldelser om selvcertificering, hvorved de sikres fordelene ved værnet om privatlivets fred, og ministeriet vil ajourføre denne liste på grundlag af de årlige anmeldelser om selvrecertificering og meddelelser, der modtages i overensstemmelse med det supplerende princip om bilæggelse af tvister og håndhævelse. Sådanne selvcertificeringsanmeldelser skal fremsendes mindst én gang om året. I modsat fald vil foretagendet blive slettet fra listen over deltagere i værnet om privatlivets fred, og det kan ikke længere drage fordel af værnet om privatlivets fred. Både listen over deltagere i værnet om privatlivets fred og foretagendernes selvcertificeringsanmeldelser vil være offentligt tilgængelige. Alle foretagender, som ministeriet opfører på listen over deltagere i værnet om privatlivets fred, skal

i deres relevante offentliggjorte programmer til beskyttelse af privatlivets fred, angive, at de tilslutter sig principperne til værn mod privatlivets fred. Hvis et foretagendes program til beskyttelse af privatlivets fred er tilgængeligt online, skal det derudover indeholde et hyperlink til ministeriets websted for værn om privatlivets fred samt et hyperlink til webstedet og klageformular for den uafhængige klageinstans, der kan behandle uløste sager.

- e. Principperne om privatlivets fred finder anvendelse straks efter certificering. Det anerkendes, at principperne vil få indvirkning på forretningsforbindelserne med tredjemand, og foretagender, som certificerer deres deltagelse i ordningen for værn om privatlivets fred de to første måneder efter iværksættelsen af værn, skal bringe deres forretningsforbindelser med tredjemand i overensstemmelse med princippet om ansvar for videreoverførsel så hurtigt som muligt og under alle omstændigheder senest ni måneder fra datoen for certificering af deres deltagelse i værn om privatlivets fred. I den mellemliggende periode skal foretagender, der overfører oplysninger til tredjemand, i) anvende principperne om oplysningspligt og valgfrihed og ii) bekræfte, at mellemmanden er forpligtet til at sikre mindst samme beskyttelse som i principperne, når personoplysninger overføres til en tredjemand, der fungerer som mellemmand.
- f. Et foretagende skal anvende principperne til værn om privatlivets fred på alle personoplysninger modtaget fra EU under værn om privatlivets fred. Tilslutningen til principperne til værn om privatlivets fred er ikke tidsbegrænset med hensyn til de personoplysninger, der modtages i den periode, hvor foretagendet drager fordel af værn om privatlivets fred. Hvis et foretagende først har tilsluttet sig principperne, skal det fortsat anvende dem på sådanne oplysninger, så længe det lagrer, anvender eller videre giver oplysningerne, også selv om det af en hvilken som helst grund efterfølgende forlader værn om privatlivets fred. Et foretagende, som ønsker at trække sig ud af værn om privatlivets fred, men ønsker at beholde oplysningerne, skal hvert år bekræfte over for ministeriet, at det fortsat vil anvende principperne 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 Europa-Kommissionen har godkendt). I modsat fald skal foretagendet tilbagesende eller slette oplysningerne. Et foretagende, der trækker sig ud af værn om privatlivets fred, skal fjerne alle henvisninger til værn om privatlivets fred i relevante programmer til beskyttelse af privatlivets fred, der lader formode, at foretagendet fortsat deltager aktivt i værn om privatlivets fred og er berettiget til at drage fordel heraf.
- g. Et foretagende, der som følge af en fusion eller en overtagelse ophører med at eksistere som særskilt retlig enhed, skal på forhånd underrette handelsministeriet herom. Foretagendet skal i denne meddelelse ligeledes angive, om den enhed, der overtager foretagendet, eller den enhed, der opstår som følge af fusionen, i) i henhold til de gældende lovbestemmelser om overtagelser eller fusioner fortsat vil være bundet af principperne til værn om privatlivets fred eller ii) vælger på grundlag af selvcertificering at tilslutte sig principperne til værn om privatlivets fred eller iværksætter andre sikkerhedsforanstaltninger, herunder skriftlige aftaler, der sikrer overholdelse af principperne til værn om privatlivets fred. Hvis hverken i) eller ii) finder anvendelse, skal enhver oplysning, som foretagendet har modtaget inden for rammerne af værn om privatlivets fred, straks slettes.
- h. Når et foretagende forlader værn om privatlivets fred af en eller anden årsag, skal det fjerne alle erklæringer, der lader formode, at foretagendet fortsat deltager i værn om privatlivets fred eller er berettiget til at drage fordel af værn om privatlivets fred. Certificeringsmærket for værn om privatlivets fred skal ligeledes fjernes, hvis det anvendes. Et foretagende, der afgiver urigtige oplysninger til offentligheden vedrørende dets tilslutning til principperne til værn om privatlivets fred, kan indbringes for FTC eller andre kompetente regeringsorganer. Et foretagende, der afgiver urigtige oplysninger til ministeriet, kan retsforfølges efter False Statements Act (18 U.S.C. § 1001).

7. Kontrol (verifikation)

- a. Foretagender 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 rammerne af værn om privatlivets fred, og om disse foranstaltninger er blevet iværksat som beskrevet og i overensstemmelse med principperne til værn om beskyttelse af privatlivets fred.
- b. For at opfylde kontrolkravene i princippet om klageadgang, håndhævelse og ansvar skal et foretagende kontrollere sådanne erklæringer og løfter ved hjælp af selvevaluering eller ekstern kontrol af overholdelsen.
- c. Det skal i tilfælde af selvevaluering kontrolleres, om foretagendets offentliggjorte program til beskyttelse af privatlivets fred vedrørende personoplysninger, der modtages fra EU, er i overensstemmelse med de faktiske forhold, og om det er dækkende, fuldstændigt iværksat og tilgængeligt samt offentliggjort i tilstrækkeligt omfang. Det skal ligeledes fremgå af denne kontrol, om programmet til beskyttelse af privatlivets fred er i overensstemmelse med principperne til værn om privatlivets fred, om de registrerede er informeret om eventuelle interne muligheder for klagebehandling og om de eksterne uafhængige klageinstanser, som de har adgang til, om det pågældende foretagende har udarbejdet procedurer for uddannelse af de ansatte

i gennemførelsen af disse foranstaltninger og for at gribe ind, hvis de ikke overholder foranstaltningerne, samt om foretagendet har interne procedurer for regelmæssigt og objektivt at kontrollere ovenstående. Mindst én gang om året skal en ledende medarbejder eller en anden bemyndiget repræsentant for foretagendet 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 overtrædelse af principperne.

- d. Hvis et foretagende har valgt at anvende ekstern kontrol af overholdelsen, skal denne kontrol påvise, at foretagendets program til beskyttelse af privatlivets fred vedrørende personoplysninger, der modtages fra EU, er i overensstemmelse med principperne til værn mod privatlivets fred, at foretagendet efterlever dette, og at registrerede oplyses om klagemulighederne. Kontrolmetoderne kan uden begrænsning omfatte revision, uvarslet kontrol, anvendelsen af fiktive oplysninger («decoys») eller passende teknologiske midler. Mindst én gang om året skal kontrollanten, en ledende medarbejder eller en anden bemyndiget repræsentant for foretagendet 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. Foretagender skal føre protokol over iværksættelsen af deres databeskyttelsesforanstaltninger inden for rammerne af værnet om privatlivets fred og gøre denne protokol tilgængelig efter anmodning derom i forbindelse med en undersøgelse eller en klage over overtrædelse af principperne til det uafhængige organ, som er ansvarlig for at undersøge klager, eller til den myndighed, der har kompetence i sager om illoyal eller vildledende praksis. Foretagenderne skal ligeledes straks besvare forespørgsler og andre anmodninger om oplysninger fra ministeriet om foretagendets tilslutning til principperne.

8. Indsigt

a. Princippet om indsigt i praksis

- i. I henhold til principperne til værn om privatlivets fred 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 et foretagende behandler personoplysninger om dem ⁽¹⁾
 2. få udleveret oplysningerne, således at de kan kontrollere nøjagtigheden heraf og behandlingens lovlighed og
 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. Foretagender, 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 foretagendet f.eks. indgå i en dialog med den pågældende for bedre at kunne forstå motiverne for anmodningen og give de relevante oplysninger. Foretagendet kan anmode om at få oplyst, hvilke(n) del(e) af foretagendet den pågældende har haft med at gøre, eller hvilken slags oplysninger (eller anvendelse) der er genstand for anmodningen om indsigt.
- iii. Foretagender 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 foretagendet bortredigere de beskyttede oplysninger og give indsigt i de andre oplysninger. Hvis et foretagende beslutter at begrænse indsigten i personoplysninger i særlige tilfælde, skal det 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.

⁽¹⁾ 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 behandlingstidspunkt 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.

- 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 foretagendet 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 uforholdsmæssig 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 et foretagende give indsigt i disse oplysninger.

c. Fortrolige forretningsoplysninger

- i. Fortrolige forretningsoplysninger er oplysninger, som et foretagende har truffet foranstaltninger for at beskytte imod videregivelse, fordi en sådan videregivelse ville være til fordel for en konkurrent på markedet. Foretagender 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 foretagendet har udarbejdet, eller andres fortrolige forretningsoplysninger, når disse oplysninger i henhold til en aftale skal behandles fortroligt.
- ii. Hvis fortrolige forretningsoplysninger nemt kan adskilles fra andre oplysninger, hvori der anmodes om indsigt, skal foretagendet bortredigere de fortrolige forretningsoplysninger og give indsigt i de ikke-fortrolige oplysninger.

d. Organisering af databaser

- i. Et foretagende kan give indsigt ved at aflevere de relevante personoplysninger til de pågældende personer, som således ikke skal have adgang til foretagendets database.
- ii. Der skal kun gives indsigt i det omfang, et foretagende lagrer oplysningerne. Princippet om indsigt forpligter i sig selv ikke et foretagende til at opbevare, vedligeholde, organisere eller omstrukturere registre med personoplysninger.

e. Begrænset indsigt

- i. Da foretagender 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 direktivet kan et foretagende 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. vanskeliggør 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. er til skade for den nødvendige fortrolige behandling af oplysninger i forbindelse med overvågning, kontrol eller regulering inden for rammerne af en god forvaltning eller under kommende eller igangværende forhandlinger, som foretagendet er involveret i.
- ii. Et foretagende, 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 et foretagende behandler personoplysninger om den pågældende. En registreret har ret til at få udleveret sine personoplysninger. Et foretagende 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

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

h. Svigagtige anmodninger om indsigt

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

i. Svarfrist

Foretagender bør besvare anmodninger om indsigt inden for en rimelig frist og på en rimelig måde, som er let forståelig for den registrerede. Et foretagende, der regelmæssigt leverer oplysninger til registrerede, kan besvare en individuel anmodning om indsigt i forbindelse med foretagendets regelmæssige fremsendelse af oplysninger, hvis det ikke medfører en for stor forsinkelse.

9. **Oplysninger om menneskelige ressourcer**

a. Anvendelsesområdet for værnet om privatlivets fred

- i. Når en virksomhed 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, et associeret foretagende eller et ikkeassocieret foretagende, som deltager i værnet om privatlivets fred, er overførslen underlagt dette værn. 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 til værn om privatlivets fred 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. Et amerikansk foretagende, der inden for rammerne af værnet om privatlivets fred 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 et amerikansk foretagende f.eks. agter at anvende personoplysninger, der er indsamlet i forbindelse med et ansættelsesforhold, til ikke-ansættelsesrelaterede formål, f.eks. til markedsføringshenvendelser, skal det først give de berørte personer den nødvendige valgfrihed, medmindre de allerede har tilladt anvendelsen af oplysningerne til sådanne formål. Denne anvendelse må ikke være uforenelige 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 til at straffe de pågældende ansatte.

- ii. Det skal bemærkes, at visse bestemmelser, der generelt finder anvendelse på overførsel af personoplysninger fra visse 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. Et foretagende 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 det pågældende foretagendes muligheder for at foretage forfremmelser eller udnævnelser eller behandle andre personaleanliggender af lignende karakter.

c. Anvendelse af princippet om indsigt

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. Et foretagende, der behandler denne type oplysninger i USA, er i henhold til værnet om privatlivets fred 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 foretagendet 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 det amerikanske foretagende, der har modtaget oplysningerne fra arbejdsgiveren, og således medfører et formodet brud på principperne til værn af privatlivets fred. 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. Et amerikansk foretagende, der deltager i værnet om privatlivets fred 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 til værn om privatlivets fred, 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 for ansvar for videreoverførsel

I forbindelse med lejlighedsvis ansættelsesrelaterede operationelle behov i foretagendet i værnet om privatlivets fred for at overføre personoplysninger under værnet om privatlivets fred, 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 videreoverførsel, forudsat at foretagendet i værnet om privatlivets fred har overholdt principperne om oplysningspligt og valgfrihed.

10. **Obligatoriske aftaler om videreoverførsel**

a. Aftaler om behandling af oplysninger

- i. Uanset databehandlerens deltagelse i værnet om privatlivets fred 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 værnet om privatlivets fred. 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 ikke-autoriseret adgang og ved, om videreoverførsel er tilladt og
3. tager hensyn til behandlingens karakter, bistår den dataansvarlige med at besvare anmodninger fra registrerede, der udøver deres rettigheder under principperne.

- iii. Da deltagerne i værnet om privatlivets fred anses for at give en tilstrækkelig beskyttelse, kræver aftaler med sådanne deltagere, der udelukkende vedrører behandling af oplysninger, ingen forudgående tilladelse (eller også gives sådanne tilladelser automatisk af EU-medlemsstaterne), hvilket til gengæld kræves i forbindelse med aftaler med modtagere, der ikke deltager i værnet om privatlivets fred, eller som på anden vis ikke giver en tilstrækkelig beskyttelse.

b. Overførsler i en kontrolleret gruppe af selskaber eller enheder

Når personoplysninger overføres mellem to dataansvarlige i en kontrolleret gruppe af selskaber eller enheder, er det ikke altid nødvendigt at etablere en kontakt 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 koncerninterne instrumenter (f.eks. overholdelses- og kontrolprogrammer), der sikrer kontinuitet i beskyttelsen af personoplysninger i henhold til principperne til værn om privatlivets fred. I forbindelse med disse overførsler har foretagendet i værnet om privatlivets fred fortsat ansvaret for, at principperne til værn om privatlivets fred overholdes.

c. Overførsler mellem dataansvarlige

I forbindelse med overførsler mellem dataansvarlige behøver den modtagende dataansvarlige ikke deltage i værnet om privatlivets fred eller have en uafhængig klageinstans. Foretagendet i værnet om privatlivets fred skal indgå en aftale med den modtagende dataansvarlige tredjemand, der sikrer samme beskyttelsesniveau som under værnet om privatlivets fred, men den dataansvarlige tredjemand behøver ikke deltage i værnet om privatlivets fred eller have en uafhængig klageinstans, forudsat at tredjemanden stiller en tilsvarende mekanisme til rådighed.

11. Bilægelse af tvister og håndhævelse

- a. Kravene til håndhævelse af værnet om privatlivets fred fastsættes i princippet om klageadgang, håndhævelse og ansvar. Det fastsættes i det supplerende princip om kontrol, hvorledes kravene i princippet punkt a), nr. ii), skal overholdes. Dette supplerende princip omhandler punkt a), nr. i) og iii), hvor der stilles krav om uafhængige klageinstanser. Ordningen kan håndhæves ved hjælp af forskellige mekanismer, der dog alle skal opfylde kravene i princippet om klageadgang, håndhævelse og ansvar. Et foretagende kan opfylde kravene: i) ved at overholde programmer til beskyttelse af privatlivets fred udviklet i den private sektor og baseret på principperne til værn om privatlivets fred, 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 venligst, at kravene i princippet om klageadgang, håndhævelse og

ansvar supplerer kravet om, at selvregulering skal kunne håndhæves efter Section 5 i Federal Commission Act, der forbyder illoyal eller vildledende praksis, eller en anden lov derom.

- c. Foretagender og deres uafhængige klageinstanser skal tilvejebringe oplysninger om værnet om privatlivets fred, når ministeriet anmoder herom, for at medvirke til at sikre, at de påfylder deres forpligtelser under værnet om privatlivets fred, og for at lette forvaltningen af programmet. Foretagender 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 foretagendet vil afhjælpe problemet. Ministeriet vil beskytte modtagne fortrolige oplysninger i overensstemmelse med amerikansk ret.

d. Klageinstanser

- i. Forbrugerne skal opfordres til først at klage til det pågældende foretagende, inden de indbringer deres klage for uafhængige klageinstanser. Foretagenderne skal svare forbrugeren senest 45 dage efter modtagelse af klagen. En klageinstans er navnlig uafhængig, hvis den er upartisk, hvis der er åbenhed omkring sammensætningen og finansieringen, eller 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. Tvistbilæggesinstanser skal behandle hver enkelt klage, som de modtager fra registrerede, medmindre klagerne tydeligt er ubegrundede eller chikanerende. 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 til værn om privatlivets fred. 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 til værn om privatlivets fred og om de tjenester, de tilvejebringer under værnet om privatlivets fred, på deres offentlige websteder. Disse oplysninger skal omfatte: 1) oplysninger om eller et link til kravene vedrørende uafhængige klageinstanser i henhold til principperne til værn om privatlivets fred, 2) et link til ministeriets websted for værnet om privatlivets fred, 3) oplysninger om, at deres tvistbilægges-tjenester under værnet om privatlivets fred er gratis for registrerede, 4) oplysninger om indgivelse af klager vedrørende værnet om privatlivets fred, 5) oplysninger om tidsrammen for behandling af klager vedrørende værnet om privatlivets fred 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 relateret til værnet om privatlivets fred modtaget i rapporteringsåret, 2) de modtagne typer klager, 3) kvalitetsmål for tvistbilægges såsom klagebehandlingstid og 4) resultaterne af de modtagne klager, navnlig antal og typer pålagte retsmidler eller 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 et foretagende i værnet om privatlivets fred 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 værnet om privatlivets fred. Denne mulighed for voldgift giver udelukkende panelet i værnet om privatlivets fred (der består af en eller tre voldgiftsmænd som aftalt af 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 afhjælpe overtrædelsen af principperne i forhold til de registrerede. Registrerede og foretagender i værnet om privatlivets fred har adgang til domstolsprøvelse og håndhævelse af voldgiftsafgørelser i henhold til amerikansk ret under Federal Arbitration Act.

⁽¹⁾ Foretagendet bør 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.

e. Retsmidler og sanktioner

Anvendelsen af de retsmidler, som tvistbilægelsesinstansen giver adgang til, bør resultere i, at det pågældende foretagende så vidt muligt udbedrer konsekvenserne af den manglende overholdelse, og at foretagendets 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 tilstrækkelig strenge til at få foretagendet til at overholde principperne. Tvistbilægelsesinstanser 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 slette oplysninger⁽¹⁾. Andre sanktioner kan være suspendering eller tilbagestrækning af en godkendelse, betaling af skadeserstatning til registrerede for tab som følge af en overtrædelse af principperne og forbud eller påbud. Tvistbilægelsesinstanser og selvregulerende instanser i den private sektor skal underrette den kompetente statslige instans eller i påkommende tilfælde domstolene samt ministeriet om foretagender i værnet om privatlivets fred, der ikke efterlever deres afgørelser.

f. Federal Trade Commissions (FTC) behandling af klager

FTC har forpligtet sig til at give højeste prioritet til behandling af sager om påstået manglende overholdelse af principperne, som den får henvist fra i) selvregulerende instanser med kompetence inden for beskyttelse af privatlivets fred og andre uafhængige tvistbilægelsesinstanser, ii) EU-medlemsstaterne, og iii) ministeriet, for at fastslå, om Section 5 i FTC 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 (federal district court), hvilket, såfremt klageren får medhold, kan resultere i retsafgørelse med samme indhold truffet af forbundsdomstolen. Dette omfatter falske påstande om tilslutning til principperne til værn om privatlivets fred eller deltagelse i værnet om privatlivets fred fremsat af foretagender, der ikke længere er opført på listen over deltagere i værnet om privatlivets fred 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 iværksætter indleder. Ministeriet opfordrer de øvrige regeringsorganer til at underrette ministeriet om den endelige afgørelse i sådanne sager eller om andre afgørelser om tilslutning til principperne til værn om privatlivets fred.

g. Vedvarende overtrædelse af principperne

- i. Hvis et foretagende vedvarende overtræder principperne, kan det ikke længere drage fordel af værnet om privatlivets fred. Foretagender, der vedvarende overtræder principperne, vil blive fjernet fra listen over deltagere i værnet om privatlivets fred af ministeriet, og de skal tilbagesende eller slette modtagne personoplysninger under værnet om privatlivets fred.
- ii. En vedvarende overtrædelse af principperne forekommer, når et foretagende, der har foretaget selvcertificering over for ministeriet, nægter at rette sig efter den endelige afgørelse truffet af en uafhængig selvregulerende tvistbilægelsesinstans med kompetence inden for beskyttelse af privatlivets fred eller af en statslig instans, eller når en sådan instans fastslår, at et foretagende hyppigt har overtrådt principperne i et sådant omfang, at det ikke længere er rimeligt at påstå, at det overholder principperne. Foretagendet skal i så fald straks underrette ministeriet derom. Et foretagende, der ikke opfylder denne forpligtelse, kan retsforfølges efter False Statements Act (18 U.S.C. § 1001). Et foretagende, der trækker sig fra et selvreguleringsprogram til beskyttelse af privatlivets fred eller fra en uafhængig selvregulerende tvistbilægelsesinstans 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 foretagendet selv, fra en selvregulerende instans med kompetence inden for beskyttelse af privatlivets fred, fra en anden uafhængig tvistbilægelsesinstans eller fra en statslig instans, fjerne

⁽¹⁾ Afsnit I.5 i principperne.

foretagendet fra listen over deltagere i værnet om privatlivets fred, dog først efter at have givet det pågældende foretagende en frist på 30 dage og en mulighed for at svare. Det vil således tydeligt fremgå af den offentligt tilgængelige liste fra handelsministeriet (eller dets repræsentant), hvilke foretagender der er eller ikke er dækket af værnet om privatlivets fred.

- iv. Et foretagende, der ønsker at tilslutte sig en selvregulerende instans med henblik på igen at kvalificere sig til værnet om privatlivets fred, skal give denne instans fuldstændige oplysninger om sin tidligere deltagelse i værnet om privatlivets fred.

12. Valgfrihed (choice) 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 (opt-out) ikke at lade sine personoplysninger anvende til direkte markedsføring. Det pågældende foretagende kan dog fastsætte passende tidsfrister for denne valgfrihed, f.eks. for at have tid til at indføre dette fravalg i systemet. Et foretagende kan ligeledes anmode om tilstrækkelige oplysninger for at bekræfte identiteten på den person, der ønsker at vælge fra. I USA kan fysiske personer gøre brug af denne valgfrihed ved hjælp af en central fravalgsordning, f.eks. Direct Marketing Association's Mail Preference Service. Foretagender, der deltager i denne Direct Marketing Association's Mail Preference Service, skal oplyse forbrugere, der ikke ønsker at modtage kommercielle oplysninger, om denne mulighed. Den registrerede skal under alle omstændigheder nemt og uden uforholdsmæssig store omkostninger kunne gøre brug af denne valgfrihed.
- b. På samme måde kan et foretagende 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 foretagendet 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 foretagendet 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 foretagender uden for EU i flere forskellige tilfælde. Personoplysninger kan i henhold til direktivets artikel 26 »videregives til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2«, i) hvis det er nødvendigt for at kunne yde de tjenester, kunden anmoder om, eller for at honorere en aftale, f.eks. en »frequent flyer«-aftale, eller ii) hvis kunden har givet udtrykkelig tilladelse dertil. Amerikanske foretagender, der tilslutter sig værnet om privatlivets fred, giver en tilstrækkelig beskyttelse af personoplysninger og kan derfor modtage dataoverførsler fra EU uden at opfylde disse krav eller andre krav i direktivets artikel 26. Eftersom værnet om privatlivets fred 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 deltagere i værnet om privatlivets fred. Det foretagende, der overfører oplysninger, skal dog under alle omstændigheder overholde lovgivningen i de EU-medlemsstater, hvor det udøver sine aktiviteter, hvilket bl.a. kan medføre særlige krav til behandlingen af følsomme oplysninger.

14. Farmaceutiske og medicinske produkter

- a. Anvendelse af EU-Medlemsstaternes lovgivning eller principperne til værn om privatlivets fred

EU-medlemsstaternes lovgivning finder anvendelse på indsamlingen af personoplysninger og på enhver behandling, der foretages forud for overførslen til USA. Principperne til værn om privatlivets fred 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 oplysninger indsamlet til et bestemt forskningsprojekt overføres til et foretagende i USA omfattet af værnet om privatlivets fred, kan foretagendet 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

Deltagere kan til enhver tid beslutte eller blive anmodet om at trække sig ud af et klinisk forsøg. Enhver personoplysning, 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

Virksomheder, der fremstiller farmaceutiske eller medicinske anordninger, må levere 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 en sådan adgang til oplysningerne om deres behandling under forsøget, hvis de fik oplyst denne begrænsning ved tilmeldingen til forsøget, og hvis videregivelsen af sådanne oplysninger vil 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 det sponsorerende foretagende.

f. Produktsikkerhed og kontrol

En virksomhed, der fremstiller farmaceutiske eller medicinske anordninger, behøver ikke anvende principperne til værn om privatlivets fred om oplysningspligt, valgfrihed og ansvar for videreoverførsel og indsigt i sine produktsikkerheds- og kontrolaktiviteter, herunder meddelelse om negative konstateringer og registreringen 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

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 denne måde, vil ikke udgøre en overførsel af personoplysninger, der er underlagt principperne til værn om privatlivets fred.

15. Oplysninger i offentlige registre og offentligt tilgængelige oplysninger

- a. Et foretagende skal anvende principperne i værnet om privatlivets fred 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. registre hos statsorganer eller statslige enheder på ethvert niveau, som er offentligt tilgængeligt.
- b. Det er ikke nødvendigt at anvende princippet om oplysningspligt, valgfrihed eller ansvar for videreoverførsel på oplysninger i offentlige registre, såfremt de ikke sammenføres med oplysninger i ikke-offentlige registre, og såfremt alle betingelser for indsigt, der fastsættes af den kompetente myndighed, overholdes. Det er generelt heller ikke nødvendigt at anvende princippet om oplysningspligt, valgfrihed eller ansvar for videreoverførsel på offentligt tilgængelige oplysninger, medmindre den europæiske dataafsender meddeler, at de pågældende oplysninger er underlagt begrænsninger, der kræver, at det pågældende foretagende anvender disse principper til de tilsigtede formål. Foretagender er ikke ansvarlige for den måde, hvorpå disse oplysninger anvendes af andre, der indhenter oplysningerne fra offentliggjort materiale.
- c. Foretagender vil blive udelukket fra værnet om privatlivets fred, 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 anførte ovenfor), skal et foretagende 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 i tilfælde af oplysninger, der allerede er offentligt tilgængelige, såfremt disse oplysninger ikke er sammenført med oplysninger, der ikke er offentligt tilgængelige. Foretagender, 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 det foretagende, 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 foretagender i værnet om privatlivets fred 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 foretagenderne i værnet om privatlivets fred tilvejebringer i disse rapporter, samt oplysninger offentliggjort af de amerikanske efterretningstjenester og andre oplysninger kan anvendes i den årlige fælles evaluering af, om værnet om privatlivets fred fungerer i overensstemmelse med principperne.
 - c. Manglende overholde af oplysningspligten i henhold til punkt a), nr. xii), i princippet om oplysningspligt forhindrer eller forringer et foretagendes mulighed for at besvare en lovlig anmodning.
-

*Bilag I***Voldgiftsmodel**

I dette bilag I angives de betingelser, på hvilke foretagender i værnet om privatlivets fred 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's og USA's værn om privatlivets fred. 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 mekanismer i værnet om privatlivets fred.

A. Anvendelsesområde

Den registrerede har adgang til voldgift i forbindelse med øvrige krav for at få afgjort, om et foretagende i værnet om privatlivets fred 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 værnet om privatlivets fred.

B. Tilgængelige retsmidler

Denne mulighed for voldgift giver udelukkende panelet i værnet om privatlivets fred (der består af en eller tre voldgiftsmænd som aftalt af 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 afhjælpe overtrædelser af principperne i forhold til de registrerede. Dette er voldgiftspanelets eneste beføjelser, for så vidt angår retsmidler. Panelet skal tage højde for andre retsmidler, der allerede er blevet pålagt gennem andre mekanismer i værnet om privatlivets fred, 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 at kræve voldgift, skal træffe følgende foranstaltninger inden indgivelse af en begæring om voldgift: 1) rette direkte henvendelse til foretagendet og fremføre den påståede overtrædelse og give foretagendet mulighed for at løse problemet inden for den tidsramme, der er anført i afsnit III.11, d), nr. i) i principperne, 2) gøre brug af den uafhængige klageinstans i henhold til principperne, og 3) rejse sagen gennem den pågældendes databeskyttelsesmyndighed over for handelsministeriet og give handelsministeriet 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 EU-databeskyttelsesmyndighed 1) er bemyndiget i henhold til afsnit III.5 eller III.9 i principperne, eller 2) er bemyndiget til at rette direkte henvendelse til foretagendet 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. Voldgiftsavgørelser 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⁾ Afsnit I.5 i principperne.

E. Domstolsprøvelse og håndhævelse

Registrerede og foretagender i værnet om privatlivets fred har adgang til domstolsprøvelse og håndhævelse af voldgiftsafgørelser i henhold til amerikansk ret under Federal Arbitration Act (⁽¹⁾). Disse sager skal indbringes for den forbundsdomstol (federal district court), inden for hvis jurisdiktion hovedforretningsstedet for foretagendet i værnet om privatlivets fred 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 fra den nedenstående liste over voldgiftsmænd.

I overensstemmelse med gældende ret vil det amerikanske handelsministerium og Europa-Kommissionen udarbejde en liste med mindst 20 voldgiftsmænd valgt på baggrund af deres uafhængighed, integritet og ekspertise. Processen er som følger:

Voldgiftsmænd:

- 1) er opført på listen i en periode på tre år, der ekstraordinært kan forlænges i yderligere tre år
- 2) må ikke modtage instrukser fra eller være tilknyttet nogen part eller noget foretagende i værnet om privatlivets fred, 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.

G. Voldgiftsprocedurer

I henhold til gældende ret skal det amerikanske handelsministerium og Europa-Kommissionen senest seks måneder efter vedtagelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet nå til enighed om en række eksisterende veletablerede amerikanske voldgiftsprocedurer (f.eks. AAA eller JAMS), som skal finde anvendelse på sager, der indbringes for panelet i værnet om privatlivets fred, 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 foretagendet. 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.

(¹) 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. juni 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, forholdet 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 opstået 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.

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 beslutter, at dette i den specifikke voldgiftssag ville føre til uberettigede eller uforholdsmæssige omkostninger.
7. Materiale forelagt voldgiftsmænd vil blive fortroligt behandlet 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 leveringen af meddelelsen til det pågældende foretagende, medmindre parter aftaler andet.

H. Omkostninger

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

Under iagttagelse af gældende ret vil handelsministeriet etablere en fond, der skal finansieres via årlige bidrag fra foretagenderne i værnet om privatlivets fred, som til dels er baseret på foretagendets størrelse, og fonden vil dække voldgiftsomkostningerne, herunder voldgiftsmændenes honorarer, op til maksimumsbeløb i samråd med Europa-Kommissionen. Fonden vil blive forvaltet af en tredjemand, der regelmæssigt vil rapportere om fondens drift. I forbindelse med den årlige evaluering vil handelsministeriet og Europa-Kommissionen evaluere fondens drift, herunder behovet for at justere bidragene eller maksimumsbeløbene, og vil bl.a. se på antallet af voldgiftssager, voldgiftsomkostningerne og behandlingstiden ud fra en fælles forståelse af, at foretagenderne i værnet om privatlivets fred ikke må pålægges en urimelig stor økonomisk byrde. Advokatsalærer er ikke omfattet af denne bestemmelse eller nogen fond under denne bestemmelse.

BILAG III

Brev fra den amerikanske udenrigsminister John Kerry

Den 7. juli 2016

Kære kommissær Věra Jourová,

Jeg glæder mig over, at vi er nået til enighed om EU's og USA's værn om privatlivets fred, som kommer til at omfatte en ombudsmandsmekanisme, hvorigennem myndighederne i EU kan indgive anmodninger på vegne af privatpersoner i EU om amerikansk signalefterretningspraksis.

Den 17. januar 2014 annoncerede præsident Barack Obama en række vigtige efterretningsreformer, som er indeholdt i Presidential Policy Directive 28 (PPD-28). I medfør af PPD-28 har jeg udpeget viceminister Catherine A. Novelli, der også er Senior Coordinator for International Information Technology Diplomacy, som vores kontaktpunkt for udenlandske regeringer, der ønsker at rejse spørgsmål om amerikanske signalefterretningsaktiviteter. Jeg har udvidet denne funktion ved at oprette en ombudsmandsmekanisme i værnet om privatlivets fred på de vilkår, som er fastlagt i bilag A, og som er blevet ajourført siden mit brev af 22. februar 2016. Jeg har anmodet viceminister Catherine A. Novelli om at påtage sig denne opgave. Viceminister Novelli er uafhængig af de amerikanske efterretningstjenester og refererer direkte til mig.

Jeg har anmodet mit personale om at afsætte de nødvendige ressourcer til at gennemføre denne nye ombudsmandsmekanisme, og jeg er sikker på, at mekanismen vil være et effektivt redskab, som kan imødegå EU-borgernes bekymringer.

Med venlig hilsen

John F. Kerry

Bilag A

Ombudsmandsmekanismen i EU's og USA's værn om privatlivets fred Signalefterretning

I erkendelse af betydningen af ordningen for EU's og USA's værn om privatlivets fred redegøres i dette memorandum for processen til gennemførelse af en ny mekanisme i henhold til Presidential Policy Directive 28 (PPD-28) om signalefterretninger ⁽¹⁾.

Den 17. januar 2014 holdt præsident Obama en tale, hvor han annoncerede vigtige efterretningsreformer. Han understregede i denne tale, at »vores indsats ikke blot bidrager til at beskytte vores nation, men også vores venner og allierede. Vores indsats vil kun være effektiv, hvis almindelige mennesker i andre lande har tillid til, at USA også respekterer deres privatliv«. Præsident Obama annoncerede udstedelsen af et nyt præsidentielt direktiv, PPD-28, der »skal beskrive klart, hvad vi gør og ikke gør, når det kommer til oversøisk overvågning«.

I medfør af Section 4(d) i PPD-28 skal den amerikanske udenrigsminister udpege en »Senior Coordinator for International Information Technology Diplomacy« (seniorkoordinator), der skal »[...] være kontaktpunkt for udenlandske regeringer, der ønsker at rejse spørgsmål om amerikanske signalefterretningsaktiviteter«. Viceminister C. Novelli har været seniorkoordinator siden januar 2015.

I dette memorandum redegøres for en ny mekanisme, som seniorkoordinatoren skal anvende for at lette behandlingen af anmodninger om adgang til oplysninger overført fra EU til USA til nationale sikkerhedsformål under værnet om privatlivets fred eller i henhold til standardkontraktbestemmelser, bindende virksomhedsregler, »undtagelser« ⁽²⁾ eller »mulige fremtidige undtagelser« ⁽³⁾ gennem de kanaler, der er fastlagt i gældende amerikanske love og politikker, og for at lette besvarelsen af disse anmodninger.

- 1. Ombudsmanden i værnet om privatlivets fred** Seniorkoordinatoren vil fungere som ombudsmanden i værnet om privatlivets fred og i relevant omfang udpege yderligere embedsmænd i det amerikanske udenrigsministerium, der skal hjælpe seniorkoordinatoren med at varetage de opgaver, der redegøres for i detaljer i dette memorandum (i det følgende vil koordinatoren og embedsmænd, der varetager sådanne opgaver, blive benævnt »ombudsmanden i værnet om privatlivets fred«). Ombudsmanden i værnet om privatlivets fred vil arbejde tæt sammen med relevante embedsmænd i andre ministerier og agenturer med ansvar for behandling af anmodninger i henhold til gældende amerikanske love og politikker. Ombudsmanden er uafhængig af efterretningstjenesterne. Ombudsmanden indberetter direkte til den amerikanske udenrigsminister, der sørger for, at ombudsmanden udøver sin funktion på objektiv vis og fri for indflydelse, som kan påvirke de svar, der skal gives.
- 2. Effektiv koordinering** Ombudsmanden i værnet om privatlivets fred har mulighed for at gøre effektiv brug af og koordinere med de nedenfor beskrevne tilsynsorganer for at sikre, at ombudsmandens svar på anmodninger, som

⁽¹⁾ Forudsat at Kommissionens afgørelse om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred, finder anvendelse på Island, Liechtenstein og Norge, omfatter pakken vedrørende værnet om privatlivets fred både Den Europæiske Union og disse tre lande. Henvisninger til EU og EU's medlemsstater læses derfor som omfattende Island, Liechtenstein og Norge.

⁽²⁾ I denne sammenhæng skal »undtagelser« forstås som en eller flere kommercielle overførsler, som finder sted på betingelse af, at: a) der ikke hersker tvivl om, at den registrerede har givet sit samtykke, eller b) videregivelsen er nødvendig af hensyn til opfyldelsen af en kontrakt mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan kontrakt, eller c) videregivelsen er nødvendig af hensyn til indgåelsen eller udførelsen af en kontrakt, der i den registreredes interesse er indgået mellem den registeransvarlige og tredjemand, eller d) videregivelsen er nødvendig eller følger af lov eller bestemmelser fastsat med hjemmel i lov for at beskytte en vigtig samfundsinteresse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares, eller e) videregivelsen er nødvendig for at beskytte den registreredes vitale interesser, eller f) videregivelsen finder sted fra et offentligt register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri, i det omfang de ved lov fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde.

⁽³⁾ I denne sammenhæng skal »fremtidige mulige undtagelser« forstås som en eller flere kommercielle overførsler, som finder sted på en af følgende betingelser, i det omfang betingelsen udgør en lovlig grund til overførsel af personoplysninger fra EU til USA: a) den registrerede udtrykkelig har givet samtykke til den foreslåede overførsel efter at være blevet informeret om de mulige risici, som sådanne overførsler kan medføre for den registrerede på grund af den manglende afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller fornødne garantier, eller b) overførslen er nødvendig for at beskytte den registreredes eller andre personers vitale interesser, hvis den registrerede ikke fysisk eller juridisk er i stand til at give samtykke, eller c) en overførsel til et tredjeland eller en international organisation, hvor ingen af de andre undtagelser eller fremtidige mulige undtagelser finder anvendelse, og hvis overførslen ikke er gentagen, kun vedrører et begrænset antal registrerede, er nødvendig for, at den dataansvarlige kan forfølge vægtige legitime interesser, medmindre den registreredes interesser, grundlæggende rettigheder og frihedsrettigheder går forud herfor, og den dataansvarlige har vurderet samtlige de forhold, der har indflydelse på dataoverførslen, og på grundlag af denne vurdering yder de passende garantier for beskyttelsen af personoplysninger.

indgives af det organ med ansvar for behandling af klager fra personer i EU, baseres på de nødvendige oplysninger. Når en anmodning vedrører overvågningens forenelighed med amerikansk lovgivning, vil ombudsmanden i værnet om privatlivets fred kunne samarbejde med en af de uafhængige tilsynsorganer med undersøgelsesbeføjelser.

- a. Ombudsmanden i værnet om privatlivets fred vil arbejde tæt sammen med andre embedsmænd i ministerierne og agenturerne, herunder med uafhængige tilsynsorganer, for at sikre, at udfyldte anmodninger behandles og besvares i henhold til gældende amerikanske love og politikker. Ombudsmanden i værnet om privatlivets fred har mulighed for i relevant omfang at koordinere tæt med Office of the Director of National Intelligence, det amerikanske justitsministerium og andre ministerier og agenturer, der beskæftiger sig med amerikanske nationale sikkerhedsanliggender, generalinspektører, Freedom of Information Act Officers og databeskyttelsesansvarlige (civil liberties and privacy officers).
- b. Den amerikanske regering vil anvende mekanismerne for koordinering af og tilsyn med nationale sikkerhedsanliggender på tværs af ministerier og agenturer for at medvirke til at sikre, at ombudsmanden i værnet om privatlivets fred i henhold til punkt 4, e), har mulighed for at besvare udfyldte anmodninger i henhold til punkt 3, b).
- c. Ombudsmanden i værnet om privatlivets fred kan indbringe spørgsmål relateret til anmodninger for Privacy and Civil Liberties Oversight Board.

3. Indgivelse af anmodninger

- a. En anmodning indgives først til de tilsynsmyndigheder i medlemsstaterne, der fører tilsyn med nationale sikkerhedstjenester og/eller offentlige myndigheders behandling af personoplysninger. Anmodningen indgives til ombudsmanden af en centraliseret EU-instans (i det følgende samlet benævnt »EU-klageinstansen for individuelle klager«).
- b. EU-klageinstansen for individuelle klager vil sikre, at anmodningen er udfyldt, ved at:
 - i) kontrollere den pågældendes identitet, og at den pågældende handler på egne vegne og ikke som repræsentant for en regering eller et mellemstatsligt foretagende
 - ii) sikre, at anmodningen indgives skriftlig, og at den indeholder følgende grundlæggende oplysninger:
 - alle oplysninger, der danner grundlag for klagen
 - oplysninger om karakteren af oplysningerne og den ønskede afhjælpning
 - oplysninger om eventuelle amerikanske statslige enheder, der menes at være involveret
 - oplysninger om andre iværksatte tiltag med henblik på at få udleveret de ønskede oplysninger eller den ønskede afhjælpning og om udfaldet af disse tiltag
 - iii) kontrollere, at anmodningen vedrører oplysninger, der med rimelighed kan antages at være overført fra EU til USA under værnet om privatlivets fred eller i henhold til standardkontraktbestemmelser, bindende virksomhedsregler, undtagelser eller mulige fremtidige undtagelser
 - iv) træffe en foreløbig beslutning om, at anmodningen ikke er useriøs, chikanerende eller indgivet i ond tro.
- c. Da den udfyldte anmodning skal behandles af ombudsmanden i værnet om privatlivets fred, er det ikke nødvendigt at dokumentere i anmodningen, at den amerikanske regering rent faktisk har haft adgang til den anmodende parts oplysninger gennem signalefterretningsaktiviteter.

4. Tilsagn om kommunikation med den indgivende EU-klageinstans for individuelle klager

- a. Ombudsmanden i værnet om privatlivets fred anerkender modtagelsen af anmodningen over for den indgivende EU-klageinstans for individuelle klager.
- b. Ombudsmanden i værnet om privatlivets fred foretager en foreløbig gennemgang for at kontrollere, at anmodninger er udfyldt i overensstemmelse med punkt 3, b). Hvis ombudsmanden i værnet om privatlivets fred konstaterer mangler eller har spørgsmål vedrørende udfyldningen af anmodningen, vil ombudsmanden i værnet om privatlivets fred forsøge at løse disse problemer i samarbejde med den indgivende EU-klageinstans for individuelle klager.

- c. Hvis ombudsmanden i værnet om privatlivets fred har brug for yderligere oplysninger om anmodningen af hensyn til behandlingen, eller hvis den person, der oprindeligt indgav anmodningen, skal gøre yderligere tiltag, underretter ombudsmanden i værnet om privatlivets fred den indgivende EU-klageinstans for individuelle klager herom.
 - d. Ombudsmanden i værnet om privatlivets fred følger status for anmodninger og holder den indgivende EU-klageinstans for individuelle klager ajour.
 - e. Når en anmodning er udfyldt som beskrevet i punkt 3 i dette memorandum, skal ombudsmanden i værnet om privatlivets fred give den indgivende EU-klageinstans for individuelle klager et rettidigt og passende svar under hensyntagen til den vedvarende forpligtelse til at beskytte oplysninger i henhold til gældende love og politikker. Ombudsmanden i værnet om privatlivets fred vil give den indgivende EU-klageinstans for individuelle klager et svar, hvor det bekræftes, i) at klagen er blevet behørigt undersøgt, og ii) at amerikanske love, præsidentielle dekretter, præsidentielle direktiver og agenturernes politikker, hvormed de begrænsninger og garantier, der er redegjort for ODNI-brevet, er blevet indført, er blevet overholdt, eller at den manglende overholdelse er blevet afhjulpet i tilfælde af en overtrædelse. Ombudsmanden i værnet om privatlivets fred vil hverken bekræfte eller benægte, at den pågældende har været et overvågningsmål, og ombudsmanden i værnet om privatlivets fred vil heller ikke oplyse, hvilket specifikt retsmiddel der blev anvendt. Som nærmere beskrevet i punkt 5 behandles FOIA-anmodninger som foreskrevet i denne lov og gældende bestemmelser.
 - f. Ombudsmanden i værnet om privatlivets fred skal kommunikere direkte med EU-klageinstansen for individuelle klager, som herefter skal varetage kommunikationen med den person, der indgiver anmodningen. Hvis direkte henvendelser er et led i en af de nedenfor beskrevne »underliggende processer«, vil disse henvendelser ske i overensstemmelse med gældende procedurer.
 - g. Tilsagnene i dette memorandum finder ikke anvendelse på generelle påstande om, at EU's og USA's værn om privatlivets fred er i strid med EU-databeskyttelseskrav. Tilsagnene i dette memorandum er afgivet ud fra Europa-Kommissionens og den amerikanske regerings fælles erkendelse af, at der kan opstå ressourcebegrænsninger, herunder i forbindelse med anmodninger under Freedom of Information Act (FOIA), i lyset af omfanget af afgivne tilsagn i dette memorandum. Hvis varetagelsen af ombudsmanden i værnet om privatlivets freds opgaver overstiger rimelige ressourcemæssige begrænsninger og hindrer opfyldelsen af disse tilsagn, vil den amerikanske regering drøfte relevante justeringer, som kunne afhjælpe situationen, med Europa-Kommissionen.
5. **Anmodninger om oplysninger.** Anmodninger om indsigt i amerikanske offentlige myndigheders optegnelser indgives og behandles i medfør af Freedom of Information Act (FOIA).
- a. Enhver kan henholde sig til FOIA som et middel til at søge indsigt i de amerikanske forbundsorganers eksisterende optegnelser, uanset den anmodende parts nationalitet. Denne lov er kodificeret i United States Code 5 U.S.C. § 552. Loven og yderligere oplysninger om FOIA er tilgængelige på adressen: www.foia.gov og <http://www.justice.gov/oip/foia-resources>. Det enkelte agentur har en Chief FOIA Officer og har offentliggjort oplysninger på sit offentlige websted om, hvordan FOIA-anmodninger indgives til agenturet. Agenturerne har indført procedurer for kommunikation agenturerne imellem i forbindelse med FOIA-anmodninger om optegnelser i flere agenturer.
 - b. Eksempler:
 - i) Office of the Director of National Intelligence (ODNI) har oprettet ODNI FOIA Portal for ODNI: <http://www.dni.gov/index.php/about-this-site/foia>. Denne portal indeholder oplysninger om indgivelse af anmodninger, opfølgning på status for en eksisterende anmodning og om adgang til oplysninger, der er blevet frigivet og offentliggjort af ODNI under FOIA. ODNI FOIA-indeholder link til andre FOIA-websteder for efterretningsenheder: <http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites>.
 - ii) Det amerikanske justitsministeriums Office of Information Policy tilvejebringer omfattende oplysninger om FOIA: <http://www.justice.gov/oip>. Der er ikke kun tale om oplysninger om indgivelse af FOIA-anmodninger til justitsministeriet, idet webstedet ligeledes indeholder retningslinjer til den amerikanske regering om fortolkningen og anvendelsen af FOIA-krav.

- c. Indsigt i de amerikanske offentlige myndigheders optegnelser er omfattet af visse anførte undtagelser i FOIA. Disse omfatter begrænsninger for adgang til klassificerede informationer om national sikkerhed, tredjemands personoplysninger og oplysninger om retshåndhævende efterforskninger og kan sammenlignes med de begrænsninger, som de enkelte EU-medlemsstater pålægger i deres egne offentlighedslove. Disse begrænsninger gælder både for amerikanere og ikkeamerikanere.
- d. Tvister om udlevering af optegnelser udbedt i medfør af FOIA kan påklages administrativt og herefter ved forbundsdomstolene. Domstolen skal træffe en de novo-afgørelse om, hvorvidt optegnelserne tilbageholdes lovligt, 5 U.S.C. § 552(a)(4)(B), og kan tvinge offentlige myndigheder til at give adgang til optegnelser. I nogle tilfælde har domstolene ophævet myndighedernes afgørelser om tilbageholdelse af oplysninger som klassificerede informationer. Selv om der ikke gives økonomisk erstatning, kan domstolen tilkende et beløb til dækning af advokatsalær.
6. **Anmodninger om yderligere foranstaltninger.** En anmodning med påstand om en lovovertrædelse eller anden embedsmisbrug vil blive henvist til det kompetente amerikanske regeringsorgan, herunder uafhængige tilsynsorganer, med beføjelser til at undersøge den pågældende anmodning og gribe ind over for manglende overholdelse som beskrevet nedenfor.
- a. Inspectors General (generalinspektører) er lovmæssigt uafhængige, de har brede beføjelser til at foretage undersøgelser, revisioner og kontrol af programmer, herunder af svig og misbrug eller overtrædelse af loven, og de kan anbefale korrigerende foranstaltninger.
- i) Federal Inspectors General (IG) (føderale generalinspektører) blev oprettet ved Inspector General Act of 1978 som ændret som uafhængige og objektive enheder i de fleste agenturer, og de har til opgave at bekæmpe ødselhed, svig og misbrug i deres respektive agenturers programmer og operationer. IGERne har i denne forbindelse ansvaret for at gennemføre revisioner og undersøgelser af deres respektive agenturers programmer og operationer. Derudover varetager de ledelses- og koordineringsopgaver og anbefaler politikker for aktiviteter til fremme af sparsommelighed, produktivitet og effektivitet og forebyggelse og afsløring af svig og misbrug i agenturernes programmer og operationer.
- ii) Hver efterretningsenhed har sit eget Office of the Inspector General (generalinspektørens kontor) med ansvar for tilsyn med bl.a. udenlandske efterretningsaktiviteter. Der er blevet offentliggjort en række rapporter fra generalinspektørerne om efterretningsprogrammer.
- iii) Eksempler:
- Office of the Inspector General of the Intelligence Community (IC IG) blev oprettet i medfør af Section 405 i Intelligence Authorization Act of Fiscal Year 2010. IC IG har ansvaret for at gennemføre revisioner, undersøgelser, inspektioner og kontroller af alle amerikanske efterretningstjenester med henblik på at identificere og afhjælpe systemiske risici, sårbarheder og mangler på tværs af agenturerne med det formål at fremme efterretningstjenesternes besparende foranstaltninger og effektivitet. IC IG har beføjelser til at undersøge klager eller oplysninger om påstande om overtrædelser af love og bestemmelser, ødselhed, svig eller magtmisbrug eller en alvorlig eller specifik fare for den offentlige sundhed og sikkerhed i forbindelse med ODNI's og/eller IC-efterretningsprogrammer og -aktiviteter. IC IG har anført direkte kontaktoplysninger til indgivelse af en rapport på sit websted: <http://www.dni.gov/index.php/about-this-site/contact-the-ig>.
- Office of the Inspector General (OIG) i det amerikanske justitsministerium (ministeriet) er en uafhængig enhed oprettet ved lov, der har til opgave at afsløre og forebygge ødselhed, svig, misbrug og embedsmisbrug i ministeriets programmer og blandt personalet og at fremme sparsommelighed og effektivitet i disse programmer. OIG undersøger påståede overtrædelser af straffe- og civilretlige bestemmelser begået af ministeriets ansatte og reviderer og undersøger ligeledes ministeriets programmer. OIG har kompetence til at behandle alle klager over embedsmisbrug begået af ministeriets ansatte, herunder Federal Bureau of Investigation, Drug Enforcement Administration, Federal Bureau of Prisons, U. S. Marshals Service, Bureau of Alcohol, Tobacco, Firearms, and Explosives, United States Attorneys Offices og ansatte i andre afdelinger eller kontorer i justitsministeriet (den eneste undtagelse er, at påstande om

embedsmisbrug begået af en af ministeriets advokater eller retshåndhævelsesmedarbejdere relateret til udøvelsen af advokatens beføjelser til at efterforske, føre retssager eller yde rådgivning, henhører under ministeriets Office of Professional Responsibility). I henhold til Section 1001 i USA Patriot Act, der blev undertegnet den 26. oktober 2001, skal generalinspektøren gennemgå oplysninger og modtage klager med påstand om krænkelse af borgerlige rettigheder og borgerlige frihedsrettigheder begået af justitsministeriets ansatte. OIG har et offentligt websted — <https://www.oig.justice.gov> — med en »Hotline« til indgivelse af klager — <https://www.oig.justice.gov/hotline/index.htm>.

b. Den amerikanske regerings kontorer og enheder med ansvar for beskyttelse af privatlivets fred og borgerlige rettigheder har ligeledes vigtige ansvarsområder: Eksempler:

- i) I medfør af Section 803 i Implementing Recommendations of the 9/11 Commission Act of 2007, kodificeret i United States Code 42 U.S.C. § 2000ee-1, er der udpeget databeskyttelsesansvarlige (privacy and civil liberties officers) i visse ministerier og agenturer (herunder udenrigsministeriet, justitsministeriet og ODNI). Det præciseres i Section 803, at disse databeskyttelsesansvarlige skal være hovedrådgivere, bl.a. for at sikre, at ministeriet, agenturet eller enheden har indført passende procedurer for behandling af klager fra personer, der påstår, at ministeriet, agenturet eller enheden har krænket deres privatliv eller borgerlige rettigheder.
- ii) ODNI's Civil Liberties and Privacy Office (ODNI CLPO) ledes af ODNI Civil Liberties Protection Officer, en stilling, der blev oprettet ved National Security Act fra 1948 som ændret. ODNI CLPO har bl.a. til opgave at sikre, at efterretningsenhedernes politikker og procedurer i tilstrækkelig grad sikrer privatlivets fred og borgerlige rettigheder, og at gennemgå og undersøge klager med påstand om misbrug eller krænkelse af borgerlige rettigheder og privatlivets fred i ODNI's programmer og aktiviteter. ODNI CLPO har lagt oplysninger ud til offentligheden på sit websted, herunder om indgivelse af klager: www.dni.gov/clpo. Når ODNI CLPO modtager en klage over krænkelse af privatlivets fred eller borgerlige rettigheder, der involverer IC-programmer og -aktiviteter, koordinerer kontoret de amerikanske efterretningstjenesters videre behandling af klagen med andre IC-enheder. Bemærk, at National Security Agency (NSA) ligeledes har et Civil Liberties and Privacy Office, der oplyser om kontorets ansvarsområder på sit websted: https://www.nsa.gov/civil_liberties/. Hvis oplysningerne indikerer, at et agentur ikke opfylder kravene om beskyttelse af privatlivets fred (f.eks. et krav i Section 4 i PPD-28), har agenturerne instanser, der skal sikre, at principperne overholdes og undersøge og afhjælpe hændelsen. Agenturerne skal indberette tilfælde af manglende overholdelse i henhold til PPD-28 til ODNI.
- iii) Office of Privacy and Civil Liberties (OPCL) i det amerikanske justitsministerium bistår ministeriets Chief Privacy and Civil Liberties Officer (CPCLO) med dennes officielle opgaver og ansvarsområder. OPCL's vigtigste opgave er at beskytte den amerikanske befolknings privatliv og borgerlige rettigheder gennem kontrol af, tilsyn med og koordinering af ministeriets aktiviteter til beskyttelse af privatlivets fred. OPCL yder juridisk rådgivning og vejledning til ministeriets enheder, sikrer, at ministeriet opfylder bestemmelserne om beskyttelse af privatlivets fred, herunder i Privacy Act of 1974, bestemmelserne om beskyttelse af privatlivets fred i E-Government Act fra 2002 og Federal Information Security Management Act samt administrationens politiske direktiver udstedt i forbindelse med disse love, udvikler og afholder kurser om beskyttelse af privatlivets fred i ministeriet, bistår CPCLO ved udarbejdelsen af ministeriets politik for beskyttelse af privatlivets fred, udarbejder rapporter om beskyttelse af privatlivets fred til præsidenten og den amerikanske kongres og gennemgår ministeriets praksis for håndtering af oplysninger for at sikre, at denne praksis er forenelig med beskyttelsen af privatlivets fred og borgerlige rettigheder. OPCL har lagt oplysninger ud til offentligheden om sine ansvarsområder på adressen: <http://www.justice.gov/opcl>.
- iv) I henhold til 42 U.S.C. § 2000ee et seq. skal Privacy and Civil Liberties Oversight Board løbende gennemgå i) ministeriernes, agenturerne og enhederne inden for den udøvende magts politikker og procedurer og gennemførelsen heraf, for så vidt angår foranstaltninger til at beskytte nationen mod terrorisme med det formål at sikre, at privatlivets fred og borgerlige rettigheder beskyttes, og ii) den udøvende magts andre foranstaltninger desangående med det formål at vurdere, om disse foranstaltninger beskytter privatlivets fred og borgerlige rettigheder behørigt, og om de er i overensstemmelse med gældende love, bestemmelser og politikker til beskyttelse af privatlivets fred og borgerlige rettigheder. Rådet skal ligeledes modtage og gennemgå rapporter og andre oplysninger modtaget fra de databeskyttelsesansvarlige (privacy and civil liberties officers) og i påkommende tilfælde udstede anbefalinger til dem om deres aktiviteter. I henhold til Section 803 i Implementing Recommendations of the 9/11 Commission Act of 2007, kodificeret i 42 U.S.C. § 2000ee-1, skal de databeskyttelsesansvarlige i otte føderale agenturer (herunder forsvarsministeren, ministeren for Homeland Security, direktøren for National Intelligence og direktøren for Central Intelligence

Agency) og ethvert andet agentur udpeget af PCLOB indgive periodiske rapporter til PCLOB, herunder om antallet og karakteren af og afgørelsen på de klager, som det pågældende agentur har modtaget over påståede krænkelse. I henhold til PCLOB's bemyndigelseslov skal rådet modtage disse rapporter og i påkommende tilfælde udstede anbefalinger til de databeskyttelsesansvarlige om deres aktiviteter.

BILAG IV

Brev fra formanden for den føderale handelskommission, Federal Trade Commission, Edith Ramirez

Den 7. juli 2016

VIA E-MAIL

Věra Jourová
Kommissær for retlige anliggender, forbrugere og ligestilling mellem mænd og kvinder
Europa-Kommissionen
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
Belgien

Kære kommissær Věra Jourová,

United States Federal Trade Commission (»FTC«) glæder sig over at få lejlighed til at redegøre for sin håndhævelse af den nye ordning for EU's og USA's værn om privatlivets fred (»ordningen for værnet om privatlivets fred« eller »ordningen«). Vi tror, at ordningen vil komme til at 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. FTC har længe haft fokus på at beskytte privatlivets fred på tværs af grænser og vil prioritere håndhævelsen af den nye ordning højt. Vi redegør nedenfor for FTC's historik med hensyn til at sikre en stærk håndhævelse af beskyttelsen af privatlivets fred generelt, herunder for vores håndhævelse af det oprindelige safe harbor-program og for FTC's tilgang til håndhævelse af den nye ordning.

FTC forpligtede sig første gang offentligt til at håndhæve safe harbor-programmet i 2000. FTC's daværende formand Robert Pitofsky sendte på dette tidspunkt et brev til Europa-Kommissionen, hvori han redegjorde for FTC's tilsagn om at håndhæve safe harbor-principperne til beskyttelse af privatlivets fred strengt. FTC opfylder stadig dette tilsagn gennem næsten 40 håndhævelsessager, en lang række yderligere undersøgelser og samarbejde med individuelle europæiske databeskyttelsesmyndigheder (»EU's databeskyttelsesmyndigheder«) om spørgsmål af fælles interesse.

Efter at Europa-Kommissionen i november 2013 gav udtryk for bekymringer over forvaltningen og håndhævelsen af safe harbor-programmet, indledte vi sammen med det amerikanske handelsministerium drøftelser med tjenestemænd fra Europa-Kommissionen for at undersøge, hvordan vi kunne styrke ordningen. Sideløbende med disse drøftelser traf EU-Domstolen den 6. oktober 2015 en afgørelse i Schrems-sagen, der bl.a. gjorde Europa-Kommissionens beslutning om tilstrækkeligheden af safe harbor-programmet ugyldig. Efter denne afgørelse fortsatte vi vores tætte samarbejde med det amerikanske handelsministerium og Europa-Kommissionen i et forsøg på at styrke beskyttelsen af personers privatliv i EU. Ordningen for værnet om privatlivets fred er resultatet af disse løbende drøftelser. Som det var tilfælde i forbindelse med safe harbor-programmet forpligter FTC sig hermed til at håndhæve den nye ordning stramt. Dette brev understreger dette tilsagn.

Vi bekræfter navnlig vores tilsagn på fire hovedområder: 1) prioritering af henviste sager og undersøgelser, 2) håndtering af falske eller vildledende påstande om deltagelse i værnet om privatlivets fred, 3) løbende overvågning af overholdelsen af afgørelser og 4) øget inddragelse af og samarbejde med EU's databeskyttelsesmyndigheder. Vi redegør nedenfor i detaljer for de enkelte tilsagn og den relevante baggrund for FTC's rolle i beskyttelsen af forbrugernes privatliv og håndhævelsen af safe harbor og for de generelle regler om beskyttelse af privatlivets fred i USA ⁽¹⁾.

I. BAGGRUND**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 om beskyttelsen og sikkerheden af forbrugeroplysninger. Den vigtigste lov, som FTC håndhæver, FTC

⁽¹⁾ Der er yderligere oplysninger om den amerikanske lovgivning om beskyttelse af personoplysninger på forbunds- og delstatsniveau i bilag A og en sammenfatning af vores nylige håndhævelsessager til beskyttelse af privatlivets fred og datasikkerheden på FTC's websted på adressen: <https://www.ftc.gov/reports/privacy-data-security-update-2015>.

Act, forbyder »illoyal« eller vildledende adfærd eller praksis i forbindelse med handel ⁽¹⁾. En erklæring, en udeladelse eller en praksis er vildledende, hvis den er væsentlig og kan antages at vildlede forbrugere, der handler fornuftigt under omstændighederne ⁽²⁾. En adfærd eller praksis betegnes som illoyal, hvis den medfører eller kan antages at ville medføre en betydelig skade for forbrugerne, der ikke på rimelig vis kan undgås, og som ikke opvejes af andre fordele for forbrugerne eller den almindelige konkurrencesituation ⁽³⁾. 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's kompetence under FTC Act omfatter anliggender »i forbindelse med handel«. 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 ⁽⁴⁾. I nogle tilfælde falder FTC's kompetence sammen med andre retshåndhavende organers kompetence.

Vi har udviklet et stærkt samarbejde med forbunds- og delstatsmyndighederne og samarbejder tæt med disse myndigheder om koordineringen af undersøgelser eller henvisning af sager, når det er relevant.

Håndhævelse er grundpillen i FTC's tilgang til beskyttelse af privatlivets fred. FTC har indtil dato anlagt over 500 sager om beskyttelsen og sikkerheden af forbrugeroplysninger. Disse sager omfatter både offline- og onlineinformation og håndhævelsessager anlagt mod store og små virksomheder med påstand om, at de ikke har slettet følsomme forbrugeroplysninger korrekt, ikke har sikret forbrugeres personoplysninger, har sporet forbrugere online på ulovlig vis, spammet forbrugere, installeret spyware eller anden malware på forbrugeres computere, overtrådt »Do Not Call«-reglerne og andre telemarketingsregler og uretmæssigt har indsamlet og udvekslet forbrugeroplysninger på mobilenheder. FTC's håndhævelsessager — både i den fysiske og digitale verden — sender et vigtigt budskab til virksomheder om behovet for at beskytte forbrugernes privatliv.

FTC har ligeledes iværksat flere politiske initiativer med det formål at øge beskyttelsen af forbrugernes privatliv, som er grundlaget for disse håndhævelsesforanstaltninger. FTC har afholdt workshopper og offentliggjort rapporter med anbefalinger om bedste praksis med henblik på at øge beskyttelsen af privatlivets fred i det mobile økosystem, øge gennemsigtigheden inden for datamægling, maksimere fordelene ved »big data« og afbøde risiciene, navnlig for lavindkomstforbrugere og underforsynede forbrugere, og understrege konsekvenserne af bl.a. ansigtsgenkendelse og tingenes internet for privatlivets fred og sikkerheden.

FTC har også fokus på oplysning af forbrugerne og virksomhederne med det formål at øge indvirkningen af FTC's håndhævelse og politikudviklingsinitiativer. FTC har anvendt en række forskellige redskaber — publikationer, onlineresourcer, workshopper og sociale medier — til at tilvejebringe undervisningsmateriale om en bred vifte af emner, herunder mobile apps, beskyttelse af børns privatliv og datasikkerhed. FTC har senest lanceret sit »Start With Security«-initiativ, der omfatter nye retningslinjer til virksomheder og bygger på erfaringerne fra FTC's sager om datasikkerhed og på en række workshopper i hele landet. FTC har desuden længe været i front med hensyn til at oplyse forbrugerne om grundlæggende computersikkerhed. Sidste år havde vores websted OnGuard Online og den spanske udgave Alerta en Línea over 5 mio. sidevisninger.

B. Retsbeskyttelse til gavn for EU-forbrugere

Ordningen kommer til at fungere inden for rammerne af de generelle regler om beskyttelse af privatlivets fred, som beskytter forbrugerne på forskellige måder.

⁽¹⁾ 15 U.S.C. § 45(a).

⁽²⁾ Se FTC Policy Statement on Deception, knyttet som bilag til Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), tilgængelig på adressen: <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

⁽³⁾ Se 15 U.S.C. § 45(n), FTC Policy Statement on Unfairness, knyttet som bilag til Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), tilgængelig på adressen: <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

⁽⁴⁾ Se California Dental Ass'n v. FTC, 526 U.S. 756 (1999).

Forbuddet i FTC Act mod illoyal eller vildledende adfærd eller praksis beskytter ikke kun amerikanske forbrugere mod amerikanske foretagender, da loven ligeledes omfatter praksis, der 1) forårsager eller vil kunne forårsage skade i USA, som med rimelighed kan forudses, 2) involverer den faktiske adfærd i USA. FTC kan desuden anvende alle tilgængelige retsmidler til beskyttelse af amerikanske forbrugere, herunder genoprejsning (restitution), til beskyttelse af udenlandske forbrugere.

FTC's håndhævelsesarbejde er rent faktisk til stor fordel for både amerikanske og udenlandske forbrugere. Vores sager om håndhævelse af Section 5 i FTC Act har f.eks. både beskyttet amerikanske og udenlandske forbrugeres privatliv. I en sag mod en informationsformidler, Accusearch, hævdede FTC, at virksomhedens salg af fortrolige optagelser af telefonsamtaler til tredjemænd uden forbrugernes viden eller samtykke var en illoyal praksis, der var i strid med Section 5 i FTC Act. Accusearch solgte oplysninger om både amerikanske og udenlandske forbrugere ⁽¹⁾. Domstolen udstedte et forbud mod Accusearch, bl.a. mod markedsføring eller salg af forbrugeres personoplysninger uden skriftligt samtykke, medmindre oplysningerne var lovligt indsamlede offentligt tilgængelige oplysninger, og fastslog, at virksomheden skulle tilbagebetale en fortjeneste på næsten 200 000 USD ⁽²⁾.

FTC's forlig med TRUSTe er et andet eksempel. Det sikrer, at forbrugere, herunder forbrugere i EU, kan have tillid til globale selvregulerende instansers erklæringer om kontrol og certificering af nationale og udenlandske onlinetjenester ⁽³⁾. Det skal understreges, at vores retssag mod TRUSTe ligeledes styrker selvreguleringssystemet til beskyttelse af privatlivets fred mere generelt ved at sikre, at enheder, som spiller en vigtig rolle i selvreguleringsordninger, herunder grænseoverskridende ordninger, drages til ansvar.

FTC håndhæver ligeledes andre relevante love, hvis bestemmelser også finder anvendelse på ikke-amerikanske 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. Ud over de amerikanske forbundslove, der håndhæves af FTC, kan der være andre love om beskyttelse af forbrugerne og privatlivets fred på forbunds- og delstatsniveau, som sikrer EU-forbrugere yderligere fordele.

C. Håndhævelse af safe harbor-principperne

Som led i sit program for håndhævelse af beskyttelsen af privatlivets fred og sikkerheden har FTC ligeledes grebet ind for at beskytte EU-forbrugere ved at anlægge sager om overtrædelser af safe harbor-ordningen. FTC har anlagt 39 håndhævelsessager vedrørende safe harbor-ordningen: 36 sager om påståede falske påstande om certificering og tre sager — mod Google, Facebook og Myspace — om påståede overtrædelser af safe harbor-principperne ⁽⁴⁾. Disse sager viser, at certificeringer kan håndhæves, og at manglende overholdelse har konsekvenser. 20-årige forligsafgørelser pålægger Google, Facebook og Myspace at gennemføre omfattende programmer til beskyttelse af privatlivets fred, der i rimeligt omfang skal være udformet med henblik på at afhjælpe risici for udviklingen og forvaltningen af nye og eksisterende produkter og tjenester og beskytte sikkerheden og fortroligheden af personoplysninger. De omfattende programmer til beskyttelse af privatlivets fred, der skal gennemføres i medfør af disse forligsafgørelser, skal identificere væsentlige risici og omfatte kontroller til imødegåelse af disse risici. Virksomhederne skal ligeledes indsende løbende uafhængige vurderinger af deres programmer til beskyttelse af privatlivets fred til FTC. Disse afgørelser forbyder ligeledes disse virksomheder at afgive urigtige oplysninger om deres databeskyttelsesforanstaltninger og deltagelse i programmer til

⁽¹⁾ Se Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Office of the Privacy Commissioner of Canada indgav et amicus curiae-indlæg i forbindelse med appellen af FTC-sagen og foretog sin egen undersøgelse, hvor konklusionen var, at Accusearchs praksis ligeledes var en overtrædelse af canadisk ret.

⁽²⁾ Se *FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

⁽³⁾ Se *In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (afgørelse og kendelse), tilgængelig på adressen: <https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf>.

⁽⁴⁾ Se *In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13 2011) (afgørelse og kendelse), tilgængelig på adressen: <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>, *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (afgørelse og kendelse), tilgængelig på adressen: <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>, *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (afgørelse og kendelse), tilgængelig på adressen: <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace>.

beskyttelse af privatlivets fred og sikkerheden. Dette forbud gælder ligeledes for virksomhedernes adfærd og praksis under den nye ordning for værnet om privatlivets fred. FTC kan håndhæve disse afgørelser ved at henvise sagen til domstolene med henblik på idømmelse af civile retlige sanktioner. Google blev rent faktisk idømt en rekordstor bøde på 22,5 mio. USD i 2012 for overtrædelse af afgørelsen. Disse FTC-afgørelser medvirker således til at beskytte over 1 mia. forbrugere i hele verden, heraf flere hundrede millioner i Europa.

Der har ligeledes været fokus på falske eller vildledende påstande om deltagelse i safe harbor-ordningen i FTC's sager. FTC tager disse påstande alvorligt. I sagen FTC mod Karnani anlagde FTC f.eks. sag i 2011 mod en internetudbyder i USA med påstand om, at udbyderen og udbyderens virksomhed narrede britiske forbrugere til at tro, at virksomheden var baseret i Det Forenede Kongerige, herunder ved brug af uk-domænenavne og henvisninger til den britiske valuta og det britiske postvæsen ⁽¹⁾. Da forbrugerne modtog produkterne, opdagede de imidlertid, at der var uventede importafgifter, garantier, som ikke var gyldige i Det Forenede Kongerige, og omkostninger forbundet med at få pengene tilbage. FTC gjorde ligeledes gældende, at de sagsøgte førte forbrugerne bag lyset med hensyn til deres deltagelse i safe harbor-programmet. Det skal understreges, at alle de berørte forbrugere var bosiddende i Det Forenede Kongerige.

Mange af vores andre sager om håndhævelse af safe harbor-ordningen involverede foretagender, som havde tilsluttet sig safe harbor-ordningen, men fortsatte med at fremstille sig selv som medlemmer uden at forny den årlige certificering. Som nærmere beskrevet nedenfor sætter FTC også ind over for falske påstande om deltagelse i værnet om privatlivets fred. Denne strategiske håndhævelsesaktivitet supplerer handelsministeriets øgede indsats for at kontrollere overholdelsen af programkravene om certificering og recertificering, dets overvågning af den effektive overholdelse, herunder ved brug af spørgeskemaer til deltagere i ordningen, og dets øgede indsats for at identificere falske påstande om deltagelse i ordningen og misbrug af ordningens certificeringsmærke ⁽²⁾.

II. PRIORITERING AF HENVISTE SAGER OG UNDERSØGELSER

Som under safe harbor-ordningen vil FTC give højeste prioritet til sager under værnet om privatlivets fred, der henvises fra EU-medlemsstaterne. Vi vil ligeledes prioritere sager om manglende overholdelse af retningslinjer for selvregulering relateret til ordningen for værnet om privatlivets fred, der henvises fra selvregulerende instanser med kompetence inden for beskyttelse af privatlivets fred og andre uafhængige tvistbilæggesinstanser.

For at lette henvisningen af sager under ordningen fra EU-medlemsstaterne er FTC ved at udvikle 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 vil i denne forbindelse udpege 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 henvisning fra en EU-medlemsstat eller en selvregulerende instans kan FTC træffe en række forskellige foranstaltninger i forhold til de henviste sager. Vi kan f.eks. gennemgå virksomhedens programmer til beskyttelse af privatlivets fred, indhente yderligere oplysninger direkte fra virksomheden eller fra tredjemænd, 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 iværksætte oplysningsforanstaltninger over for forbrugerne og virksomhederne, og eventuelt indlede en håndhævelsesprocedure.

FTC forpligter sig ligeledes til at udveksle oplysninger om henviste sager med de henvisende retshåndhavende myndigheder, herunder om status for de henviste sager, i det omfang det er foreneligt med fortrolighedskrav. 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

⁽¹⁾ Se *FTC v. Karnani*, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (endelig kendelse — stipulated final order), tilgængelig på adressen: <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf>, se også Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, <http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways> (June 9, 2011).

⁽²⁾ Brev fra Ken Hyatt, fungerende viceminister for international handel, International Trade Administration, til Věra Jourová, kommissær for retlige anliggender, forbrugere og ligestilling mellem mænd og kvinder.

vedrørende 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 retshåndhævende 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 ⁽¹⁾. 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 ⁽²⁾.

Ud over prioriteringen af henviste sager under værnet om privatlivets fred fra EU-medlemsstaterne og selvregulerende instanser med kompetence inden for beskyttelse af privatlivets fred ⁽³⁾ vil FTC på eget initiativ og i relevant omfang undersøge mulige overtrædelser af ordningen ved brug af en række redskaber.

FTC har i mere end ti år haft et robust program for undersøgelser af aspekter af privatlivets fred og sikkerhed i relation til kommercielle foretagender. Som led i disse undersøgelser har FTC rutinemæssigt undersøgt, om de pågældende foretagender har afgivet oplysninger om safe harbor-ordningen. Hvis et foretagende afgav sådanne oplysninger og undersøgelsen viste, at safe harbor-principperne tydeligvis blev overtrådt, medtog FTC påstande om overtrædelser af safe harbor-ordningen i sine håndhævelsessager. Vi vil fortsætte denne proaktive tilgang under den nye ordning. Det skal understreges, at FTC foretager langt flere undersøgelser end dem, der i sidste ende resulterer i offentlige håndhævelsesforanstaltninger. Mange FTC-undersøgelser nedlukkes, fordi personalet ikke identificerer en åbenlys lovovertrædelse. Da FTC-undersøgelser er fortrolige og ikke offentliggøres, offentliggøres nedlukningen af en undersøgelse ofte ikke.

De næsten 40 håndhævelsessager indledt af FTC vedrørende safe harbor-programmet vidner om, at FTC har fokus på proaktiv håndhævelse af grænseoverskridende programmer til beskyttelse af privatlivets fred. FTC vil søge efter potentielle overtrædelser af ordningen som led i sine jævnlige undersøgelser af beskyttelsen af privatlivets fred og sikkerheden.

III. HÅNDTERING AF FALSKE ELLER VILDLEDENDE PÅSTANDE OM DELTAGELSE I VÆRNET OM PRIVATLIVETS FRED

Som anført ovenfor vil FTC gribe ind over for enheder, der afgiver urigtige oplysninger om deres deltagelse i ordningen. FTC vil give højeste prioritet til sager henvist fra handelsministeriet vedrørende foretagender, der ifølge ministeriet fremstiller sig selv som værende deltagere i ordningen eller anvender et certificeringsmærke under ordningen uden tilladelse.

Vi understreger endvidere, at hvis et foretagende i sit program til beskyttelse af privatlivets fred erklærer, at det overholder principperne til værn mod privatlivets fred, fritager det forhold, at foretagendet ikke foretager eller opretholder en registrering i handelsministeriet, ikke i sig selv foretagendet fra FTC's håndhævelse af de pågældende forpligtelser under ordningen.

⁽¹⁾ 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 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.

⁽²⁾ I budgetåret 2012-2015 anvendte FTC f.eks. sin bemyndigelse under U.S. SAFE WEB Act til at udveksle oplysninger i forbindelse med besvarelsen af næsten 60 anmodninger fra udenlandske instanser og udstedte næsten 60 editionspålæg (civil investigative demands) (svarer til administrative pålæg (administrative subpoenas)) i forbindelse med 25 udenlandske undersøgelser.

⁽³⁾ Selv om FTC ikke behandler eller mægler i sager om individuelle forbrugerklager, bekræfter FTC, at handelskommissionen vil prioritere henviste sager under værnet om privatlivets fred fra EU's databeskyttelsesmyndigheder. FTC anvender desuden klager i sin Consumer Sentinel-database, som mange andre retshåndhævende organer har adgang til, til at kortlægge tendenser, fastlægge prioriteter for håndhævelsen og identificere potentielle foretagender, 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: www.ftc.gov/complaint. I forbindelse med individuelle klager over krænkelse af privatlivets fred kan det imidlertid være mest hensigtsmæssigt, hvis privatpersoner i EU indgiver deres klager til databeskyttelsesmyndigheden i deres respektive medlemsstater eller til en alternativ tvistbilæggelsesinstans.

IV. OVERVÅGNING AF AFGØRELSE

FTC bekræfter ligeledes, at handelskommissionen vil overvåge håndhævelsesafgørelser for at sikre, at ordningen for værnet om privatlivets fred overholdes.

Vi vil stille krav om, at ordningen overholdes, gennem en række forskellige relevante bestemmelser om forbud i fremtidige FTC-afgørelser under ordningen. Dette omfatter forbud mod urigtige oplysninger om ordningen og andre programmer til beskyttelse af privatlivets fred, når disse er grundlaget for den underliggende FTC-sag.

FTC's sager om håndhævelse af det oprindelige safe harbor-program er lærerige. I 36 sager om falske eller vildledende påstande om safe harbor-certificering forbyder afgørelsen den sagsøgte at afgive urigtige oplysninger om sin deltagelse i safe harbor-ordningen eller andre programmer til beskyttelse af privatlivets fred og sikkerheden og pålægger virksomheden at forelægge overholdelsesrapporter for FTC. I sager om overtrædelser af safe harbor-principperne er virksomheder blevet pålagt at gennemføre omfattende programmer til beskyttelse af privatlivets fred og få udarbejdet uafhængige eksterne vurderinger af disse programmer hvert andet år i 20 år til forelæggelse for FTC.

Overtrædelser af FTC's administrative afgørelser kan resultere i idømmelse af civilretlige sanktioner på op til 16 000 USD for hver overtrædelse eller 16 000 USD pr. dag, hvis overtrædelsen fortsætter ⁽¹⁾, 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. Foretagender 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 safe harbor-afgørelser, som den gør med alle sine afgørelser. FTC tager håndhævelsen af sine afgørelser om privatlivets fred og datasikkerhed alvorligt og anlægger sager med henblik på håndhævelse af disse afgørelser, når det er nødvendigt. Som anført ovenfor blev Google f.eks. idømt en bøde på 22,5 mio. USD for overtrædelse af FTC-afgørelsen. 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 også fremover føre en onlineliste over foretagender omfattet af afgørelser truffet i forbindelse med håndhævelsen af safe harbor-programmet og den nye ordning for værnet om privatlivets fred ⁽²⁾. I henhold til principperne til værn om privatlivets fred skal foretagender omfattet af en FTC- eller retsafgørelse på grund af manglende overholdelse af principperne desuden offentliggøre alle relevante afsnit relateret til værnet om privatlivets fred i alle overholdelses- eller vurderingsrapporter forelagt FTC, i det omfang det er foreneligt med reglerne om fortrolighed.

V. INDDRAGELSE AF OG SAMARBEJDE MED EU'S DATABESKYTTELSESMYNDIGHEDER

FTC anerkender, at EU's databeskyttelsesmyndigheder spiller en vigtig rolle med hensyn til at sikre, at ordningen overholdes, og fremmer inddragelsen af og samarbejdet med disse myndigheder. Ud over samarbejdet med de henvisende databeskyttelsesmyndigheder om sagsspecifikke spørgsmål vil FTC deltage i regelmæssige møder med udpegede repræsentanter fra Artikel 29-Gruppen med henblik på en generel drøftelse af, hvordan samarbejdet om håndhævelse af ordningen kan forbedres. FTC vil ligeledes deltage i den årlige evaluering af ordningen sammen med det amerikanske handelsministerium, Europa-Kommissionen og repræsentanter fra Artikel 29-Gruppen for at drøfte ordningens gennemførelse.

FTC fremmer ligeledes udviklingen af redskaber, som kan forbedre håndhævelsessamarbejdet med EU's databeskyttelsesmyndigheder og med andre databeskyttelsesmyndigheder verden over. Sammen med sine håndhævelsespartnere i EU og verden over lancerede FTC sidste år navnlig et varslingsystem inden for rammerne af Global Privacy Enforcement Network («GPEN») for at udveksle oplysninger om undersøgelser og fremme håndhævelsessamarbejdet. Dette GPEN-varslingsredskab kunne være særdeles nyttigt for ordningen for værnet om privatlivets fred. FTC og EU's databeskyttelsesmyndigheder kunne anvende dette redskab til at koordinere ordningen og andre undersøgelser af mulige krænkelse af

⁽¹⁾ 15 U.S.C. § 45(m), 16 C.F.R. § 1.98.

⁽²⁾ Se FTC, Business Center, Legal Resources, <https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251>.

privatlivets fred, herunder som udgangspunkt for udveksling af oplysninger med henblik på en koordineret og mere effektiv beskyttelse af forbrugernes privatliv. Vi ser frem til et fortsat samarbejde med deltagende EU-myndigheder om en mere generel anvendelse af GPEN-varslingssystemet og om udvikling af andre redskaber, der kan forbedre samarbejdet om håndhævelse i sager om beskyttelse af privatlivets fred, herunder sager, der er omfattet af ordningen.

FTC bekræfter med glæde sit tilsagn om at håndhæve den nye ordning for værnet om privatlivets fred. Vi glæder os ligeledes til at fortsætte samarbejdet med vores kolleger i EU om beskyttelsen af forbrugernes privatliv på begge sider af Atlanten.

Med venlig hilsen

Edith Ramirez

Formand

Tillæg A

Konteksten for ordningen for EU's og USA's værn om privatlivets fred: et overblik over rammerne for EU's og USA's værn om privatlivets fred

Den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred (»ordningen«), indebærer en del af den bredere beskyttelse af privatlivets fred, som ydes af det amerikanske retsvæsen som helhed. For det første har USA's føderale handelskommission Federal Trade Commission (»FTC«) i forbindelse med amerikansk handelspraksis et robust program for privatlivets fred og datasikkerhed, som beskytter forbrugere i hele verden. For det andet har rammerne for beskyttelsen af forbrugernes privatliv og sikkerhed i USA udviklet sig i væsentlig grad siden 2000, da det oprindelige safe harbor-program mellem USA og EU blev vedtaget. Siden da er der på forbunds- og delstatsniveau blevet vedtaget mange love om beskyttelse af privatlivets fred og sikkerhed, og antallet af offentlige og private søgsmål, der er anlagt med hensyn til beskyttelse af privatlivet, er steget betydeligt. Den omfattende amerikanske retsbeskyttelse af forbrugernes privatliv og sikkerhed i forbindelse med kommerciel datapraksis supplerer den beskyttelse, der ydes privatpersoner i EU inden for rammerne af den nye ordning.

I. FTC'S OVERORDNEDE HÅNDHÆVELSESPROGRAM FOR BESKYTTELSE AF PRIVATLIVETS FRED OG SIKKERHED

FTC er USA's førende forbrugerbeskyttelsesagentur med fokus på beskyttelse af privatlivets fred i erhvervssektoren. FTC har beføjelse til at skride ind over for illoyal og vildledende adfærd eller praksis, der krænker forbrugernes privatliv, samt til at håndhæve mere målrettede love om privatlivets fred, der har til formål at beskytte visse finansielle og sundhedsmæssige oplysninger, oplysninger om børn og oplysninger, som anvendes til at træffe visse afgørelser om klassificering af forbrugere.

FTC's erfaring er uden lige, når det gælder om at håndhæve beskyttelsen af forbrugernes privatliv. Med FTC's håndhævelsesforanstaltninger er der blevet taget hånd om ulovlig praksis inden for offline- og onlinemiljøer. FTC har f.eks. indledt håndhævelsessager mod kendte virksomheder som f.eks. Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC og Snapchat samt mod mindre kendte virksomheder. FTC har anlagt sag mod virksomheder, som angiveligt havde spammet forbrugere, installeret spyware på computere, undladt at sikre forbrugeres personoplysninger, sporet forbrugere online på ulovlig vis, krænket børns privatliv, ulovligt indsamlet oplysninger på forbrugeres mobilenheder og undladt at sikre internetforbundne enheder, der anvendes til at lagre personoplysninger. De afgørelser, der er truffet i disse sager, har typisk medført løbende overvågning af FTC for en periode på 20 år, forhindret yderligere lovovertrædelser og pålagt virksomheder betydelige finansielle sanktioner for ikke at have efterkommet afgørelsen⁽¹⁾. Det skal understreges, at FTC's afgørelser ikke kun beskytter de personer, der kan have klaget over et problem. De beskytter snarere alle forbrugere, der fremover vil have med virksomheden at gøre. Uden for USA's grænser har FTC beføjelse til at beskytte forbrugere i hele verden mod praksis, der foregår i USA⁽²⁾.

FTC har indtil videre anlagt over 130 spam- og spywaresager, over 120 »Do Not Call«-telemarketingsager, over 100 sager i forbindelse med Fair Credit Reporting Act, næsten 60 datasikkerhedssager, mere end 50 generelle sager om privatlivets fred, næsten 30 sager om overtrædelse af Gramm-Leach-Bliley Act og over 20 sager om håndhævelse af Children's Online Privacy Protection Act (»COPPA«)⁽³⁾. Ud over disse sager har FTC også udstedt og offentliggjort varslings-skrivelser⁽⁴⁾.

⁽¹⁾ Enhver enhed, der ikke overholder en FTC-afgørelse, idømmes en bøde på op til 16 000 USD pr. overtrædelse eller 16 000 USD pr. dag, hvis overtrædelsen fortsætter. Se 15 U.S.C. § 45(l) og 16 C.F.R. § 1.98(c).

⁽²⁾ Den amerikanske kongres har udtrykkeligt fastlagt FTC's beføjelse til at gøre brug af retsmidler, herunder genoprejsning (restitution), i forbindelse med enhver adfærd eller praksis, som involverer udenlandske foretagender, der 1) forårsager eller vil kunne forårsage skade i USA, som med rimelighed kan forudses, eller 2) involverer den faktiske adfærd i USA. Se 15 U.S.C. § 45(a)(4).

⁽³⁾ I visse tilfælde er det i FTC's sager om privatlivets fred og datasikkerhed blevet gjort gældende, at en virksomhed var involveret i både illoyal og vildledende praksis; disse sager omfattede af og til også angivelige overtrædelser af flere lovbestemmelser som f.eks. Fair Credit Reporting Act, Gramm-Leach-Bliley Act og COPPA.

⁽⁴⁾ Se f.eks. Press Release, Fed. Trade Comm'n, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (Dec. 22, 2014), <https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa>, Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), <https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations> og Press Release, Fed. Trade Comm'n, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 3, 2013), <https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may>.

FTC har som vigtig håndhævelsesmyndighed for så vidt angår beskyttelse af privatlivets fred gennem tiden også regelmæssigt undersøgt eventuelle overtrædelser af safe harbor-programmet. Siden safe harbor-programmets vedtagelse har FTC på eget initiativ iværksat adskillige undersøgelser om overholdelsen af safe harbor-programmet, hvilket har ført til 39 sager mod amerikanske virksomheder, der havde overtrådt programmet. FTC vil fortsætte sin proaktive strategi ved at prioritere håndhævelsen af den nye ordning højt.

II. BESKYTTELSE AF FORBRUGERNES PRIVATLIV PÅ FORBUNDS- OG DELSTATSNIVEAU

Oversigten over håndhævelsen af safe harbor-principperne, der findes som bilag til Europa-Kommissionens beslutning om tilstrækkeligheden af safe harbor-principperne, indeholder en sammenfatning af de mange love om privatlivets fred på forbunds- og delstatsniveau, der var gældende på tidspunktet for safe harbor-programmets vedtagelse i 2000 ⁽¹⁾. På daværende tidspunkt blev indsamlingen og brugen af personoplysninger til kommercielle formål reguleret af mange føderale lovbestemmelser, der foruden Section 5 i FTC Act omfattede Cable Communications Policy Act, Driver's Privacy Protection Act, Electronic Communications Privacy Act, Electronic Funds Transfer Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Right to Financial Privacy Act, Telephone Consumer Protection Act og Video Privacy Protection Act. Mange af delstaterne havde også tilsvarende love på disse områder.

Siden 2000 er der sket meget på både forbunds- og delstatsniveau, hvilket har medført yderligere beskyttelse af forbrugernes privatliv ⁽²⁾. På forbundsniveau ændrede FTC f.eks. COPPA-reglen i 2013 for yderligere at beskytte børns personoplysninger. FTC udstedte også to regler for gennemførelse af Gramm-Leach-Bliley Act, nemlig Privacy Rule og Safeguards Rule, som pålægger finansielle institutioner ⁽³⁾ at offentliggøre deres praksis for deling af oplysninger og gennemføre et omfattende informationssikkerhedsprogram for at beskytte forbrugeroplysninger ⁽⁴⁾. Tilsvarende supplerer Fair and Accurate Credit Transactions Act («FACTA»), der blev vedtaget i 2003, den mangeårige amerikanske lovgivning på kreditområdet med det formål at fastsætte kriterier for maskering, deling og sletning af visse følsomme finansielle oplysninger. FTC udarbejdede som led i FACTA en række regler vedrørende bl.a. forbrugernes ret til en gratis årlig kreditrapport, krav om en sikker sletning af oplysninger i forbrugerrapporter, forbrugeres ret til at fravælge visse kredit- og forsikringstilbud, forbrugeres ret til at fravælge anvendelsen af oplysninger, som et associeret foretagende leverer for at markedsføre sine produkter og tjenester, og krav til finansielle institutioner og kreditgivere om at gennemføre programmer for sporing og forebyggelse af identitetstyveri ⁽⁵⁾. Derudover blev de regler, der blev gennemført som led i Health Insurance Portability and Accountability Act, taget op til fornyet revision i 2013, hvilket medførte yderligere beskyttelse af privatlivets fred og sikkerheden af sundhedsrelaterede personoplysninger ⁽⁶⁾. Regler vedrørende beskyttelse af forbrugere mod uønskede telemarketingsopkald, automatiske opkald (robocalls) og spam er også trådt i kraft. Kongressen har også vedtaget love, som forpligter visse virksomheder, der indsamler sundhedsoplysninger, til at underrette forbrugerne i tilfælde af sikkerhedsbrud ⁽⁷⁾.

Delstaterne har også været meget aktive, når det drejer sig om at vedtage love vedrørende privatlivets fred og sikkerhed. Siden 2000 har 47 delstater, District of Columbia, Guam, Puerto Rico og De Amerikanske Jomfruøer vedtaget love, der

⁽¹⁾ Se USA's handelsministeriums oversigt over håndhævelsen af safe harbor-principperne over på adressen: https://build.export.gov/main/safeharbor/eu/eg_main_018476.

⁽²⁾ Se Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015), for en mere omfattende sammenfatning af retsbeskyttelsen i USA.

⁽³⁾ Finansielle institutioner defineres i Gramm-Leach-Bliley Act meget bredt og omfatter alle virksomheder, som «i væsentlig grad beskæftiger sig» med finansielle produkter eller tjenester. Dette omfatter f.eks. checkindløsningsvirksomheder, «payday lenders» (lån som forskud på forventet indkomst), realkreditmæglere, långivere, som ikke er banker, vurderingsmænd med hensyn til personlige ejendele eller fast ejendom og personer, der professionelt beskæftiger sig med at udarbejde andres selvangivelser.

⁽⁴⁾ Som led i Consumer Financial Protection Act of 2010 («CFPA»), Title X of Pub. L. 111-203, 124 Stat. 1955 (July 21, 2010) (også kendt som «Dodd-Frank Wall Street Reform and Consumer Protection Act») blev de fleste af FTC's lovgivningsbeføjelser under Gramm-Leach-Bliley Act overført til Consumer Financial Protection Bureau («CFPB»). FTC har fortsat håndhævelsesbeføjelse efter Gramm-Leach-Bliley Act samt lovgivningsbeføjelse efter Safeguards Rule og begrænset lovgivningsbeføjelse efter Privacy Rule i forbindelse med bilforhandlere.

⁽⁵⁾ FTC deler ifølge CFPA sine FCRA-beføjelser med CFPB, men en stor del af dens lovgivningsbeføjelser er blevet overført til CFPB (med undtagelse af Red Flags Rule og Disposal Rule).

⁽⁶⁾ Se 45 C.F.R. pts. 160, 162, 164.

⁽⁷⁾ Se f.eks. American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) og relevante forordninger, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

pålægger virksomheder at underrette personer om brud på sikkerheden af personoplysninger ⁽¹⁾. Mindst 32 delstater samt Puerto Rico har indført love om sletning af oplysninger, hvori der fastsættes krav om fjernelse eller sletning af personoplysninger ⁽²⁾. En række delstater har også vedtaget overordnede love om datasikkerhed. Derudover har Californien vedtaget adskillige love om privatlivets fred, herunder en lov, hvorefter virksomheder forpligtes til at indføre en politik for privatlivets fred og offentliggøre deres Do Not-praksis ⁽³⁾, en »Shine the Light«-lov, som pålægger dataformidlere at være mere gennemsigtige ⁽⁴⁾, og en lov om en »sletteknop«, der gør det muligt for mindreårige at anmode om at få slettet visse oplysninger fra sociale medier ⁽⁵⁾. Ved hjælp af disse love og andre beføjelser kan forvaltningerne på forbunds- og delstatsniveau hårdt sanktionere virksomheder, der har undladt at beskytte forbrugernes privatliv og personoplysninger ⁽⁶⁾.

Private søgsmål har også ført til domme og forlig, der har sikret forbrugere yderligere beskyttelse af privatlivets fred og datasikkerhed. I 2015 gik TARGET f.eks. med til at betale 10 mio. USD som led i et forlig med kunder, der hævdede, at deres personlige finansielle oplysninger var blevet bragt i fare som følge af et omfattende brud på datasikkerheden. I 2013 indvilligede AOL i at betale 5 mio. USD som led i et forlig med henblik på at bilægge et kollektivt søgsmål med påstand om utilstrækkelig anonymisering i forbindelse med udgivelsen af hundrede tusinde AOL-medlemmers søgninger. Herudover afgjorde en forbundsdomstol, at Netflix skulle betale 9 mio. USD for angiveligt at have opbevaret udlæjningsoplysninger i strid med Video Privacy Protection Act fra 1988. Forbundsdomstole i Californien godkendte to forskellige forlig med Facebook, et forlig, der gik ud på betaling af 20 mio. USD, og et andet på 9,5 mio. USD, der vedrørte virksomhedens indsamling, anvendelse og deling af brugernes personoplysninger. I 2008 godkendte en delstatsdomstol i Californien et forlig, der indebar, at LensCrafters skulle betale 20 mio. USD efter at have videreformidlet forbrugernes medicinske oplysninger på ulovlig vis.

Kort sagt yder USA betydelig retsbeskyttelse for så vidt angår forbrugernes privatliv og sikkerhed, hvilket også fremgår af denne sammenfatning. Den nye ordning for værnet om privatlivets fred, der sikrer privatpersoner i EU en meningsfuld beskyttelse, vil indgå i en større sammenhæng, hvor beskyttelsen af forbrugernes privatliv og sikkerhed fortsat udgør en vigtig prioritet.

⁽¹⁾ Se f.eks. National Conference of State Legislatures (»NCSL«), *State Security Breach Notification Laws* (Jan. 4, 2016), tilgængelig på adressen: <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

⁽²⁾ NCSL, *Data Disposal Laws* (Jan. 12, 2016), tilgængelig på adressen: <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>.

⁽³⁾ Cal. Bus. & Professional Code §§ 22575-22579.

⁽⁴⁾ Cal. Civ. Code §§ 1798.80-1798.84.

⁽⁵⁾ Cal. Bus. & Professional Code § 22580-22582.

⁽⁶⁾ Se Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (Feb. 17, 2014), der findes på adressen: <http://www.computerworld.com/s/article/9246393/jay-cline-u.s.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1>.

BILAG V

Brev fra den amerikanske transportminister Anthony Foxx

Den 19. februar 2016

Kommissær Věra Jourová
Europa-Kommissionen
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
Belgien

Vedr.: Ordningen for EU's og USA's værn om privatlivets fred

Kære kommissær Věra Jourová,

De Forenede Staters transportministerium (»ministeriet«) glæder sig over at få lejlighed til at redegøre for sin rolle i håndhævelsen af ordningen for EU's og USA's værn om privatlivets fred. Denne ordning spiller 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 giver virksomheder mulighed for at gennemføre vigtige transaktioner i den globale økonomi og sikrer samtidig den vigtige beskyttelse af EU-forbrugernes privatliv.

Transportministeriet forpligtede sig første gang offentligt til at håndhæve safe harbor-ordningen i et brev til Europa-Kommissionen for over 15 år siden. Transportministeriet afgav i dette brev tilsagn om at håndhæve safe harbor-principperne til beskyttelse af privatlivets fred strengt. Transportministeriet opfylder fortsat dette tilsagn, og dette tilsagn understreges i dette brev.

Transportministeriet bekræfter på ny sine tilsagn på følgende hovedområder: 1) prioritering af undersøgelse af påståede overtrædelser af ordningen for værnet om privatlivets fred, 2) iværksættelse af passende håndhævelsesforanstaltninger mod foretagender, der fremsætter falske eller vildledende påstande om certificering, og 3) overvågning og offentliggørelse af håndhævelsesafgørelser vedrørende overtrædelser af principperne til værn om privatlivets fred. Vi redegør nedenfor for de enkelte tilsagn og af hensyn til den nødvendige sammenhæng for den relevante baggrund for transportministeriets rolle i beskyttelsen af forbrugernes privatliv og håndhævelsen af ordningen for værnet om privatlivets fred.

I. 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 eller illoyale konkurrencemetoder, der er eller kan være til skade for forbrugerne, i forbindelse med salg af lufttransportydelser. Section 41712 er udformet efter Section 5 i Federal Trade Commission (FTC) Act (15 U.S.C. 45). I henhold til loven om illoyal eller vildledende praksis — som vi fortolker den — må et luftfartsselskab eller et rejsebureau ikke: 1) overtræde principperne i dets program til beskyttelse af privatlivets fred eller 2) videregive personoplysninger på en måde, der strider mod den offentlige orden, er umoralsk eller medfører en betydelig skade for forbrugerne, der ikke opvejes af andre fordele. Vi fortolker ligeledes Section 41712 således, at den forbyder transportører og rejsebureauer at: 1) overtræde enhver regel udstedt af ministeriet, der identificerer specifik databeskyttelsespraksis som illoyal eller vildledende, eller 2) overtræde Children's Online Privacy Protection Act (COPPA) eller FTC's regler til gennemførelse af COPPA. I henhold til forbundslovgivningen har ministeriet enekompetence til at regulere luftfartsselskabernes databeskyttelsespraksis og deler kompetence med FTC, for så vidt angår rejsebureauernes databeskyttelsespraksis i forbindelse med salg af lufttransportydelser.

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

B. Håndhævelsespraksis

Ministeriets Office of Aviation Enforcement and Proceedings (Aviation Enforcement Office) 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 civilretlige 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 ⁽¹⁾.

Hvis der ikke indgås et rimeligt og passende forlig i en sag, har Aviation Enforcement Office kompetence til at indlede en håndhævelsesprocedure med bevisføring for ministeriets forvaltningsdommer (administrative law judge (ALJ)). ALJ er bemyndiget til at udstede forbud og idømme civilretlige sanktioner. Overtrædelser af Section 41712 kan medføre, at der udstedes forbud og idømmes civilretlige sanktioner på op til 27 500 USD for hver overtrædelse af Section 41712.

Ministeriet har ikke beføjelse til at tilkende erstatning eller give økonomisk godtgørelse til individuelle klagere, men ministeriet har beføjelse til at godkende forlig, der indgås på baggrund af undersøgelser foretaget af Aviation Enforcement Office, 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 også ske igen i forbindelse med overtrædelser af principperne i ordningen for værnet om privatlivets fred, 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 inden for lufttransport eller i forbindelse med salg af lufttransportydelser 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 luftfartsselskabets 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.

Med hensyn til luftfartsselskaber håndhæver ministeriet ligeledes andre relevante love, hvis bestemmelser også finder anvendelse på ikkeamerikanske forbrugere, f.eks. 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 VÆRNET OM PRIVATLIVETS FRED

Hvis et luftfartsselskab eller et rejsebureau vælger at deltage i ordningen for værnet om privatlivets fred, og ministeriet modtager en klage over luftfartsselskabets eller rejsebureauets påståede overtrædelse af ordningen, vil ministeriet træffe følgende foranstaltninger for at håndhæve ordningen strengt.

⁽¹⁾ <http://www.transportation.gov/airconsumer/privacy-complaints>.

A. Prioritering af undersøgelse af påståede overtrædelser

Ministeriets Aviation Enforcement Office vil undersøge hver klage over påståede overtrædelser af ordningen for værnet om privatlivets fred (herunder klager fra EU's databeskyttelsesmyndigheder) og træffe håndhævelsesforanstaltninger, hvis der er dokumentation for en overtrædelse. Aviation Enforcement Office 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 ordningen for værnet om privatlivets fred.

Når ministeriets Aviation Enforcement Office modtager klage med påstand om en overtrædelse af ordningen for værnet om privatlivets fred, kan kontoret træffe en række foranstaltninger som led i sin undersøgelse. Kontoret kan f.eks. gennemgå rejsebureauets eller luftfartsselskabets programmer til beskyttelse af privatlivets fred, indhente yderligere oplysninger fra rejsebureauet eller luftfartsselskabet eller fra tredjemænd, 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 ordningen for værnet om privatlivets fred, vil ministeriet koordinere sagen med FTC. Vi vil ligeledes rådgive FTC og handelsministeriet om udfaldet af en eventuel håndhævelsesprocedure vedrørende værnet om privatlivets fred.

B. Håndtering af falske eller vildledende påstande om deltagelse i værnet om privatlivets fred

Ministeriet vil fortsat undersøge overtrædelser af ordningen for værnet om privatlivets fred, herunder falske eller vildledende påstande om deltagelse i programmet for værnet om privatlivets fred. Vi vil give højeste prioritet til sager henvist fra handelsministeriet vedrørende foretagender, der ifølge ministeriet fremstiller sig selv som værende nuværende deltagere i ordningen eller anvender et certificeringsmærke under værnet om privatlivets fred uden tilladelse.

Vi understreger endvidere, at hvis et foretagende i sit program til beskyttelse af privatlivets fred erklærer, at det overholder væsentlige principper til værn mod privatlivets fred, fritager det forhold, at foretagendet ikke foretager eller opretholder en registrering i handelsministeriet, ikke i sig selv foretagendet fra ministeriets håndhævelse af de pågældende forpligtelser.

C. Overvågning og offentliggørelse af håndhævelsesafgørelser vedrørende overtrædelser af ordningen for værnet om privatlivets fred

Ministeriets Aviation Enforcement Office vil også fortsat overvåge håndhævelsesafgørelser for at sikre, at programmet for værnet om privatlivets fred overholdes. Hvis kontoret udsteder et forbud, der pålægger et luftfartsselskab eller rejsebureau at afholde sig fra fremtidige overtrædelser af principperne til værn om privatlivets fred og Section 41712, vil kontoret overvåge, om enheden overholder bestemmelserne om forbud. Kontoret vil desuden sikre, at forbud, der udstedes i sager om værnet om privatlivets fred, offentliggøres på dets websted.

Vi ser frem til et fortsat samarbejde med vores føderale partnere og interessenter i EU om værnet om privatlivets fred.

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

Med venlig hilsen

Anthony R. Foxx

Transportminister

BILAG VI

**Brev fra General Counsel Robert Litt
Office of the Director of National Intelligence**

Den 22. februar 2016

Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Kære Justin S. Antonipillai og Ted Dean,

I de sidste to og et halvt år har USA i forbindelse med forhandlingerne om værnet om privatlivets fred fremlagt mange oplysninger om de amerikanske efterretningstjenesters indsamling af signalefterretninger. Der er blevet redegjort for det gældende retsgrundlag, tilsynet med disse aktiviteter på flere niveauer, den store åbenhed omkring disse aktiviteter og den generelle beskyttelse af privatlivets fred og borgerlige rettigheder for at gøre det lettere for Europa-Kommissionen at vurdere tilstrækkeligheden af denne beskyttelse, da den hænger sammen med den nationale sikkerhedsundtagelse under værnet om privatlivets fred. I dette dokument sammenfattes disse oplysninger.

I. PPD-28 OG AMERIKANSKE SIGNALEFTERRETNINGSAKTIVITETER

De amerikanske efterretningstjenester indsamler udenlandske efterretninger på en nøje kontrolleret måde i fuld overensstemmelse med amerikansk lovgivning. Der føres tilsyn på flere niveauer, og der er fokus på vigtige prioriteter for udenlandsk efterretningsvirksomhed og den nationale sikkerhed. De amerikanske efterretningstjenesters indsamling af signalefterretninger reguleres af en mosaik af love og politikker, herunder den amerikanske forfatning, Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 ff.) (FISA), Executive Order 12333 og gennemførelsesprocedurerne hertil, præsidentiel vejledning og en lang række procedurer og retningslinjer godkendt af FISA-domstolen og den amerikanske justitsminister, der indeholder yderligere regler, som begrænser indsamlingen, brugen og formidlingen af udenlandske efterretningsoplysninger ⁽¹⁾.

a. PPD 28 — Overblik

I januar 2014 holdt præsident Obama en tale, hvori han redegjorde for forskellige reformer af USA's signalefterretningsaktiviteter, og udstedte efterfølgende Presidential Policy Directive 28 (PPD-28) om disse aktiviteter ⁽²⁾. Præsidenten understregede, at amerikanske signalefterretningsaktiviteter ikke kun bidrager til at sikre USA og amerikanske frihedsrettigheder, men også sikkerheden og frihedsrettighederne i andre lande, herunder EU-medlemsstaterne, der anvender de oplysninger, som de amerikanske efterretningsagenturer indsamler, til at beskytte deres egne borgere.

I PPD-28 fastsættes en række principper og krav, som finder anvendelse på alle amerikanske signalefterretningsaktiviteter og på alle mennesker, uanset nationalitet eller bopæl. Der stilles navnlig bestemte krav til procedurer for indsamling, opbevaring og formidling af personoplysninger om ikkeamerikanske personer indsamlet gennem amerikansk signalefterretning. Der redegøres nærmere for disse krav nedenfor, og de sammenfattes her:

— Det understreges i PPD, at USA kun indsamler signalefterretninger i medfør af tillagte beføjelser i amerikanske love, præsidentielle dekretter eller andre præsidentielle direktiver.

⁽¹⁾ Der er yderligere oplysninger om USA's udenlandske efterretningsaktiviteter online, og de er offentligt tilgængelige gennem efterretnings-tjenesterne (www.icontherecord.tumblr.com), ODN's offentlige websted, der skal skabe større offentlig synlighed omkring regeringens signalefterretningsaktiviteter.

⁽²⁾ Tilgængelig på adressen: <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

- I PPD fastsættes procedurer til at sikre, at der kun gennemføres signalefterretningsaktiviteter til legitime og godkendte nationale sikkerhedsformål.
- I henhold til PPD skal hensynet til privatlivets fred og borgerlige rettigheder integreres i planlægningen af amerikanske signalefterretningsaktiviteter. USA indsamler navnlig ikke efterretninger med det formål at undertrykke kritik eller uenighed, at forskelsbehandle mennesker på grund af etnisk oprindelse, race, køn, seksuel orientering eller religion eller at give amerikanske virksomheder og erhvervssektorer en kommerciel konkurrencefordel.
- I henhold til PPD skal indsamling af signalefterretninger være så målrettet som muligt, og masseindsamlede signalefterretninger kan kun anvendes til specifikke opregnede formål.
- I henhold til PPD skal de amerikanske efterretningstjenester indføre procedurer, der »i rimeligt omfang er udformet med henblik på at minimere formidlingen og opbevaringen af personoplysninger indsamlet gennem signalefterretningsaktiviteter«, og navnlig udvide en del af beskyttelsen af amerikaneres personoplysninger til at omfatte ikkeamerikanske personers personoplysninger.
- Agenturerne har indført procedurer til gennemførelse af PPD-28, og de er blevet offentliggjort.

Procedurerne og beskyttelsesforanstaltningerne kan klart anvendes under værnet om privatlivets fred. Når oplysninger er blevet overført til foretagender i USA under værnet om privatlivets fred, eller endog på enhver anden måde, kan de amerikanske efterretningstjenester kun anmode om indsigt i oplysninger fra disse virksomheder, hvis anmodningen er i overensstemmelse med FISA eller indgives i henhold til en af bestemmelserne om det nationale sikkerhedsbrev (National Security Letter), jf. nedenfor ⁽¹⁾. Uden at bekræfte eller afkræfte medierapporter, hvor det påstås, at de amerikanske efterretningstjenester indsamler oplysninger fra transatlantiske kabler under overførslen til USA, ville de amerikanske efterretningstjenester, hvis de skulle indsamle oplysninger fra transatlantiske kabler, være underlagt de begrænsninger og beskyttelsesforanstaltninger, der redegøres for her, herunder kravene i PPD-28.

b. Begrænsninger for indsamling

PPD-28 opstiller en række vigtige generelle principper for indsamling af signalefterretninger:

- Indsamlingen af signalefterretninger skal være hjulmet ved lov eller præsidentiel bemyndigelse og skal foretages i overensstemmelse med den amerikanske forfatning.
- Hensynet til privatlivets fred og borgerlige rettigheder skal integreres i planlægningen af amerikanske signalefterretningsaktiviteter.
- Der må kun indsamles signalefterretninger til godkendte udenlandske efterretnings- eller kontraspionageformål.
- USA vil ikke indsamle signalefterretninger med det formål at undertrykke kritik eller uenighed.
- USA vil ikke indsamle signalefterretninger med det formål at forskelsbehandle mennesker på grund af etnisk oprindelse, race, køn, seksuel orientering eller religion.
- USA vil ikke indsamle signalefterretninger med det formål at give amerikanske virksomheder og erhvervssektorer en kommerciel konkurrencefordel.
- Indsamlingen af signalefterretninger skal altid være så målrettet som muligt, og der skal tages højde for andre tilgængelige informationskilder. Det betyder bl.a., at indsamlingen af signalefterretninger målrettes, når det er praktisk muligt, i stedet for at foretage masseindsamling.

Kravet om, at indsamlingen af signalefterretninger skal være så »målrettet som muligt«, gælder også for den måde, hvorpå signalefterretninger indsamles, og det, der rent faktisk indsamles. Når de amerikanske efterretningstjenester f.eks. skal beslutte, om der skal indsamles signalefterretninger, skal de tage højde for andre tilgængelige oplysninger, herunder

⁽¹⁾ Retshåndhævelses- og reguleringsorganer kan anmode om oplysninger fra foretagender til efterforskningsformål i USA i medfør af andre strafferetlige, civilretlige og regulerende beføjelser, hvilket ligger uden for rammerne af dette dokument, der kun vedrører nationale sikkerhedsbeføjelser.

diplomatiske eller offentlige kilder, og prioritere indsamling ved brug af disse metoder, hvis de er hensigtsmæssige og mulige. Der skal desuden i efterretningsenhedernes politikker stilles krav om, at indsamlingen så vidt muligt rettes mod specifikke udenlandske efterretningsmål eller -emner ved brug af diskriminanter (f.eks. specifikke faciliteter, selektorer og identifikatorer).

Det er vigtigt at betragte oplysningerne til Kommissionen som en helhed. Afgørelser om, hvad der er »muligt« eller »praktisk«, overlades ikke til den enkelte, men er underlagt de politikker, som agenturerne har indført i henhold til PPD-28 — og som er blevet offentliggjort — og til de andre heri beskrevne processer ⁽¹⁾. Som fastslået i PPD-28 er masseindsamling af signalefterretninger indsamling, der »på grund af tekniske eller operationelle forhold foretages uden brug af diskriminanter (f.eks. specifikke identifikatorer, selektorer osv.)«. Det anerkendes således i PPD-28, at efterretningsenhederne er nødsaget til at foretage masseindsamling af signalefterretninger i visse situationer for at identificere nye trusler eller trusler under udvikling og andre vitale sikkerhedsoplysninger, der ofte er skjulte i det store og komplekse moderne globale kommunikationssystem. Det anerkendes ligeledes, at masseindsamling af signalefterretninger vækker bekymringer over beskyttelsen af privatlivets fred og borgerlige rettigheder. I PPD-28 pålægges de amerikanske efterretningstjenester derfor at prioritere alternativer, der gør det muligt at målrette indsamlingen af signalefterretninger i stedet for at foretage masseindsamling af signalefterretninger. Efterretningsenhederne skal derfor så vidt muligt målrette indsamlingen af signalefterretninger i stedet for at foretage masseindsamling af signalefterretninger. ⁽²⁾ Disse principper sikrer, at undtagelsen om masseindsamling ikke bliver reglen.

Med hensyn til begrebet »rimelighed« er det et grundlæggende princip i amerikansk ret. Dette betyder, at efterretningsenhederne ikke skal gennemføre enhver foranstaltning, der er teoretisk mulig, men at de i stedet skal veje deres foranstaltninger til beskyttelse af legitime hensyn til privatlivets fred og borgerlige rettigheder op mod de praktiske krav til signalefterretningsaktiviteter. Også her er agenturernes politikker blevet offentliggjort, og de kan give sikkerhed for, at formuleringen »i rimeligt omfang er udformet med henblik på at minimere formidlingen og opbevaringen af personoplysninger« ikke underminerer den generelle regel.

Det fastslås ligeledes i PPD-28, at masseindsamlede signalefterretninger kun kan anvendes til seks specifikke formål: sporing og imødegåelse af visse aktiviteter udøvet af udenlandske magter, terrorbekæmpelse, spredningsbekæmpelse, cybersikkerhed, sporing og imødegåelse af trusler mod USA eller allierede væbnede styrker og bekæmpelse af transnationale kriminelle trusler, herunder sanktionsunddragelse. Den amerikanske præsidents nationale sikkerhedsrådgiver vil i samarbejde med direktøren for National Intelligence (DNI) hvert år gennemgå disse tilladte anvendelser af masseindsamlede signalefterretninger for at se, om de bør ændres. DNI vil efterfølgende offentliggøre denne liste i muligt omfang under hensyntagen til den nationale sikkerhed. Dette sikrer en vigtig og åbenlys begrænsning af brugen af masseindsamling af signalefterretninger.

De efterretningsenheder, der gennemfører PPD-28, har desuden styrket deres analysepraksis og -standarder for søgning efter ikkeevaluerede signalefterretninger ⁽³⁾. Analytikerne skal strukturere deres søgninger eller andre søgetermer og -teknikker for at sikre, at de er egnede til at identificere efterretningsoplysninger, der er relevante for godkendte udenlandske efterretnings- eller retshåndhævelsesopgaver. Efterretningsenhederne skal i denne forbindelse rette søgninger om personer mod de kategorier af signalefterretningsoplysninger, der imødekommer et behov for udenlandske efterretninger eller retshåndhævelse, for at hindre anvendelsen af personoplysninger, der ikke opfylder behov for udenlandske efterretninger eller retshåndhævelse.

Det er vigtigt at understrege, at enhver masseindsamling af internetkommunikation, som de amerikanske efterretnings-tjenester foretager gennem signalefterretning, foretages på en lille del af internettet. Anvendelsen af målrettede søgninger sikrer desuden som beskrevet ovenfor, at analytikerne kun får forelagt de oplysninger, der formodes at have en potentiel efterretningsværdi, til analyse. Disse begrænsninger skal beskytte alle personers privatliv og borgerlige rettigheder uanset deres nationalitet og bopæl.

⁽¹⁾ Tilgængelig på adressen: www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Disse procedurer gennemfører den målrettede overvågning, der redegøres for i dette brev, på en bestemt måde i de enkelte efterretningsenheder.

⁽²⁾ Blot for at nævne et eksempel anføres det i NSA's procedurer til gennemførelse af PPD-28, at »indsamlingen så vidt muligt foretages ved brug af en eller flere selektorer for at rette indsamlingen mod specifikke udenlandske efterretningsmål (f.eks. en specifik kendt international terrorist eller terrorgruppe) eller specifikke udenlandske efterretningsmønstre (f.eks. en fremmed magt eller en agentspredning af masseødelæggelsesvåben)«.

⁽³⁾ Tilgængelig på adressen: http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

USA har udviklet procedurer til at sikre, at der kun gennemføres signalefterretningsaktiviteter til relevante nationale sikkerhedsformål. Præsidenten fastsætter hvert år nationens højeste prioriteter for indsamling af udenlandske efterretninger efter en omfattende, formel tværorganisatorisk proces. DNI skal omsætte disse efterretningsprioriteter i »National Intelligence Priorities Framework« eller NIPF. PPD-28 har styrket og forbedret den tværorganisatoriske proces ved at sikre, at alle efterretningstjenesternes prioriteter gennemgås og godkendes af politiske beslutningstagere på højt niveau. I Intelligence Community Directive (ICD) 204 opstilles yderligere retningslinjer for NIPF, og direktivet blev ajourført i 2015, hvor kravene i PPD-28 blev indarbejdet (¹). Selv om NIPF er klassificeret, angives oplysninger om specifikke amerikanske udenlandske efterretningsprioriteter hvert år i DNI's uklassificerede Worldwide Threat Assessment, der ligeledes er let tilgængelig på ODNI's websted.

Prioriteterne i NIPF er meget generelle. De omfatter emner som specifikke fremmede fjendtlige landes gennemførelse af atom- og ballistiske missilprogrammer, konsekvenserne af narkotikakarteller og korruption og krænkelse af menneskerettighederne i specifikke lande. De finder ikke kun anvendelse på signalefterretning, men på alle efterretningsaktiviteter. National Signals Intelligence Committee eller SIGCOM har ansvaret for at omsætte prioriteterne i NIPF til konkret indsamling af signalefterretninger. SIGCOM refererer til direktøren for National Security Agency ((NSA), der er udpeget ved Executive Order 12333 som den »funktionelle leder af signalefterretning« med ansvar for tilsyn med og koordinering af signalefterretning på tværs af de amerikanske efterretningstjenester under tilsyn af den amerikanske forsvarsminister og DNI. SIGCOM har repræsentanter fra alle efterretningsenhederne, og i takt med, at den amerikanske regering gennemfører PPD-28 fuldt ud, vil der også komme fuld repræsentation fra andre ministerier og agenturer med en politisk interesse i signalefterretning.

Alle amerikanske ministerier og agenturer, der anvender udenlandske efterretninger, skal indgive deres anmodninger om indsamling til SIGCOM. SIGCOM gennemgår disse anmodninger og sikrer, at de er i overensstemmelse med NIPF, og prioriterer dem ud fra kriterier såsom:

- Kan signalefterretning tilvejebringe nyttige oplysninger i dette tilfælde, eller er der mere omkostningseffektive informationskilder, som kan afhjælpe behovet, såsom billeder eller åbne kilder?
- Hvor kritisk er dette behov for oplysninger? Hvis det er en høj prioritet i NIPF, vil det som oftest også være en høj signalefterretningsprioritet.
- Hvilken type signalefterretning kan anvendes?
- Er indsamlingen så målrettet som muligt? Bør der være tidsmæssige, geografiske eller andre begrænsninger?

Ved vurderingen af behovet for signalefterretning skal der ligeledes tages udtrykkeligt stilling til andre faktorer:

- Er målet for indsamlingen eller indsamlingsmetoden særlig følsom? Hvis dette er tilfældet, skal en overordnet politisk beslutningstager gennemgå sagen.
- Vil indsamlingen medføre en urimelig risiko for privatlivets fred og borgerlige rettigheder, uanset nationalitet?
- Skal der træffes yderligere sikkerhedsforanstaltninger i forbindelse med formidling og opbevaring for at beskytte privatlivets fred eller nationale sikkerhedsinteresser?

Når processen er afsluttet søger og identificerer uddannet NSA-personale ud fra prioriteterne valideret af SIGCOM specifikke selektorer såsom telefonnumre eller e-mailadresser, som forventes at resultere i indsamlingen af udenlandske efterretninger i overensstemmelse med disse prioriteter. Enhver selektor skal gennemgås og godkendes, inden den indtastes i NSA's indsamlingssystemer. Selv i denne fase afhænger spørgsmålet om, hvorvidt og hvornår indsamlingen

(¹) Tilgængelig på adressen: <http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf>.

rent faktisk vil ske, imidlertid til dels af andre overvejelser såsom tilgængeligheden af tilstrækkelige indsamlingsressourcer. Denne proces sikrer, at USA's mål for indsamling af signalefterretninger afspejler velbegrundede og vigtige behov for udenlandske efterretninger. Når indsamlingen foretages i henhold til FISA, skal NSA og andre agenturer naturligvis overholde yderligere begrænsninger godkendt af Foreign Intelligence Surveillance Court. Hverken NSA eller nogen anden amerikansk efterretningstjeneste afgør kort sagt selv, hvad der skal indsamles.

Denne proces sikrer generelt, at alle amerikanske efterretningsprioriteter fastlægges af politiske beslutningstagere på højt niveau, som har de bedste forudsætninger for at identificere USA's behov for udenlandske efterretninger, og at disse politiske beslutningstagere ikke kun tager højde for de indsamlede efterretningers potentielle værdi, men også for risiciene forbundet med denne indsamling, herunder risiciene for privatlivets fred, nationale økonomiske interesser og udenlandske relationer.

Selv om USA ikke kan bekræfte eller benægte specifikke efterretningsmetoder eller -aktiviteter, kan det, for så vidt angår oplysninger, der overføres fra USA under værnet om privatlivets fred, oplyses, at kravene i PPD-28 finder anvendelse på alle amerikanske signalefterretningsaktiviteter, uanset karakteren af de oplysninger, der indsamles, og kilden. De begrænsninger og sikkerhedsforanstaltninger, der gælder for indsamling af signalefterretninger, gælder også for signalefterretninger indsamlet til ethvert godkendt formål, herunder både udenlandske forbindelser og den nationale sikkerhed.

Ovenstående procedurer viser, at der er en klar vilje til at forhindre vilkårlig indsamling af signalefterretninger og til at gennemføre princippet om rimelighed på højeste regeringsniveauer. I PPD-28 og agenturernes gennemførelsesprocedurer afklares nye og eksisterende begrænsninger for signalefterretning, og der redegøres nærmere for formålet med USA's indsamling og anvendelse af signalefterretning. Disse bør give sikkerhed for, at signalefterretningsaktiviteter kun gennemføres og fortsat kun vil blive gennemført med det formål at nå legitime mål for udenlandsk efterretningsvirksomhed.

c. Begrænsninger for opbevaring og formidling

I henhold til Section 4 i PPD-28 skal der sættes udtrykkelige grænser for de enkelte efterretningsenheders opbevaring og formidling af personoplysninger om ikke-amerikanske personer indsamlet gennem signalefterretning, der svarer til grænserne for amerikanske personer. Disse bestemmelser er indarbejdet i de enkelte efterretningsenheders procedurer, som blev udstedt i februar 2015 og offentliggjort. Hvis personoplysninger skal kunne opbevares eller formidles som udenlandske efterretninger, skal de være relateret til et efterretningsbehov godkendt i forbindelse med ovennævnte NIPF-proces, med rimelighed kunne formodes at være bevis for en forbrydelse eller opfylde et af de andre kriterier for opbevaring i Executive Order 12333, Section 2.3.

Hvis dette ikke er tilfældet, må oplysningerne kun opbevares i fem år, medmindre DNI udtrykkeligt beslutter, at fortsat opbevaring er i USA's nationale sikkerhedsinteresse. Efterretningsenhederne skal således slette personoplysninger om ikke-amerikanske personer indsamlet gennem signalefterretning fem år efter indsamlingen, medmindre det f.eks. er blevet besluttet, at oplysningerne er relateret til et godkendt udenlandsk efterretningsbehov, eller hvis DNI på baggrund af de holdninger, som ODNI's Civil Liberties Protection Officer samt de databeskyttelsesansvarlige (privacy and civil liberties officers) giver udtryk for, bestemmer, at fortsat opbevaring er i den nationale sikkerheds interesse.

Det er desuden nu et udtrykkeligt krav i alle agenturernes politikker til gennemførelse af PPD-28, at oplysninger om en person ikke må formidles udelukkende med den begrundelse, at den pågældende er udlænding, og ODNI har udstedt et direktiv til alle efterretningsenheder⁽¹⁾ om dette krav. Efterretningstjenesternes personale skal navnlig tage hensyn til ikkeamerikanske personers interesser i beskyttelsen af privatlivets fred i forbindelse med udarbejdelsen og formidlingen af efterretningsrapporter. Signalefterretninger om en udlændings rutinemæssige aktiviteter vil navnlig ikke blive betragtet som udenlandske efterretninger, der kan formidles eller opbevares permanent alene af denne årsag, medmindre de på anden vis opfylder et godkendt behov for udenlandske efterretninger. Herved anerkendes en vigtig begrænsning, som imødegår Europa-Kommissionens bekymringer over den brede definition af udenlandske efterretninger i Executive Order 12333.

⁽¹⁾ Intelligence Community Directive (ICD) 203, tilgængelig på adressen: <http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf>.

d. Overholdelse og tilsyn

Det amerikanske system for tilsyn med efterretningsvirksomhed i udlandet omfatter et strengt tilsyn på flere niveauer for at sikre overholdelsen af love og procedurer, herunder om indsamling, opbevaring og formidling af personoplysninger om ikke-amerikanske personer indsamlet gennem amerikansk signalefterretning i henhold til PPD-28. Opbygning:

- Efterretningstjenesterne beskæftiger flere hundrede kontrolmedarbejdere. Alene i NSA arbejder over 300 mennesker med kontrol af overholdelse, og andre efterretningsenheder har ligeledes tilsynskontorer. Justitsministeriet fører ligeledes et omfattende tilsyn med efterretningsaktiviteter, og der føres også tilsyn i forsvarsministeriet.
- Hver efterretningsenhed har sit eget Office of the Inspector General (generalinspektørens kontor) med ansvar for tilsyn med bl.a. udenlandske efterretningsaktiviteter. Inspectors General (generalinspektører) er lovmæssigt uafhængige, de har brede beføjelser til at foretage undersøgelser, revisioner og kontrol af programmer, herunder af svig og misbrug eller overtrædelse af loven, og de kan anbefale korrigerende foranstaltninger. Selv om generalinspektørernes anbefalinger ikke er bindende, offentliggøres deres rapporter ofte, og de forelægges under alle omstændigheder for den amerikanske kongres. Dette omfatter opfølgingsrapporter, hvis korrigerende foranstaltninger anbefalet i tidligere rapporter endnu ikke er blevet gennemført. Kongressen underrettes derfor om enhver manglende overholdelse og kan udøve pres, herunder gennem budgetmidler, for at sikre, at der iværksættes korrigerende foranstaltninger. Der er blevet offentliggjort en række rapporter fra generalinspektørerne om efterretningsprogrammer ⁽¹⁾.
- ODN's Civil Liberties and Privacy Office (CLPO) har til opgave at sikre, at de amerikanske efterretningstjenester opererer på en måde, der fremmer den nationale sikkerhed og samtidig beskytter borgerlige rettigheder og privatlivsrettigheder ⁽²⁾. Andre efterretningsenheder har deres egen databeskyttelsesansvarlige (privacy officer).
- Privacy and Civil Liberties Oversight Board (PCLOB), et uafhængigt organ oprettet ved lov, har til opgave at analysere og gennemgå terrorbekæmpelsesprogrammer og -politikker, herunder anvendelsen af signalefterretning, for at sikre, at de i tilstrækkelig grad beskytter privatlivets fred og borgerlige rettigheder. PCLOB har udstedt flere offentlige rapporter om efterretningsaktiviteter.
- Som nærmere forklaret i det følgende er Foreign Intelligence Surveillance Court, der består af uafhængige forbundsdommere, ansvarlig for tilsynet med indsamling af signalefterretninger i henhold til FISA, herunder for overholdelsen af reglerne.
- Endelig fører den amerikanske kongres, navnlig Repræsentanternes Hus og Senatets efterretnings- og retsudvalg — House and Senate Intelligence and Judiciary Committees — tilsyn med USA's udenlandske efterretningsaktiviteter, herunder USA's signalefterretning.

Ud over disse formelle tilsynsmekanismer har de amerikanske efterretningstjenester indført en række mekanismer for at sikre, at efterretningstjenesterne overholder de begrænsninger for indsamlingen, der er beskrevet ovenfor. For eksempel:

- Kabinettet skal validere deres behov for signalefterretninger hvert år.
- NSA kontrollerer mål for indsamling af signalefterretninger i hele indsamlingsprocessen for at vurdere, om de rent faktisk resulterer i indsamlingen af værdifulde udenlandske efterretninger i overensstemmelse med prioriteterne, og vil i modsat fald standse indsamlingen i forbindelse med de enkelte mål. Der er indført yderligere procedurer, som sikrer, at selektorerne gennemgås regelmæssigt.

⁽¹⁾ Se f.eks. rapport fra det amerikanske justitsministeriums generalinspektør »A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008« (september 2012), tilgængelig på adressen: <https://oig.justice.gov/reports/2016/o1601a.pdf>.

⁽²⁾ Se www.dni.gov/clpo.

- DNI har på grundlag af en anbefaling fra et uafhængigt undersøgelsesudvalg nedsat af præsident Obama oprettet en ny mekanisme til overvågning af indsamling og formidling af signalefterretninger, som er særlig sårbare på grund af målets karakter eller indsamlingsmetoden, for at sikre, at den er i overensstemmelse med de politiske beslutningstageres afgørelser.
- Endelig vejer ODNI hvert år de amerikanske efterretningstjenesters tildeling af ressourcer op mod NIPF-prioriteterne og efterretningstjenesternes generelle målsætning. Denne gennemgang omfatter en vurdering af værdien af alle former for indsamling af efterretninger, herunder signalefterretning, og der kigges både tilbage — i hvor høj grad er det lykkedes efterretningstjenesterne at nå deres mål? — og frem — hvad har efterretningstjenesterne brug for fremover? Dette sikrer, at signalefterretningsressourcer anvendes på de vigtigste nationale prioriteter.

Som det fremgår af denne omfattende oversigt beslutter efterretningstjenesterne ikke alene, hvilke samtaler de skal lytte til, de forsøger ikke at indsamle alt, og de er underlagt kontrol. Deres aktiviteter er rettet mod prioriteter fastlagt af politiske beslutningstagere gennem en proces, der involverer input fra mange regeringsorganer, og denne proces overvåges internt i NSA og af ODNI, justitsministeriet og forsvarsministeriet.

PPD-28 indeholder ligeledes en række andre bestemmelser, der skal sikre, at personoplysninger indsamlet gennem signalefterretning beskyttes, uanset nationalitet. I henhold til PPD-28 skal der f.eks. indføres procedurer for datasikkerhed, indsigt og kvalitet for at beskytte personoplysninger indsamlet gennem signalefterretning og obligatorisk uddannelse for at sikre, at medarbejderne forstår forpligtelsen til at beskytte personoplysninger, uanset nationalitet. PPD omfatter ligeledes andre tilsyns- og kontrolmekanismer. Tilsyns- og kontrolansvarlige skal regelmæssigt revidere og kontrollere praksis for beskyttelse af personoplysninger indeholdt i signalefterretninger. I forbindelse med kontrollen skal der ligeledes være fokus på agenturnes overholdelse af procedurerne for beskyttelse af disse oplysninger.

I henhold til PPD-28 skal alvorlige tilfælde af manglende overholdelse, der involverer ikke-amerikanske personer, behandles på øverste regeringsniveau. I alvorlige tilfælde af manglende overholdelse, der involverer personoplysninger, uanset for hvem, indsamlet gennem signalefterretning, skal de — ud over eksisterende indberetningskrav — straks indberettes til DNI. Hvis der er tale om personoplysninger om en udlænding, beslutter DNI i samråd med den amerikanske udenrigsminister og lederen af den indberettende efterretningsenhed, om der bør tages skridt til at underrette den relevante udenlandske regering i overensstemmelse med beskyttelsen af kilder og metoder og af personer i De Forenede Staters tjeneste. I medfør af PPD-28 har den amerikanske udenrigsminister desuden udpeget en seniorkoordinator, viceminister Catherine A. Novelli, der skal være kontaktpunkt for udenlandske regeringer, der ønsker at rejse spørgsmål om amerikanske signalefterretningsaktiviteter. Dette tilsagn om inddragelse på højt niveau illustrerer den indsats, som den amerikanske regering har gjort gennem de seneste år for at skabe tillid til de mange og overlappende foranstaltninger til beskyttelse af amerikanske personers og ikke-amerikanske personers personoplysninger.

e. Sammenfatning

De amerikanske procedurer for indsamling, opbevaring og formidling af udenlandske efterretninger tilvejebringer vigtige foranstaltninger til beskyttelse af alles personoplysninger, uanset nationalitet. Disse procedurer sikrer navnlig, at de amerikanske efterretningstjenester har fokus på den nationale sikkerhedsopgave i henhold til gældende love, præsidentielle dekretter og præsidentielle direktiver, at de beskytter oplysninger mod uautoriseret adgang, brug og videregivelse og gennemfører deres aktiviteter under tilsyn og kontrol på flere niveauer, herunder kongressens tilsynsudvalg. PPD-28 og procedurerne til gennemførelse heraf er resultatet af vores bestræbelser på at udvide visse principper for minimering og andre vigtige principper for beskyttelse af oplysninger til at omfatte alles personoplysninger, uanset nationalitet. Personoplysninger indsamlet gennem amerikansk signalefterretning er omfattet af principperne og kravene fastlagt i amerikansk ret og i præsidentielle direktiver og dekretter, herunder af beskyttelsesforanstaltningerne i PPD-28. Disse principper og krav sikrer, at alle personer behandles med værdighed og respekt, uanset deres nationalitet eller bopæl, og det anerkendes, at alle personer har legitime interesser i beskyttelsen af privatlivets fred ved behandlingen af deres personoplysninger.

II. FOREIGN INTELLIGENCE SURVEILLANCE ACT — SECTION 702

Indsamling under Section 702 i Foreign Intelligence Surveillance Act ⁽¹⁾ er ikke »omfattende og vilkårlig«, men snævert fokuseret på indsamling af udenlandske efterretninger fra individuelt identificerede legitime mål, indsamlingen har klar lovhjemmel og er underlagt både uafhængigt retsligt tilsyn og den udøvende magts og kongressens omfattende kontrol og tilsyn. Indsamling under Section 702 betragtes som signalefterretning omfattet af kravene i PPD-28 ⁽²⁾.

Indsamling under Section 702 er en af de mest værdifulde efterretningskilder, der beskytter både USA og vores europæiske partnere. Der er offentliggjort omfattende oplysninger om Section 702. En lang række sagsakter, retsafgørelser og tilsynsrapporter vedrørende programmet er blevet afklassificeret og offentliggjort på ODNI's offentlige websted: www.icontherecord.tumblr.com. Section 702 er desuden blevet grundigt analyseret af PCLOB i en rapport, der er tilgængelig på adressen: <https://www.pclob.gov/library/702-Report.pdf> ⁽³⁾.

Section 702 blev vedtaget som en del af FISA Amendments Act fra 2008 ⁽⁴⁾ efter en omfattende offentlig debat i den amerikanske kongres. Den tillader indsamling af udenlandske efterretningsoplysninger gennem målrettet overvågning af ikkeamerikanske personer bosiddende uden for USA med tvungen bistand fra amerikanske udbydere af elektroniske kommunikationstjenester. Section 702 bemyndiger den amerikanske justitsminister og DNI — to embedsmænd på kabinetsniveau udnævnt af præsidenten og godkendt af Senatet — til at indgive årlige certificeringer til FISA-domstolen ⁽⁵⁾. I disse certificeringer identificeres specifikke kategorier af udenlandske efterretninger, der skal indsamles, såsom efterretninger om terrorbekæmpelse eller masseødelæggelsesvåben, som skal henhøre under de kategorier af udenlandske efterretninger, der er defineret i FISA ⁽⁶⁾. Som PCLOB har bemærket, »giver disse begrænsninger ikke beføjelse til ubegrænset indsamling af oplysninger om udlændinge« ⁽⁷⁾.

Certificeringerne skal ligeledes omfatte målretnings- og minimeringsprocedurer, som skal kontrolleres og godkendes af FISA-domstolen ⁽⁸⁾. Formålet med målretningsprocedurerne er at sikre, at indsamlingen sker i medfør af tillagte beføjelser i loven, og at den er omfattet af certificeringernes anvendelsesområde. Formålet med minimeringsprocedurerne er at begrænse indsamlingen, formidlingen og opbevaringen af oplysninger om amerikanske personer, men indeholder ligeledes bestemmelser, der også i høj grad beskytter ikkeamerikanske personers personoplysninger, jf. nedenfor. Som anført ovenfor har præsidenten i PPD-28 pålagt de amerikanske efterretningstjenester at indføre yderligere beskyttelsesforanstaltninger for personoplysninger om ikkeamerikanske personer, og disse beskyttelsesforanstaltninger finder anvendelse på oplysninger indsamlet under Section 702.

Når domstolen har godkendt målretnings- og minimeringsprocedurerne, er indsamling under Section 702 ikke omfattende eller vilkårlig, men »udelukkende rettet mod specifikke [ikke-amerikanske] personer, som er blevet individuelt identificeret«, som anført af PCLOB ⁽⁹⁾. Indsamlingen målrettes ved brug af individuelle selektorer såsom e-mailadresser eller telefonnumre, som det amerikanske efterretningspersonale har vurderet sandsynligvis vil blive anvendt

⁽¹⁾ 50 U.S.C. § 1881a.

⁽²⁾ De amerikanske myndigheder kan ligeledes opnå retsafgørelser i medfør af andre bestemmelser i FISA med henblik på udlevering af oplysninger, herunder oplysninger overført under værnet om privatlivets fred. Se 50 U.S.C. § 1801 *et seq.* I Title I og III i FISA, der tillader henholdsvis elektronisk overvågning og fysiske ransagninger, stilles der krav om en retsafgørelse (undtagen i nødsituationer), og der stilles krav om, at der altid skal være en begrundet mistanke for at antage, at målet for den elektroniske overvågning er en fremmed magt eller en agent fra en fremmed magt. Title IV i FISA tillader anvendelsen af pen-register- og trap and trace-anordninger i medfør af en retsafgørelse (undtagen i nødsituationer) i forbindelse med godkendte udenlandske efterretnings-, kontraspionage- og terrorbekæmpelses efterforskninger. I Title V i FISA bemyndiges FBI til i medfør af en retsafgørelse, (undtagen i nødsituationer) at få udleveret forretningsoplysninger af relevans for godkendte udenlandske efterretnings-, kontraspionage- og terrorbekæmpelses efterforskninger. Som anført nedenfor forbyder USA FREEDOM Act specifikt anvendelsen af FISA-retsafgørelser med henblik på installation af pen-register eller masseindsamling af forretningsoplysninger, og der stilles krav om en »specifik selektor«, der skal sikre en målrettet anvendelse af disse tilladelser.

⁽³⁾ Privacy and Civil Liberties Board, »Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act« (2. juli 2014) (»PCLOB-rapport«).

⁽⁴⁾ Se Pub. L. No. 110-261, 122 Stat. 2436 (2008).

⁽⁵⁾ Se 50 U.S.C. § 1881a(a) og (b).

⁽⁶⁾ Se *id.* § 1801(e).

⁽⁷⁾ Se PCLOB-rapport, s. 99.

⁽⁸⁾ Se 50 U.S.C. § 1881a(d) og (e).

⁽⁹⁾ Se PCLOB-rapport, s. 111.

til at kommunikere udenlandske efterretningsoplysninger af den type, der er omfattet af certificeringen indgivet til domstolen ⁽¹⁾. Grundlaget for udvælgelsen af målet skal dokumenteres, og dokumentationen for hver selektor kontrolleres efterfølgende af det amerikanske justitsministerium ⁽²⁾. Den amerikanske regering har frigivet oplysninger, der viser, at omkring 90 000 personer blev overvåget under Section 702 i 2014, en meget lille del af de over 3 mia. internetbrugere i hele verden ⁽³⁾.

Oplysninger indsamlet under Section 702 er omfattet af de minimeringsprocedurer, som domstolen har godkendt, og som beskytter både ikkeamerikanske personer og amerikanske personer. De er blevet offentliggjort ⁽⁴⁾. Kommunikation, der er opfanget under Section 702, om amerikanske personer eller ikkeamerikanske personer, lagres i databaser med streng adgangskontrol. Kommunikationen må kun gennemgås af efterretningspersonale, som er blevet uddannet i minimeringsprocedurerne til beskyttelse af privatlivets fred, og som er blevet specifikt godkendt til denne adgang, således at de kan varetage deres godkendte funktioner ⁽⁵⁾. Oplysningerne kan kun anvendes til identificering af udenlandske efterretningsoplysninger eller som bevis for en forbrydelse ⁽⁶⁾. I henhold til PPD-28 må disse oplysninger kun formidles til godkendte udenlandske efterretnings- eller retshåndhævelsesformål, og det forhold, at en af parterne i kommunikationen ikke er en amerikansk person, er ikke tilstrækkeligt ⁽⁷⁾. Der fastsættes ligeledes grænser i minimeringsprocedurerne og PPD-28 for, hvor lang tid oplysninger indsamlet under Section 702 kan opbevares ⁽⁸⁾.

Bestemmelserne om tilsyn i Section 702 er omfattende, og tilsynet føres af alle statens tre grene. I agenturer, der gennemfører loven, er der intern kontrol på flere niveauer, herunder de uafhængige generalinspektørers kontrol og teknologisk kontrol af adgangen til oplysningerne. Justitsministeriet og ODNI undersøger nøje anvendelsen af Section 702 for at kontrollere, at reglerne overholdes. Agenturerne er ligeledes selv forpligtet til at indberette potentielle tilfælde af manglende overholdelse. Disse tilfælde undersøges, og alle tilfælde af manglende overholdelse indberettes til Foreign Intelligence Surveillance Court, President's Intelligence Oversight Board og den amerikanske kongres og afhjælpes behørigt. ⁽⁹⁾ Der har indtil dato ikke været nogen tilfælde af forsætlige forsøg på at overtræde loven eller omgå retlige krav ⁽¹⁰⁾.

FISE-domstolen spiller en vigtig rolle i gennemførelsen af Section 702. Domstolen består af uafhængige forbundsdommere, der sidder i en 7-årig embedsperiode ved FISA-domstolen, men som alle forbundsdommere er de ansat i livstidsstillinger. Som anført ovenfor skal domstolen kontrollere, om de årlige certificeringer og målretnings- og minimeringsprocedurerne er i overensstemmelse med lovgivningen. Som ligeledes anført ovenfor skal regeringen desuden straks underrette domstolen om problemer med overholdelsen ⁽¹¹⁾, og en række af domstolens udtalelser er blevet afklassificeret og frigivet, og de viser den ekstraordinære grundige retlige kontrol og domstolens uafhængige kontrol af disse sager.

Domstolens strenge procedurer er blevet beskrevet af den tidligere retspræsident i et brev til den amerikanske kongres, som er blevet offentliggjort ⁽¹²⁾. I henhold til USA FREEDOM Act jf. nedenfor, er domstolen udtrykkeligt bemyndiget til at udnævne en ekstern advokat som en uafhængig fortaler for privatlivets fred i sager, der involverer nye eller væsentlige juridiske spørgsmål ⁽¹³⁾. Den betydelige inddragelse af den uafhængige dommerstand i USA i udenlandske efterretningsaktiviteter rettet mod personer, der hverken er statsborgere eller bosiddende i det pågældende land, er usædvanlig, hvis ikke uden fortilfælde, og det medvirker til at sikre, at indsamling under Section 702 finder sted inden for rammerne af relevante lovlige grænser.

⁽¹⁾ *Idem.*

⁽²⁾ *Idem* s. 8, 50 U.S.C. § 1881a(l), se også NSA Director of Civil Liberties and Privacy Report, »NSA's Implementation of Foreign Intelligence Surveillance Act Section 702« (herefter benævnt »NSA-rapporten«), s. 4, tilgængelig på adressen: <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

⁽³⁾ Director of National Intelligence 2014 Transparency Report, tilgængelig på adressen: http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

⁽⁴⁾ Minimeringsprocedurerne er tilgængelige på adressen: <http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf> (»NSA Minimization Procedures«), <http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf>, og <http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf>.

⁽⁵⁾ Se NSA Report, s. 4.

⁽⁶⁾ Se f.eks. NSA Minimization Procedures, s. 6.

⁽⁷⁾ Intelligence Agency PPD-28-procedurer er tilgængelige på adressen: <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

⁽⁸⁾ Se NSA Minimization Procedures, PPD-28 Section 4.

⁽⁹⁾ Se 50 U.S.C. § 1881(l), se også PCLOB-rapport, s. 66-76.

⁽¹⁰⁾ Se »Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence«, s. 2-3, tilgængelig på adressen: <http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf>.

⁽¹¹⁾ Regel 13 i procedurereglerne for Foreign Intelligence Surveillance Court, tilgængelig på adressen: <http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

⁽¹²⁾ Brev fra Reggie B. Walton til Patrick J. Leahy af 29. juli 2013, tilgængelig på adressen: <http://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

⁽¹³⁾ Se Section 401 i USA FREEDOM Act, P.L. 114-23.

Den amerikanske kongres udøver tilsyn gennem lovpligtige rapporter til efterretnings- og retsudvalgene og gennem hyppige briefinger og høringer. Disse omfatter en halvårlig rapport udarbejdet af den amerikanske justitsminister, der dokumenterer anvendelsen af Section 702 og eventuelle tilfælde af manglende overholdelse, ⁽¹⁾ en særskilt halvårlig vurdering fra den amerikanske justitsminister og DNI, der dokumenterer overholdelsen af målretnings- og minimeringsprocedurerne, herunder overholdelse af de procedurer, der skal sikre, at oplysninger indsamles til godkendte udenlandske efterretningsformål ⁽²⁾, og en årlig rapport fra lederne af efterretningsenheder med en certificering af, at indsamling under Section 702 fortsat genererer udenlandske efterretningsoplysninger ⁽³⁾.

Indsamling under Section 702 er kort sagt hjulmet ved lov og underlagt kontrol og retsligt tilsyn på flere niveauer, og som FISA-domstolen anførte i en nyligt afklassificeret udtalelse, er der ikke tale om masseindsamling eller vilkårlig indsamling, idet indsamlingen er baseret på [...] velafgrænsede afgørelser om målrettet overvågning af individuelle kommunikationsfaciliteter ⁽⁴⁾.

III. USA FREEDOM ACT

USA FREEDOM Act, undertegnet i juni 2015, ændrede i væsentlig grad amerikanske overvågningsbeføjelser og andre nationale sikkerhedsbeføjelser og gav øget offentlig åbenhed omkring brugen af disse beføjelser og om FISA-domstolens afgørelser, jf. nedenfor ⁽⁵⁾. Loven sikrer, at de amerikanske efterretningstjenester og håndhævelsesorganer har de nødvendige beføjelser til at beskytte nationen og samtidig sikre, at den enkeltes privatliv er behørigt beskyttet under udøvelsen af disse beføjelser. Den styrker beskyttelsen af privatlivets fred og borgerlige rettigheder og øger gennemsigtigheden.

Loven forbyder masseindsamling af oplysninger, herunder om både amerikanske og ikkeamerikanske personer, i henhold til forskellige bestemmelser i FISA eller gennem anvendelsen af nationale sikkerhedsbreve, der er en form for lovhjemlede administrative pålæg ⁽⁶⁾. Dette forbud omfatter navnlig telefonmetadata vedrørende samtaler mellem personer i USA og personer uden for USA og vil ligeledes omfatte indsamling af oplysninger under værnet om privatlivets fred i medfør af disse beføjelser. Ifølge loven skal regeringen basere anmodninger om oplysninger i medfør af disse beføjelser på en specifik selektor (»specific selection term«), dvs. en term, der specifikt identificerer en person, konto, adresse eller personlig anordning på en måde, der begrænser mængden af indhentede oplysninger, når det med rimelighed kan lade sig gøre ⁽⁷⁾. Dette sikrer endvidere, at indsamlingen af disse oplysninger til efterretningsformål er nøje målrettet.

Loven har ligeledes i væsentlig grad ændret proceduren ved FISA-domstolen, der både øger gennemsigtigheden og giver større sikkerhed for, at privatlivets fred vil blive beskyttet. Som anført ovenfor giver loven hjemmel til nedsættelse af et fast panel bestående af sikkerhedsclearede advokater med ekspertise inden for beskyttelse af privatlivets fred, indsamling af efterretninger, kommunikationsteknologi eller andre relevante områder, og de kan udpeges til at møde for domstolen som *amicus curiae* i sager, som involverer væsentlige eller nye fortolkninger af lovgivningen. Disse advokater er bemyndiget til at fremsætte retlige argumenter, der øger beskyttelsen af privatlivets fred og borgerlige rettigheder, og de vil få adgang til alle oplysninger, herunder klassificerede informationer, som domstolen beslutter, er nødvendige for, at de kan varetage deres opgaver ⁽⁸⁾.

Loven er ligeledes baseret på den amerikanske regerings hidtil usete gennemsigtighed omkring efterretningsaktiviteter ved at stille krav om, at DNI i samråd med den amerikanske justitsminister foretager en afklassificeringsgennemgang af enhver afgørelse, kendelse eller udtalelse udstedt af FISA-domstolen eller af Foreign Intelligence Surveillance Court of Review, som indeholder en væsentlig forståelse eller fortolkning af lovbestemmelser.

⁽¹⁾ Se 50 U.S.C. § 1881f.

⁽²⁾ Se også § 1881a(l)(1).

⁽³⁾ Se også § 1881a(l)(3). Nogle af disse rapporter er klassificerede.

⁽⁴⁾ Udtalelse og afgørelse, 26 (FISC 2014), tilgængelig på adressen: <http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

⁽⁵⁾ Se USA FREEDOM Act fra 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.

⁽⁶⁾ Se *idem* §§ 103, 201, 501. Nationale sikkerhedsbreve har hjemmel i en række love og giver kun FBI mulighed for at indhente registeroplysninger såsom kreditoplysninger, finansielle oplysninger og elektroniske abonnent- og transaktionsoplysninger fra visse typer virksomheder med henblik på beskyttelse mod international terrorisme eller hemmelige efterretningsaktiviteter. Se 12 U.S.C. § 3414, 15 U.S.C. §§ 1681u-1681v og 18 U.S.C. § 2709. FBI anvender typisk nationale sikkerhedsbreve til at indsamle kritiske ikke-indholdsmæssige oplysninger i de tidlige faser af terrorbekæmpelses- og kontrapionageefterforskninger — såsom identiteten af en abonnent, som muligvis har kommunikeret med agenter i en terrorgruppe som f.eks. ISIL. Modtagere af et nationalt sikkerhedsbrev kan anfægte det ved domstolene. Se 18 U.S.C. § 3511.

⁽⁷⁾ Se *idem*.

⁽⁸⁾ Se *idem* § 401.

Loven foreskriver desuden omfattende åbenhed omkring anmodninger om indsamling i henhold til FISA og gennem nationale sikkerhedsbreve. Den amerikanske regering skal hvert år bl.a. oplyse den amerikanske kongres og offentligheden om det antal FISA-kendelser og -certificeringer, der er anmodet om og udstedt, om det skønnede antal overvågede og berørte amerikanske og ikkeamerikanske personer og om antallet af udnævnelser af amici curiae ⁽¹⁾. I loven stilles der ligeledes yderligere krav om offentliggørelse af antallet af anmodninger om nationale sikkerhedsbrev vedrørende både amerikanske og ikkeamerikanske personer ⁽²⁾.

Med hensyn til gennemsigtighed i virksomhederne giver loven virksomheder en række muligheder for at offentliggøre det samlede antal FISA-kendelser og direktiver eller nationale sikkerhedsbreve, de modtager fra myndighederne, samt antallet af kundekonti, som er omfattet af disse kendelser ⁽³⁾. Flere virksomheder har allerede offentliggjort disse tal, hvilket har vist, at der kun er blevet anmodet om oplysninger om et begrænset antal kunder.

Disse virksomheders gennemsigtighedsrapporter viser, at de amerikanske efterretningstjenesters anmodninger om efterretninger kun berører en meget lille del af alle oplysninger. En stor virksomheds nylige gennemsigtighedsrapport viste f.eks., at de anmodninger til nationale sikkerhedsformål (i henhold til FISA eller gennem nationale sikkerhedsbreve), som virksomheden modtog, berørte under 20 000 af virksomhedens konti på et tidspunkt, hvor virksomheden havde mindst 400 mio. abonnenter. Med andre ord var under 0,005 % af virksomhedens abonnenter berørt af anmodningerne til nationale sikkerhedsformål i USA. Selv hvis hver eneste af disse anmodninger havde vedrørt safe harbor-data, hvilket naturligvis ikke er tilfældet, er det åbenlyst, at anmodningerne er målrettede og passende med hensyn til mængden af oplysninger, og at der ikke er tale om masseindsamling eller vilkårlig indsamling.

Endelig understreges det, at selv om de love, der hjemler nationale sikkerhedsbreve, allerede begrænsede de omstændigheder, under hvilke en modtager af et sådant brev kan forbydes at offentliggøre brevet, blev det ligeledes fastslået i loven, at krav om beskyttelse af oplysninger skal evalueres regelmæssigt, og at modtagere om nationale sikkerhedsbreve skal underrettes, når et krav om beskyttelse af oplysninger ikke længere er begrundet i faktiske forhold, og loven kodificerede procedurerne for modtagernes anfægtelse af krav om beskyttelse af oplysninger ⁽⁴⁾.

De vigtige ændringer af de amerikanske efterretningstjenesters beføjelser, der blev indført med USA FREEDOM Act, er således et klart bevis på USA's omfattende bestræbelser på at bringe beskyttelsen af personoplysninger, privatlivets fred, borgerlige rettigheder og gennemsigtighed i front i hele den amerikanske efterretningspraksis.

IV. GENNEMSIGTIGHED

Ud over den gennemsigtighed, der er foreskrevet i USA FREEDOM Act, giver de amerikanske efterretningstjenester offentligheden mange yderligere oplysninger og sætter således et godt eksempel med hensyn til gennemsigtighed i amerikanske efterretningsaktiviteter. De amerikanske efterretningstjenester har offentliggjort mange af deres politikker og procedurer, afgørelser fra Foreign Intelligence Surveillance Court og andet afklassificeret materiale og sikrer således en ekstraordinær høj grad af gennemsigtighed. Efterretningstjenesterne offentliggør derudover nu i langt højere grad statistikker vedrørende regeringens anvendelse af nationale sikkerhedsbeføjelser til indsamling af oplysninger. Den 22. april 2015 udstedte de amerikanske efterretningstjenester den anden årsrapport med statistikker over, hvor ofte regeringen anvender disse vigtige beføjelser. ODNI har på sit websted og på IC On the Record ligeledes offentliggjort en række konkrete gennemsigtighedsprincipper ⁽⁵⁾ og en gennemførelsesplan, der omsætter principperne til konkrete, målbare initiativer ⁽⁶⁾. I oktober 2015 pålagde direktøren for National Intelligence de enkelte efterretningsenheder at udpege en ansvarlig for gennemsigtighed i efterretningsaktiviteter på ledelsesniveau, der skal fremme gennemsigtighed og stå i spidsen for gennemsigtighedsinitiativer ⁽⁷⁾. Den ansvarlige vil arbejde tæt sammen med den databeskyttelsesansvarlige (privacy and civil liberties officer) i den enkelte efterretningstjeneste for at sikre, at gennemsigtighed, beskyttelse af privatlivets fred og borgerlige rettigheder vedbliver med at være topprioriteter.

⁽¹⁾ Se *idem* § 602.

⁽²⁾ Se *idem*.

⁽³⁾ Se *idem* § 603.

⁽⁴⁾ Se *idem* §§ 502(f)-503.

⁽⁵⁾ Tilgængelig på adressen: <http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles>.

⁽⁶⁾ Tilgængelig på adressen: <http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf>.

⁽⁷⁾ Se *idem*.

Som et eksempel på disse bestræbelser har NSA's Chief Privacy and Civil Liberties Officer frigivet flere uklassificerede rapporter gennem de seneste par år, herunder rapporter om aktiviteter i henhold til Section 702, Executive Order 12333 og USA FREEDOM Act⁽¹⁾. De amerikanske efterretningstjenester samarbejder desuden tæt med PCLOB, den amerikanske kongres og andre aktører inden for beskyttelse af privatlivets fred om at skabe yderligere åbenhed omkring amerikanske efterretningstjenester, når det er muligt og foreneligt med beskyttelsen af følsomme efterretningskilder og -metoder. De amerikanske efterretningsaktiviteter er som helhed lige så eller mere gennemsigtige end mange andre nationers efterretningsaktiviteter verden over og er så gennemsigtige som muligt under hensyntagen til behovet for at beskytte følsomme kilder og metoder.

Sammenfatning af den omfattende gennemsigtighed omkring amerikanske efterretningsaktiviteter:

- De amerikanske efterretningstjenester har frigivet og offentliggjort flere tusinde sider online vedrørende domstolsudtalelser og agenturernes procedurer, hvor der redegøres for de specifikke procedurer og krav, der gælder for de amerikanske efterretningsaktiviteter. Vi har ligeledes frigivet rapporter om efterretningstjenesternes overholdelse af gældende begrænsninger.
- Ledende embedsmænd i efterretningstjenesterne taler jævnligt offentligt om deres organisationers rolle og aktiviteter og redegør i denne forbindelse for de efterlevelsensordninger og sikkerhedsforanstaltninger, der gælder for deres arbejde.
- Efterretningstjenesterne har frigivet mange andre dokumenter om efterretningsaktiviteter omfattet af Freedom of Information Act.
- Præsidenten har udstedt PPD-28, der officielt lægger yderligere begrænsninger på vores efterretningsaktiviteter, og ODNI har udstedt to offentlige rapporter om gennemførelsen af disse begrænsninger.
- Efterretningstjenesterne skal nu i henhold til loven frigive FISA-domstolens væsentlige udtalelser og sammendrag af disse udtalelser.
- Regeringen skal hvert år rapportere om omfanget af anvendelsen af visse nationale sikkerhedsbeføjelser, og virksomhederne er ligeledes bemyndiget hertil.
- PCLOB har udstedt flere detaljerede offentlige rapporter om efterretningsaktiviteter og vil også gøre dette fremover.
- De amerikanske efterretningstjenester forelægger omfattende klassificerede informationer for kongressens tilsynsudvalg.
- DNI har udstedt gennemsigtighedsprincipper, der regulerer efterretningstjenesternes aktiviteter.

Denne store åbenhed vil blive større fremover. Alle oplysninger, der offentliggøres, vil naturligvis blive stillet til rådighed for det amerikanske handelsministerium og Europa-Kommissionen. Handelsministeriets og Europa-Kommissionens årlige evaluering af gennemførelsen af værnet om privatlivets fred vil være en anledning for Europa-Kommissionen til at drøfte eventuelle spørgsmål foranlediget af nye frigivne oplysninger og andre spørgsmål vedrørende værnet om privatlivets fred og dets funktion, og vi forstår, at ministeriet i påkommende tilfælde kan invitere repræsentanter fra andre organer, herunder de amerikanske efterretningstjenester, til at deltage i denne evaluering. EU-medlemsstaterne kan naturligvis derudover i medfør af PPD-28 rejse overvågningsrelaterede spørgsmål over for en udpeget embedsmand i det amerikanske udenrigsministerium.

V. KLAGEGADGANG

Amerikansk ret indeholder en række klagemuligheder for personer, der har været genstand for ulovlig elektronisk overvågning til nationale sikkerhedsformål. I henhold til FISA er retten til at søge erstatning ved amerikanske domstole ikke begrænset til amerikanske borgere. En person, der kan dokumentere sin søgsmålskompetence, har adgang til retsmidler, der gør det muligt at klage over ulovlig elektronisk overvågning i henhold til FISA. I henhold til FISA kan

⁽¹⁾ Tilgængelig på adressen: https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf, https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf, https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

personer, der har været genstand for ulovlig elektronisk overvågning, f.eks. sagsøge embedsmænd personligt for økonomisk erstatning, herunder pønalt begrundet forhøjet erstatning (punitive damages) og dækning af advokatsalær. Se 50 U.S.C. § 1810. Personer, der kan dokumentere deres søgsmålskompetence, kan ligeledes anlægge private søgsmål for økonomisk erstatning, herunder til dækning af procesomkostninger, mod USA, når deres personoplysninger indsamlet ved elektronisk overvågning i henhold til FISA er blevet ulovligt og forsægtligt anvendt eller videregivet. Se 18 U.S.C. § 2712. Hvis regeringen agter at bruge eller videregive oplysninger indhentet via eller udledt af elektronisk overvågning af den forurettede part i henhold til FISA mod den pågældende i forbindelse med retslige eller administrative procedurer i USA, skal den underrette domstolen og den pågældende om sin hensigt på forhånd, og den pågældende kan herefter gøre indsigelse mod lovligheden af overvågningen og anmode om at få oplysningerne fjernet. Se 50 U.S.C. § 1806. Endelig kan personer, der med forsæt foretager ulovlig elektronisk overvågning i lovens navn eller med forsæt anvender eller videregiver oplysninger indhentet ved ulovlig overvågning, i henhold til FISA, pålægges strafferetlige sanktioner. Se 50 U.S.C. § 1809.

EU-borgere har andre muligheder for at sagsøge embedsmænd for ulovlig statslig brug af eller adgang til oplysninger, herunder embedsmænd, der overtræder loven i forbindelse med ulovlig adgang til eller brug af oplysninger til påståede nationale sikkerhedsformål. Computer Fraud and Abuse Act forbyder bevidst uautoriseret adgang (eller adgang ud over autoriseret adgang) for at indhente oplysninger fra en finansiell institution, den amerikanske regerings computersystemer eller en computer, der opnå adgang til via internettet, samt trusler om at skade beskyttede computere med henblik på afpresning eller misbrug. Se 18 U.S.C. § 1030. Enhver person, uanset nationalitet, der lider skade eller tab som følge af en overtrædelse af denne lov, kan sagsøge lovovertræderen (herunder en embedsmand) for erstatning, forbud eller påbud eller anden rimelig billighedsforanstaltning i henhold til Section 1030(g), uanset om der har været anlagt en straffesag, forudsat at adfærden involverer mindst en af flere af de omstændigheder, der er anført i loven. Electronic Communications Privacy Act (ECPA) regulerer regeringens adgang til lagrede elektroniske kommunikations-, transaktions- og abonnentoplysninger, som tredjepartsudbydere af elektroniske kommunikationstjenester ligger inde med. Se 18 U.S.C. §§ 2701-2712. I henhold til ECPA kan en forurettet part sagsøge embedsmænd for bevidst ulovlig adgang til lagrede oplysninger. ECPA finder anvendelse på alle personer, uanset statsborgerskab, og den forurettede part kan få tilkendt en erstatning og få dækket advokatsalæret. Right to Financial Privacy Act (RFPA) begrænser den amerikanske regerings adgang til individuelle kunders bank- og børsrådgiveroplysninger. Se 12 U.S.C. §§ 3401-3422. I henhold til RFPA kan en bank- eller børsrådgiverkunde sagsøge regeringen for lovbestemt, direkte og pønalt begrundet forhøjet erstatning for uretmæssigt at opnå adgang til kundens oplysninger, og en afgørelse om, at denne uretmæssige adgang var forsægtlig, udløser automatisk en undersøgelse af, om de pågældende statsansatte skal pålægges disciplinære sanktioner. Se 12 U.S.C. § 3417.

Endelig kan enhver henholde sig til Freedom of Information Act (FOIA) som et middel til at søge indsigt i de amerikanske forbundsorganers eksisterende oplysninger om ethvert emne med undtagelse af visse kategorier af oplysninger. Se 5 U.S.C. § 552(b). Disse omfatter begrænsninger for adgang til klassificerede informationer om national sikkerhed, tredjemænds personoplysninger og oplysninger om retshåndhævende efterforskninger og kan sammenlignes med de begrænsninger, som andre nationer pålægger i deres egne offentlighedslove. Disse begrænsninger gælder både for amerikanere og ikkeamerikanere. Tvister om udlevering af optegnelser udbedt i medfør af FOIA kan påklages administrativt og herefter ved forbundsdomstolene. Domstolen skal træffe en de novo-afgørelse om, hvorvidt optegnelserne tilbageholdes lovligt, 5 U.S.C. § 552(a)(4)(B), og kan tvinge offentlige myndigheder til at give adgang til optegnelser. I nogle tilfælde har domstolene ophævet myndighedernes afgørelser om tilbageholdelse af oplysninger som klassificerede informationer⁽¹⁾. Selv om der ikke gives økonomisk erstatning, kan domstolen tilkende et beløb til dækning af advokatsalær.

VI. KONKLUSION

USA anerkender, at der i vores signalefterretnings- og andre efterretningsaktiviteter skal tages hensyn til, at alle mennesker bør behandles med værdighed og respekt, uanset deres nationalitet eller bopæl, og at alle mennesker har legitime interesser i beskyttelsen af privatlivets fred ved behandlingen af deres personoplysninger. USA bruger kun signalefterretning til at fremme sine nationale sikkerhedsinteresser og udenrigspolitiske interesser og til at beskytte sine borgere og borgerne i USA's allierede lande og partnerlande mod skade. De amerikanske efterretningstjenester foretager kort sagt ikke vilkårlig overvågning af nogen, herunder almindelige europæiske borgere. Indsamling af signalefterretninger finder kun sted, når den er behørigt godkendt, og under streng overholdelse af disse begrænsninger og først

⁽¹⁾ Se f.eks. *New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

efter en overvejelse af tilgængelige alternative kilder, herunder diplomatiske og offentlige kilder, og på en måde, der prioriterer relevante og mulige alternativer. Indsamlingen af signalefterretninger rettes desuden så vidt muligt kun mod specifikke udenlandske efterretningsmål eller -emner ved brug af diskriminanter.

Den amerikanske politik på dette område blev bekræftet i PPD-28. De amerikanske efterretningstjenester har ikke retlig myndighed, ressourcer, teknisk kapacitet eller et ønske om at opfange hele verdens kommunikation inden for disse rammer. Disse tjenester læser ikke alle amerikaneres eller alle mennesker i hele verdens e-mail. I overensstemmelse med PPD-28 beskytter USA i vidt omfang ikkeamerikanske personers personoplysninger indsamlet gennem signalefterretningsaktiviteter. Dette omfatter i muligt omfang under hensyntagen til den nationale sikkerhed politikker og procedurer udformet med henblik på at minimere opbevaringen og formidlingen af personoplysninger vedrørende ikkeamerikanske personer, der kan sammenlignes med den beskyttelse, som amerikanere har. Som anført ovenfor er det omfattende tilsyn i henhold til Section 702 FISA uden fortilfælde. Endelig øger de vigtige ændringer af lovgivningen om efterretningsvirksomhed i USA FREEDOM Act og ODNI's initiativer til fremme af gennemsigtighed i de amerikanske efterretnings-tjenester i betydelig grad beskyttelsen af alle menneskers privatliv og borgerlige rettigheder, uanset deres nationalitet.

Med venlig hilsen

Robert S. Litt

Den 21. juni 2016

Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Avenue, N.W.
Washington, DC 20230

Kære Justin S. Antonipillai og Ted Dean,

Jeg henvender mig til Dem for at fremlægge yderligere oplysninger om måden, hvorpå USA foretager masseindsamling af signalefterretninger. Som det fremgår af fodnote 5 i Presidential Policy Directive 28 (PPD-28), henviser »masseindsamling« til indhentning af et forholdsvist højt antal signalefterretningsoplysninger eller -data under omstændigheder, hvor efterretningstjenesterne ikke kan anvende en identifikator knyttet til et specifikt mål (såsom målets e-mailadresse eller telefonnummer) for at målrette indsamlingen. Dette betyder dog ikke, at denne form for indsamling er »omfattende« eller »vilkårlig«. Af PPD-28 fremgår det desuden, at »[i]ndsamlingen af signalefterretninger skal være så målrettet som muligt«. For at udføre denne opgave træffer efterretningstjenesterne foranstaltninger for at øge sandsynligheden for, at de oplysninger, der skal indsamles, selv når vi ikke kan anvende specifikke identifikatorer til at målrette indsamlingen, indeholder udenlandske efterretninger, der opfylder de behov, som de amerikanske beslutningstagere har fastsat efter den fremgangsmåde, jeg redegjorde for i mit tidligere brev, og minimerer mængden af indsamlet information, som ikke er relevant.

Efterretningstjenesterne kan eksempelvis blive anmodet om at indhente signalefterretninger om en terrorgruppe, som er aktiv i en region i et land i Mellemøsten, og som menes at planlægge angreb mod vesteuropæiske lande, men hvor der ikke er kendskab til navnene, telefonnumrene, e-mailadresserne eller andre specifikke identifikatorer på de personer, der er knyttet til denne terrorgruppe. Vi kan vælge at foretage en målrettet overvågning af denne gruppe ved at indsamle meddelelser til og fra denne region med henblik på nærmere undersøgelse og analyse, således at de meddelelser, der vedrører denne gruppe, kan indkredses. I forbindelse hermed vil efterretningstjenesterne forsøge at indsnævre indsamlingen så meget som muligt. Dette betragtes som »masseindsamling«, fordi brugen af diskriminanter ikke er mulig, men indsamlingen er hverken »omfattende« eller »vilkårlig«, men snarere snævert fokuseret i videst muligt omfang.

Selv når det ikke er muligt at foretage en målrettet indsamling ved hjælp af specifikke selektorer, indsamler USA derfor ikke alle meddelelser fra samtlige kommunikationsfaciliteter i hele verden, men gør brug af filtre og andre tekniske redskaber til at målrette sin indsamling til de faciliteter, hvor der er sandsynlighed for at indsamle meddelelser, der indeholder relevante udenlandske efterretninger. Således indsamler USA kun efterretningssignaler fra en brøkdel af de meddelelser, der overføres via internettet.

Fordi »masseindsamling« udgør en større risiko for at indsamle ikkerekvante meddelelser, hvilket også blev fremhævet i mit tidligere brev, begrænser PPD-28 efterretningstjenesternes anvendelse af masseindsamlede signalefterretninger til seks bestemte formål. Ved PPD-28 og agenturernes politikker til gennemførelse af PPD-28 er der også indført begrænsninger for opbevaring og formidling af personoplysninger indhentet via signalefterretninger, uanset om oplysningerne blev indhentet via masseindsamling eller målrettet indsamling, og uanset den enkelte persons nationalitet.

Efterretningstjenesternes »masseindsamling« er derfor ikke »omfattende« eller »vilkårlig«, men indebærer anvendelsen af metoder og redskaber til filtrering af indsamlingen, således at der med indsamlingen fokuseres på materiale, som opfylder beslutningstagernes behov for udenlandske efterretninger, samtidig med at indsamlingen af ikkerekvante

oplysninger mindskes, samt strenge regler for at beskytte ikkerelevante oplysninger, som eventuelt indhentes. De politikker og procedurer, der er beskrevet i dette brev, gælder for alle former for masseindsamling af signalefterretninger, herunder en eventuel masseindsamling af meddelelser til og fra Europa, idet det hverken bekræftes eller benægtes, hvorvidt en sådan indsamling finder sted.

De har også anmodet om flere oplysninger om tilsynsrådet Privacy and Civil Liberties Oversight Board (PCLOB) og generalinspektørerne samt om deres beføjelser. PCLOB er et uafhængigt agentur, der henhører under den udøvende magt. Rådet består af fem medlemmer, som uanset politisk parti udnævnes af præsidenten og bekræftes af senatet ⁽¹⁾. Hvert medlem er udnævnt for en periode på seks år. Rådets medlemmer og personale gennemgår den fornødne sikkerhedsgodkendelse for at kunne udføre deres arbejde og ansvar fuldt ud ⁽²⁾.

PCLOB's mission er at sikre, at den føderale regerings bestræbelser på at forhindre terrorisme står i et rimeligt forhold til behovet for at beskytte privatlivets fred og borgerlige rettigheder. Rådet har to grundlæggende ansvarsområder — tilsyn og rådgivning. PCLOB fastsætter sin egen dagsorden og afgør selv, hvilke tilsyns- eller rådgivningsaktiviteter den ønsker at foretage.

For så vidt angår *tilsyn* undersøger og analyserer PCLOB de foranstaltninger, som den udøvende magt træffer med henblik på at beskytte nationen mod terrorisme, og sikrer dermed, at behovet for sådanne foranstaltninger står i et rimeligt forhold til behovet for at beskytte privatlivets fred og borgerlige rettigheder ⁽³⁾. I PCLOB's seneste tilsynsundersøgelse blev der fokuseret på overvågningsprogrammer gennemført i henhold til Section 702 i FISA ⁽⁴⁾. Rådet er i øjeblikket i færd med at foretage en undersøgelse af efterretningsaktiviteter foretaget som led i Executive Order 12333 ⁽⁵⁾.

For så vidt angår *rådgivning* sørger PCLOB for, at der i forbindelse med udarbejdelsen og gennemførelsen af love, bestemmelser og politikker, som vedrører bestræbelserne på at beskytte nationen mod terrorisme, tages tilstrækkeligt hensyn til betænkeligheder på frihedsområdet ⁽⁶⁾.

For at gennemføre sin mission er rådet ved lov tillagt beføjelser til at få indsigt i samtlige organers relevante optegnelser, rapporter, revisioner, evalueringer, dokumenter, papirer og anbefalinger, herunder klassificerede oplysninger i overensstemmelse med loven ⁽⁷⁾. Derudover kan rådet gennemføre interview og indhente erklæringer eller offentlige vidneudsagn fra enhver embedsmand eller medarbejder, der er ansat inden for den udøvende magt ⁽⁸⁾. Rådet kan desuden skriftligt anmode justitsministeren om på rådets vegne at indstævne parter uden for den udøvende magt til at fremlægge relevante oplysninger ⁽⁹⁾.

Endelig er PCLOB ved lov underlagt offentlige gennemsigtighedskrav. Dette indebærer, at offentligheden gennem offentlige høringer og offentligt tilgængelige rapporter holdes orienteret om rådets aktiviteter i videst mulig omfang og under hensyntagen til beskyttelsen af klassificerede oplysninger ⁽¹⁰⁾. Derudover er PCLOB forpligtet til at aflægge rapport, hvis et agentur under den udøvende magt undlader at følge rådets rådgivning.

Generalinspektørerne i efterretningstjenesterne foretager revisioner, inspektioner og undersøgelser af efterretningstjenesternes programmer og aktiviteter for at indkredse og håndtere systemiske risici, svagheder og mangler. Derudover undersøger generalinspektørerne klager eller oplysninger om angivelige overtrædelser af love, regler eller bestemmelser eller dårlig forvaltning, spild af offentlige midler, magtmisbrug eller en betydelig eller specifik fare for folkesundheden eller den offentlige sikkerhed i efterretningstjenestens programmer og aktiviteter. For at sikre objektivitet og integritet

⁽¹⁾ 42 U.S.C. 2000ee(a), (h).

⁽²⁾ 42 U.S.C. 2000ee(k).

⁽³⁾ 42 U.S.C. 2000ee(d)(2).

⁽⁴⁾ Generelle oplysninger er tilgængelige på adressen: <https://www.pclob.gov/library.html#oversightreports>.

⁽⁵⁾ Generelle oplysninger er tilgængelige på adressen: <https://www.pclob.gov/events/2015/may13.html>.

⁽⁶⁾ 42 U.S.C. 2000ee(d)(1); se også PCLOB Advisory Function Policy and Procedure, Policy 2015-004, tilgængelig på adressen: https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.

⁽⁷⁾ 42 U.S.C. 2000ee(g)(1)(A).

⁽⁸⁾ 42 U.S.C. 2000ee(g)(1)(B).

⁽⁹⁾ 42 U.S.C. 2000ee(g)(1)(D).

⁽¹⁰⁾ 42 U.S.C. 2000ee(f).

i samtlige rapporter, resultater og anbefalinger, som generalinspektørerne udarbejder, er det yderst vigtigt, at generalinspektørerne er uafhængige. Nogle af de vigtigste komponenter for at sikre generalinspektørernes uafhængighed omfatter proceduren for generalinspektørernes udnævnelse og afsættelse, de separate beføjelser for så vidt angår drift, budget og personale og kravene om dobbelt indberetning til lederne af agenturerne under den udøvende magt og kongressen.

Kongressen har i hvert agentur under den udøvende magt, herunder i alle efterretningstjenester, oprettet et uafhængigt kontor for generalinspektørerne ⁽¹⁾. Med vedtagelsen af Intelligence Authorization Act for Fiscal Year 2015 bliver næsten alle generalinspektører med ansvar for tilsynet med en efterretningsenhed udnævnt af præsidenten og bekræftet af senatet, herunder justitsministeriet, den centrale efterretningstjeneste (CIA), det nationale sikkerhedsagentur (NSA) og efterretningstjenesterne ⁽²⁾. Derudover er disse generalinspektører fastansatte embedsmænd uden partitilknytning, som kun præsidenten kan afsætte. Selv om præsidenten ifølge den amerikanske forfatning skal have beføjelse til at afsætte en generalinspektør, er den sjældent blevet udøvet, og præsidenten skal 30 dage inden afsættelsen af en generalinspektør skriftligt fremsende en begrundelse til kongressen ⁽³⁾. Ved hjælp af denne generalinspektørudnævnelsesprocedure sikres det, at embedsmænd under den udøvende magt ikke uretmæssigt påvirker udnævnelsen eller afsættelsen af en generalinspektør.

For det andet har generalinspektørerne betydelige, lovbestemte beføjelser til at foretage revisioner, undersøgelser og kontroller af den udøvende magts programmer og aktiviteter. Foruden de lovpligtige tilsynsundersøgelser og -kontroller har generalinspektørerne meget frie hænder til at fungere som tilsynsmyndighed for at kontrollere programmer og aktiviteter efter eget valg ⁽⁴⁾. I forbindelse med udøvelsen af denne beføjelse er generalinspektørerne ved lov sikret, at de har selvstændige ressourcer til at udføre deres ansvarsområde, herunder beføjelse til at ansætte deres egne medarbejdere og separat dokumentere deres budgetanmodninger over for kongressen ⁽⁵⁾. Generalinspektørerne har ved lov adgang til de oplysninger, som er nødvendige for at udføre deres ansvarsområde. Dette omfatter beføjelsen til at få direkte indsigt i alle agentureres optegnelser og oplysninger, der uanset klassificering omhandler agentureres programmer og aktiviteter, beføjelsen til at anmode om at få oplysninger og dokumenter fremlagt på grundlag af en »subpoena« og beføjelsen til at administrere edsaflæggelser ⁽⁶⁾. I begrænsede tilfælde kan lederen af et agentur under den udøvende magt forbyde en generalinspektørs aktivitet, f.eks. hvis en generalinspektørs revision eller undersøgelse i væsentlig grad ville gå imod USA's nationale sikkerhedsinteresser. Dog er udøvelsen af denne beføjelse yderst usædvanlig, og det kræver, at lederen af agenturet inden for 30 dage underretter kongressen om begrundelsen herfor ⁽⁷⁾. Faktisk har direktøren for den nationale efterretningstjeneste aldrig udøvet denne beføjelse i forbindelse med en aktivitet udført af en generalinspektør.

For det tredje har generalinspektørerne ansvaret for, at både lederne af den udøvende magts agenturer og formanden for kongressen gennem rapporter orienteres fuldt ud og løbende om svig og andre alvorlige problemer, misbrugsager og mangler i forbindelse med den udøvende magts programmer og aktiviteter ⁽⁸⁾. Ved hjælp af dobbelt indberetning styrkes generalinspektørernes uafhængighed, idet det giver mere gennemsigtighed i generalinspektørernes tilsynsprocedure og agentureres ledere mulighed for at gennemføre generalinspektørernes anbefalinger, inden der træffes lovgivningsmæssige foranstaltninger af kongressen. Generalinspektørerne er f.eks. ved lov forpligtet til at udarbejde halvårslige rapporter, hvori der redegøres for disse problemer samt for de hidtil trufne korrigerende foranstaltninger ⁽⁹⁾. Agenturerne under den udøvende magt tager generalinspektørernes resultater og anbefalinger meget alvorligt, og generalinspektørerne er

⁽¹⁾ Section 2 og 4 i Inspector General Act fra 1978, som ændret (i det følgende benævnt »IG Act«), Section 103H(b) og (e) i National Security Act fra 1947, som ændret (i det følgende benævnt »Nat'l Sec. Act«), og Section 17(a) i Central Intelligence Act (i det følgende benævnt »CIA Act«).

⁽²⁾ Se Pub. L. No. 113-293, 128 Stat. 3990, (Dec. 19, 2014). Det er kun generalinspektørerne for det amerikanske forsvars efterretnings-tjeneste (Defense Intelligence Agency — DIA) og det amerikanske nationale agentur for geospatiale efterretninger (National Geospatial-Intelligence Agency — NGA), som ikke udnævnes af præsidenten. Generalinspektøren for forsvarsministeriet og generalinspektøren for efterretningstjenesterne har dog sammenfaldende beføjelser over disse agenturer.

⁽³⁾ Section 3 i IG Act of 1978, som ændret, Section 103H(c) i Nat'l Sec. Act og Section 17(b) i CIA Act.

⁽⁴⁾ Se Section 4(a) og 6(a)(2) i IG Act fra 1947, Section 103H(e) og (g)(2)(A) i Nat'l Sec. Act og Section 17(a) og (c) i CIA Act.

⁽⁵⁾ Section 3(d), 6(a)(7) og 6(f) i IG Act, Section 103H(d), (i), (j) og (m) i Nat'l Sec. Act og Section 17(e)(7) og (f) i CIA Act.

⁽⁶⁾ Section 6(a)(1), (3), (4), (5) og (6) i IG Act, Section 103H(g)(2) i Nat'l Sec. Act og Section 17(e)(1), (2), (4) og (5) i CIA Act.

⁽⁷⁾ Se f.eks. Section 8(b) og 8E(a) i IG Act, Section 103H(f) i Nat'l Sec. Act og Section 17(b) i CIA Act.

⁽⁸⁾ Section 4(a)(5) i IG Act, Section 103H(a)(b)(3) og (4) i Nat'l Sec. Act og Section 17(a)(2) og (4) i CIA Act.

⁽⁹⁾ Section 2(3), 4(a) og 5 i IG Act, Section 103H(k) i Nat'l Sec. Act og Section 17(d) i CIA Act. Generalinspektøren for justitsministeriet offentliggør sine rapporter på internetadressen: <http://oig.justice.gov/reports/all.htm>. Generalinspektøren for efterretningstjenesterne offentliggør ligeledes sine halvårslige rapporter på adressen: <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

ofte i stand til at indarbejde agenturernes godkendelse og gennemførelse af generalinspektørernes anbefalinger i disse og andre rapporter, der forelægges kongressen og i visse tilfælde offentligheden ⁽¹⁾. Foruden denne dobbelt indberetning er generalinspektørerne også ansvarlige for, at whistleblowere inden for den udøvende magt stilles for de rigtige tilsynsudvalg i kongressen, hvor de kan afsløre påstået svig, spild eller misbrug i den udøvende magts programmer og aktiviteter. Identiteten på de personer, der står frem, holdes hemmelig over for den udøvende magt, hvilket beskytter whistleblowerne fra potentielle disciplinær- eller sikkerhedsgodkendelsesforanstaltninger, der uberettiget træffes som repressalie for at have underrettet generalinspektøren ⁽²⁾. Eftersom whistleblowere ofte er kilder i en generalinspektørs undersøgelse, er muligheden for, at de kan underrette kongressen om deres betænkeligheder uden den udøvende magts indflydelse, med til at øge effektiviteten af generalinspektørernes tilsyn. På grund af denne uafhængighed kan generalinspektørerne fremme økonomi, effektivitet og ansvarlighed i agenturerne under den udøvende magt med objektivitet og integritet.

Endelig har kongressen oprettet Council of Inspectors General on Integrity and Efficiency. Dette råd har bl.a. til opgave at udarbejde standarder for generalinspektørernes revisioner, undersøgelser og kontroller samt at fremme uddannelse og har beføjelse til at foretage undersøgelser af påstået embedsmisbrug blandt generalinspektørerne med henblik på at holde et vågent øje med generalinspektørerne, som er blevet bemyndiget til overvåge alle andre ⁽³⁾.

Jeg håber, at disse oplysninger kan hjælpe Dem videre.

Med venlig hilsen

Robert S. Litt

General Counsel

⁽¹⁾ Section 2(3), 4(a) og 5 i IG Act, Section 103H(k) i Nat'l Sec. Act og Section 17(d) i CIA Act. Generalinspektøren for justitsministeriet offentliggør sine rapporter på internetadressen: <http://oig.justice.gov/reports/all.htm>. Generalinspektøren for efterretningstjenesterne offentliggør ligeledes sine halvårige rapporter på adressen: <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

⁽²⁾ Section 7 i IG Act, Section 103H(g)(3) i Nat'l Sec. Act og Section 17(e)(3) i CIA Act.

⁽³⁾ Section 11 i IG Act.

BILAG VII

**Brev fra Deputy Assistant Attorney General and Counselor for International Affairs Bruce Swartz,
det amerikanske justitsministerium**

Den 19. februar 2016

Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Kære Justin S. Antonipillai og Ted Dean,

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 begrænsningerne for adgang i disse metoder ⁽¹⁾. Disse pålæg indebærer ikke forskelsbehandling, da de anvendes til at indhente oplysninger fra virksomheder i USA, herunder virksomheder, som vil foretage selvcertificering under ordningen for EU's og USA's værn om privatlivets fred, uanset den registreredes nationalitet. 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 amendement til den amerikanske forfatning, hvor det fastslås at, [f]olkets ret til sikkerhed for deres personer, boliger, papirer og ejendele imod urimelige ransagninger og anholdelser må ikke krænkes, og ingen kendelse herom må afsiges uden en sandsynlig årsag, der støtter sig til ed eller højtidelig erklæring og nøje beskriver det sted, der skal ransages, de personer, der skal arresteres, eller de ting, der skal beslaglægges, den amerikanske forfatning, fjerde amendement. IV. 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) (*citing Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). I henhold til fjerde amendement skal de retshåndhævende myndigheder generelt have en dommerkendelse inden en ransagning i forbindelse med indenlandske strafferetlige efterforskninger. Se *Katz v. United States*, 389 U.S. 347, 357 (1967). I de tilfælde, hvor der ikke skal udstedes en kendelse, er regeringsforanstaltningen betinget af en »rimelighedstest« i henhold til fjerde amendement. Forfatningen sikrer derfor i sig selv, at den amerikanske regering ikke har ubegrænsede eller vilkårlige beføjelser til at beslaglægge privatoplysninger.

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

⁽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, se 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v, 18 U.S.C. § 2709, og elektronisk overvågning, ransagningskendelser, forretningsoplysninger og anden indsamling af kommunikation i henhold til Foreign Intelligence Surveillance Act, se 50 U.S.C. § 1801 *et seq.*

⁽²⁾ I dette dokument redegøres for føderale retshåndhævelses- og reguleringsbeføjelser. Overtrædelser af delstatslovgivningen efterforskes af delstaterne 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 påbud kan omfattes af beskyttelse under delstatsforfatninger, der har forrang for beskyttelsen under den amerikanske forfatning. Beskyttelsen under delstatslovgivningen skal mindst svare til beskyttelsen under den amerikanske forfatning, herunder, men ikke begrænset til, fjerde amendement.

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.

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 bistå anklagejuryens efterforskning ved mistanke om en bestemt overtrædelse af straffelovgivningen. Anklagejurier 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. Se Federal Rules of Criminal Procedure — Fed. Se 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 sundhedsydelse, børnemishandling, beskyttelse af efterretningstjenester og kontrollerede stoffer, og i forbindelse med generalinspektørernes undersøgelser af regeringsorganer. Hvis regeringen 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 få ikke-indholdsmæssige 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. Se 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 regeringens adgang til internetudbydere, teleselskabers og andre eksterne tjenesteudbydere 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 ud over, hvad der kræves i forfatningsretten, fra kunder og abonnenter hos internetudbydere. I henhold til SCA øges niveauet af beskyttelsen af privatlivets fred afhængigt af indsamlingens indgribende karakter. Strafferetlige håndhævende myndigheder kan kun få udleveret abonnentoplysninger, IP-adresser og tilknyttede tidsstempler på grundlag af et påbud. I forbindelse med de fleste andre lagrede, ikke-indholdsmæssige oplysninger såsom e-mail-hoveder 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 påbud af en dommer med den begrundelse, at der er begrundet mistanke for at antage, 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 trådbårne, mundtlige eller elektroniske kommunikationer i realtid til strafferetlige efterforskningsformål i medfør af den føderale lovgivning om aflytning. Se 18 U.S.C. §§ 2510-2522. Denne tilladelse gives kun på grundlag af en retsafgørelse, hvor en dommer bl.a. vurderer, at der er begrundet mistanke for at antage, at aflytningen eller den

elektroniske aflytning 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 — Regel 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 ting 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. Se den amerikanske forfatning, fjerde amendement (se nærmere redegørelse ovenfor), Fed. R. Crim. P. 41. Den person, som ransagningskendelsen er udstedt mod, kan anfægte kendelsen med den begrundelse, at den er overdreven, chikanerende eller på anden vis uretmæssigt udstedt, og forurettede parter med søgsmålskompetence kan anmode om at få afvist alle beviser indhentet ved en ulovlig ransagning. Se *Mapp v. Ohio*, 367 U.S. 643 (1961).

Justitsministeriets retningslinjer og politikker: Ud over disse forfatnings-, lov- og regelbaserede begrænsninger for regeringens 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 rettigheder. I den amerikanske justitsministers retningslinjer, Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (september 2008) (i det følgende benævnt AG FBI Guidelines), tilgængelig 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 borgerlige rettigheder 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 unødvendige indtrængninger i lovlige menneskers liv«. Se AG FBI Guidelines, s. 5. FBI har integreret disse retningslinjer i FBI Domestic Investigations and Operations Guide (DIOG), tilgængelig på adressen: [https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20\(DIOG\)](https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG)), en omfattende håndbog, hvor der redegøres i detaljer for begrænsningerne for brugen af efterforskningsmetoder og opstilles retningslinjer, der skal sikre, at borgerlige rettigheder og privatlivets fred beskyttes i enhver efterforskning. Der er fastlagt yderligere regler og politikker, der begrænser forbundsanklagernes efterforskningsaktiviteter i **United States Attorneys' Manual** (USAM), der ligeledes er tilgængelig online på adressen: <http://www.justice.gov/usam/united-states-attorneys-manual>.

Civile og regulerende myndigheder (offentlig interesse)

Der er ligeledes 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 things«). Disse myndigheders administrative eller civilretlige beføjelser til at udstede pålæg er begrænsede, ikke kun på grund af deres statutter, men også på grund af uafhængig domstolsprøvelse af pålæg inden potentiel retshåndhævelse. Se 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. ovenfor.

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. Se 31 U.S.C. § 5318, 31 C.F.R. Part X. Andre virksomheder kan henvise til Fair Credit Reporting Act, se 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. Se f.eks. Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422. 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. Se *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, 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 regeringen i medfør af disse beføjelser.

Med venlig hilsen

Bruce C. Swartz

Deputy Assistant Attorney General and Counselor for
International Affairs
